

Microsoft Customer Agreement

This Microsoft Customer Agreement (the “Agreement”) is between Customer and Microsoft and consists of these General Terms, the applicable Use Rights and SLAs, and any terms mutually agreed upon by Microsoft and Customer which are incorporated into the Agreement.

1. General Terms

These General Terms apply to all of Customer’s orders under this Agreement. Capitalized terms have the meanings given under “Definitions.”

License to use Microsoft Products

- a. **License grant.** Products are licensed and not sold. Upon Microsoft’s acceptance of each order and subject to Customer’s compliance with this Agreement, Microsoft grants Customer a nonexclusive and limited license to use the Products ordered as provided in the applicable Use Rights and this Agreement. These licenses are solely for Customer’s own use and business purposes and are nontransferable except as expressly permitted under this Agreement or applicable law.
- b. **Duration of licenses.** Licenses granted on a subscription basis or for a specified term expire at the end of the applicable subscription period or term unless renewed. Licenses granted for Products billed periodically based on metered usage continue as long as Customer continues to pay for usage of the Product. All other licenses become perpetual upon payment in full.
- c. **Applicable Use Rights.** The latest Use Rights, as updated from time to time, apply to the use of all Products, subject to the following exceptions. (1) For Versioned Software: Material adverse changes published after the date a Product is licensed will not apply to the use of that Product during that license or subscription term unless the changes are published with the release of a new version and a subscription customer chooses to update to that version. (2) For other Products: Material adverse changes published after the start of the subscription term will not apply during the subscription.
- d. **End Users.** Customer will control access to and use of the Products by End Users and is responsible for any use of the Products that does not comply with this Agreement.
- e. **Affiliates.** Customer may order Products for use by its Affiliates. If it does, the licenses granted to Customer under this Agreement will apply to such Affiliates, but Customer will have the sole right to enforce this Agreement against Microsoft. Customer will remain responsible for all obligations under this Agreement and for its Affiliates’ compliance with this Agreement.
- f. **Reservation of Rights.** Microsoft reserves all rights not expressly granted in this Agreement. No rights will be granted or implied by waiver or estoppel. Rights to access or use a Product, Fix, or Services Deliverable on a device do not give Customer any right to implement Microsoft patents or other Microsoft intellectual property in the device itself or in any other software or devices.
- g. **Restrictions.** Except as expressly permitted in this Agreement, or Product, Fix, or Services Deliverable documentation, Customer must not (and is not licensed to): (1) reverse engineer, decompile, or disassemble any Product, Fix, or Services Deliverable or attempt to do so; (2) install or use non-Microsoft software or technology in any way that would subject Microsoft’s intellectual property or technology to any other license terms; (3) work around any technical limitations in a Product, Fix, or Services Deliverable or restrictions in Product, Fix, or Services Deliverable documentation; (4) separate and run parts of the Product, Fix, or Services Deliverable on more than one device; (5) upgrade or downgrade parts of the Product, Fix, or Services Deliverable at different times; (6) transfer parts of a Product, Fix, or Services Deliverable separately; or (7) distribute, sublicense, rent, lease, or lend any Product, Fix, or Services Deliverable, in whole or in part, or use them to offer hosting services to a third party.

- h. License transfers and assignments.** Customer may only transfer fully-paid, perpetual licenses to (1) an Affiliate or (2) a third party solely in connection with the transfer of hardware to which, or employees to whom, the licenses have been assigned as part of (a) a divestiture of all or part of an Affiliate or (b) a merger involving Customer or an Affiliate. Upon such transfer, Customer must uninstall and discontinue using the licensed Product and render any copies unusable. Customer must notify Microsoft of a License transfer and provide the transferee a copy of these General Terms, the applicable Use Rights and any other documents necessary to show the scope, purpose and limitations of the licenses transferred. Attempted license transfers that do not comply with this section are void.
- i. Customer Eligibility.** Customer agrees that if it is purchasing academic, government or nonprofit offers, Customer meets the respective eligibility requirements (<https://aka.ms/eligibilitydefinition>). Microsoft reserves the right to verify eligibility and suspend product use if requirements are not met.

Non-Microsoft Products

Non-Microsoft Products are provided under separate terms by the Publishers of such products. Customer will have an opportunity to review those terms prior to placing an order for a Non-Microsoft Product through a Microsoft online store or Online Service. Microsoft is not a party to the terms between Customer and the Publisher. Microsoft may provide Customer's contact information and transaction details to the Publisher. Microsoft makes no warranties and assumes no responsibility or liability whatsoever for Non-Microsoft Products. Customer is solely responsible and liable for its use of any Non-Microsoft Product.

Verifying compliance

- a. Right to verify compliance.** Microsoft has the right, at its expense, to verify compliance on all use and distribution of products by Customer's and its Affiliates. To such end, Customer must keep records relating to all use and distribution of products. Verification will be conducted through an independent auditor retained by Microsoft, and Customer must provide, without undue delay, all necessary information, including visible access to systems running the Products and evidence of licenses for Products the Customer acquired from a third party, hosts, sublicenses, or distributes to third parties.
- b. Verifying process.** Microsoft will notify Customer at least thirty (30) calendar days in advance of its intent to verify Customer's compliance with the license terms for the Products Customer and its Affiliates use or distribute. The independent auditor is also subject to confidentiality obligation. This verification will take place during normal business hours and the auditor will make best efforts not to interfere with Customer's operations, during the course of the audit.
- c.** All verification efforts undertaken in accordance with this section shall comply with the Customer's reasonable security and safety rules, policies, and procedures ("security rules"), provided that such security rules are applicable to the performance of the verification process(es); the Customer makes such security rules available to Microsoft prior to the commencement of the verification process(es); and such security rules do not modify or amend the terms and conditions of this Agreement.
- d. Remedies for non-compliance.** If verification reveals any use of Products without applicable license rights, then within thirty (30) days, Customer must order sufficient licenses to cover its use and Microsoft will invoice for such licenses at then current GSA MAS schedule rates. Microsoft does not waive its rights to enforce this Agreement or to protect its intellectual property by any other legal or contractual means. Nothing in this section prevents the Customer from disputing any invoice in accordance with the Contract Disputes Act (41 U.S.C. §§7101-7109).
- e. Customer self-audit.** Microsoft, at its sole discretion, may require Customer to conduct a self-audit, subject to the non-compliance remedies as set forth herein.

Privacy

- a. Customer's privacy.** Customer's privacy is important to Microsoft. Please read the Microsoft Privacy Statement (<https://go.microsoft.com/fwlink/?LinkId=521839>) and in Attachment 1 as it describes

the types of data Microsoft collects from Customer and Customer's devices ("Data"), how Microsoft uses that Data, and the legal bases Microsoft has to process that Data.

Confidentiality

- a. **Confidential Information.** "Confidential Information" is non-public information that is designated "confidential" or that a reasonable person should understand is confidential, including, but not limited to, Customer Data, Support and Consulting Data, and Customer's account authentication credentials. Confidential Information does not include information that (1) becomes publicly available without a breach of a confidentiality obligation; (2) the receiving party received lawfully from another source without a confidentiality obligation; (3) is independently developed; or (4) is a comment or suggestion volunteered about the other party's business, products, or services.
- b. **Protection of Confidential Information.** Each party will take reasonable steps to protect the other's Confidential Information and will use the other party's Confidential Information only for purposes of the parties' business relationship. Neither party will disclose Confidential Information to third parties, except to its Representatives, and then only on a need-to-know basis under nondisclosure obligations at least as protective as this Agreement. Each party remains responsible for the use of Confidential Information by its Representatives and, in the event of discovery of any unauthorized use or disclosure, must promptly notify the other party. The Use Rights may provide additional terms regarding the disclosure and use of Customer Data.
- c. **Disclosure required by law.** A party may disclose the other's Confidential Information if required by law, but only after it notifies the other party (if legally permissible) to enable the other party to seek a protective order.
- d. **Residual information.** Neither party is required to restrict work assignments of its Representatives who have had access to Confidential Information. Each party agrees that the use of information retained in Representatives' unaided memories in the development or deployment of the parties' respective products or services does not create liability under this Agreement or trade secret law, and each party agrees to limit what it discloses to the other accordingly.
- e. **Duration of Confidentiality obligation.** These obligations apply (1) for Customer Data, until it is deleted from the Online Services; and (2) for all other Confidential Information, for a period of five years after a party receives the Confidential Information.
- f. **Freedom of Information Act (FOIA).** Notwithstanding anything in this section to the contrary, the parties acknowledge and agree that if Customer is subject to the United States Freedom of Information Act (5 U.S.C. § 552) it may disclose information in response to a valid request in accordance with FOIA. Should Customer receive a request under FOIA for Microsoft's Confidential Information, Customer agrees to give Microsoft adequate prior notice of the request and before releasing Microsoft's Confidential Information to a third party, in order to allow Microsoft sufficient time to seek injunctive relief or other relief against such disclosure.

Product warranties

a. Limited warranties and remedies.

- (1) **Online Services.** Microsoft warrants that each Online Service will perform in accordance with the applicable SLA during Customer's subscription term. Customer's sole remedies for breach of this warranty are described in the SLA.
- (2) **Software.** Microsoft warrants that the Software version that is current at the time Customer acquired it will perform substantially as described in the applicable Product documentation for one year from the date Customer acquires a license for that version. If it does not, and Customer notifies Microsoft within the warranty term, Microsoft will, at its option, (i) return the amount Customer paid for the Software license or a prorated portion of the applicable Subscription fee (ii) repair or replace the Software.

The remedies above are Customer's sole remedies for breach of the warranties in this section. Customer waives any warranty claims not made during the warranty period.

- b. **Exclusions.** The warranties in this Agreement do not apply to problems caused by accident, abuse, or use inconsistent with this Agreement or applicable documentation, including failure to meet minimum system

requirements. These warranties do not apply to free, trial, preview, or prerelease products, services, or features, or to components of Products that Customer is permitted to redistribute (each, a "Limited Offering").

- c. **Disclaimer.** Except for the limited warranties above and subject to applicable law, Microsoft provides no other warranties or conditions for Products and disclaims any other express, implied, or statutory warranties for Products, including warranties of quality, title, noninfringement, merchantability, and fitness for a particular purpose.

Professional Services warranties

- a. **Limited warranties and remedies – Professional Services.** Microsoft warrants that it will perform Professional Services with professional care and skill. If Microsoft fails to do so and Customer notifies Microsoft within 90 days of the date the Professional Services were performed, then Microsoft will, at its discretion, either re-perform the Professional Services or return the price paid for them. Subject to U.S. Federal law, these remedies are Customer's sole remedies for breach of warranties in this section. Customer waives any breach of warranty claims not made during the warranty period.
- b. **Exclusions.** The warranties in this section do not cover problems caused by accident, abuse or use in a manner inconsistent with this Agreement by the Customer, including failure to meet minimum system requirements.
- c. **DISCLAIMER.** Except for the limited warranties above, Microsoft provides no other warranties or conditions and disclaims any other express, implied, or statutory warranties, including warranties of quality, merchantability, fitness for a particular purpose, title and non-infringement.

Defense of third-party claims

Microsoft will have the right to intervene to defend Customer against the third-party claims described in this section and will pay the amount of any resulting adverse final judgment or approved settlement, but only if Microsoft is promptly notified in writing of the claim and has the right to control the defense and any settlement of it (subject to 28 U.S.C. § 516). Customer must provide Microsoft with all reasonably requested assistance and information. Microsoft will reimburse Customer for reasonable out-of-pocket expenses it incurs in providing assistance. This section describes the Customer's sole remedies and Microsoft's entire liability for such claims.

- a. **By Microsoft.** Microsoft will have the right to intervene to defend Customer against any third-party claim to the extent it alleges that a Product, Fix, or Services Deliverable made available by Microsoft for a fee and used within the scope of the license granted under this Agreement (unmodified from the form provided by Microsoft and not combined with anything else), misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party. If Microsoft is unable to resolve a claim of misappropriation or infringement, it may, at its option, either (1) modify or replace the Product, Fix, or Services Deliverable with a functional equivalent or (2) terminate Customer's license and refund any license fees (less depreciation for perpetual licenses), including amounts paid in advance for unused consumption for any usage period after the termination date. Microsoft will not be liable for any claims or damages due to Customer's continued use of a Product, Fix, or Services Deliverable after being notified to stop due to a third-party claim.
- b. **Your agreement to protect.** Customer agrees that use of Customer Data or non-Microsoft software Microsoft hosts on Customer's behalf will not infringe any third party's patent, copyright or trademark or make unlawful use of any third party's Trade Secret. In addition, Customer will not use an Online Service to gain unauthorized access to or disrupt any service, data, account or network in connection with the use of the Online Services.

Notwithstanding the foregoing, Microsoft's rights set forth in this section (and the rights of the third-party claiming infringement) shall be governed by the provisions of 28 U.S.C. § 1498.

Limitation of liability

For each Product or Professional Service, each party's maximum, aggregate liability to the other under this Agreement is limited to direct damages finally awarded in an amount not to exceed the amounts Customer was

required to pay for the Products or Professional Services during the term of the applicable licenses or Statement of Services, subject to the following:

- a. **Subscriptions.** For Products ordered on a subscription basis, Microsoft's maximum liability to Customer for any incident giving rise to a claim will not exceed the amount Customer paid for the Product during the 12 months before the incident.
- b. **Free Professional Services, Products, and distributable code.** For Products or Professional Services provided free of charge and code that Customer is authorized to redistribute to third parties without separate payment to Microsoft, Microsoft's liability is limited to direct damages finally awarded up to US\$5,000.
- c. **Exclusions.** In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, or loss of use, loss of profits, or interruption of business, however caused or on any theory of liability. The foregoing limitation of liability shall not apply to (1) personal injury or death resulting from Licensor's negligence; (2) for fraud; or (3) for any other matter for which liability cannot be excluded by law.
- d. **Exceptions.** No limitation or exclusions under this Agreement will apply to liability arising out of either party's (1) confidentiality obligations (except for liability related to Customer Data or Support and Consulting Data, which will remain subject to the limitations and exclusions above); (2) defense obligations; or (3) violation of the other party's intellectual property rights.
- e. Nothing in this Agreement shall impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Agreement under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

Pricing and payment

Pricing and payment terms related to orders placed by Customer directly with Microsoft are set by Microsoft, and Customer will pay the amount due as described in this section.

- a. **Payment method.** Customer must provide a payment method or, if eligible, choose to be invoiced for purchases made on its account. By providing Microsoft with a payment method, Customer (1) consents to Microsoft's use of account information regarding the selected payment method provided by the issuing bank or applicable payment network; (2) represents that it is authorized to use that payment method and that any payment information it provides is true and accurate; (3) represents that the payment method was established and is used primarily for commercial purposes and not for personal, family or household use; and (4) authorizes Microsoft to charge Customer using that payment method for orders under this Agreement.
- b. **Invoices.** IAW FAR 52.212-4(g), Microsoft will invoice Customers.
- c. **Invoice Payment terms.** Each invoice will identify the amounts payable by Customer to Microsoft for the period corresponding to the invoice. IAW with GSAM 552.212-4(g)(2), Customer will pay all amounts due within ten (10) calendar days following the invoice date after receiving a proper invoice from Microsoft.
- d. **Late Payment.** IAW FAR 52.233-1 Microsoft may submit a Claim on any payments to Microsoft that are more than thirty (30) calendar days past due.
- e. **Reserved.**
- f. **Taxes.** Microsoft prices exclude applicable taxes unless identified as "tax inclusive" and similar. Microsoft shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k) and 552.212-4(x). Microsoft will be responsible for all taxes based upon its net income, gross receipts taxes imposed in lieu of taxes on income or profits, and taxes on its property ownership.

If any taxes are required to be withheld on payments invoiced by Microsoft, Customer may deduct such taxes from the amount owed and pay them to the appropriate taxing authority, but only if Customer promptly

provides Microsoft an official receipt for those withholdings and other documents reasonably requested to allow Microsoft to claim a foreign tax credit or refund. Customer will ensure that any taxes withheld are minimized to the extent possible under applicable law.

Term and termination

- a. **Term.** This Agreement is effective until the expiration date of the Government Contract unless terminated earlier as provided in FAR 52.212-4 sections (l) and (m).
- b. **Termination without cause (for the government's convenience).** IAW FAR 52.212-4(l), Customer may terminate this Agreement without cause without notice. Termination without cause will not affect Customer's perpetual licenses, and licenses granted on a subscription basis will continue for the duration of the subscription period(s), subject to the terms of this Agreement.
- c. **Termination for cause.** Without limiting other remedies it may have, Customer may terminate this Agreement IAW FAR 52.212-4(m). Upon such termination, the following will apply:
 - (1) All licenses granted under this Agreement will terminate immediately except for fully-paid, perpetual licenses.
 - (2) All amounts due under any unpaid invoices shall become due and payable immediately. For metered Products billed periodically based on usage, Customer must immediately pay for unpaid usage as of the termination date.

Customer will receive a credit for any subscription fees paid in advance for unused consumption for any usage period after the termination date.
- d. **Suspension.** Microsoft may temporarily suspend use of an Online Service without terminating this Agreement: (1) if it is reasonably needed to prevent unauthorized access to Customer Data; (2) if Microsoft believes such suspension is required to prevent harm. Unless Microsoft believes an immediate suspension is required, Microsoft will give Customer notice before suspending an Online Service (except Limited Offerings, which may be suspended without notice in all cases).

Professional Services

- a. **Description of Professional Services.** The precise scope of the Professional Services may be specified in a Statement of Services. Microsoft's ability to deliver the Professional Services depends upon Customer's full and timely cooperation, as well as the accuracy and completeness of any information Customer provides. This Agreement does not obligate either party to enter into any Statements of Services.
- b. **Proprietary Rights.**
 - (1) **Pre-existing Work.** Each party owns and retains all rights, title and interest to its preexisting Confidential Information and technology, including technologies developed outside of this agreement, together with all related intellectual property rights (as to each party, its "Pre-Existing Work"). Subject to compliance with the terms of this agreement, each party grants to the other a worldwide, non-exclusive, non-assignable, fully paid-up license to use, reproduce, and create derivative works of its Pre-existing Work, provided that: (i) Microsoft's license to Customer's Pre-Existing Work is solely for the purposes of providing technical resources under this agreement; (ii) Customer's license to Microsoft Pre-Existing Work will be in accordance with this agreement; (iii) neither party may use the other party's Pre-Existing Work on a standalone basis and (iv) neither party may distribute or otherwise transfer any of the other party's Pre-Existing Work to a third party.
 - (2) **Improvements.** Each party shall exclusively own all modifications and derivative works created under this agreement to that party's Pre-Existing Work ("Improvements"), regardless of who authors such Improvements. Each party assigns to the other party all rights, title, and interest to any Improvements that it makes to the other party's Pre-Existing work. Subject to compliance with the terms of this agreement, the parties license

Improvements as follows: (i) Microsoft grants Customer a worldwide, nonexclusive, non-assignable, fully paid-up license to use, reproduce, and create derivative works, but not distribute or otherwise transfer, Improvements to Microsoft's Pre-Existing Work; and (ii) Customer grants Microsoft a worldwide, non-exclusive, non-assignable, fully paid-up license to use, reproduce, distribute, and create derivative works of only those Improvements Microsoft may create to Customer's Pre-Existing Work that are generic solutions or services.

(3) Developments. Either party may create new technology, written materials, or proofs of concept under this agreement that do not include any Pre-Existing Work or Improvements ("Developments"). All Developments will be owned by Microsoft and Customer assigns to Microsoft all rights, title, and interest to any Developments that it makes. Microsoft grants Customer a worldwide, non-exclusive, non-assignable, fully paid-up license to use, reproduce, and create derivative works, but not distribute or otherwise transfer to a third party, Developments.

(4) Open Source. Microsoft may elect to release to Customer certain Improvements or Developments as open source software, published with related end user documentation to a public repository on GitHub or another mutually accepted venue, under the terms of the MIT License (<http://opensource.org/licenses/MIT>) or another mutually accepted open source license. The open source license, and not the terms above, will apply to such Improvements or Developments.

(5) Data. Customer owns all rights to data that Customer or its Affiliates may elect to share with Microsoft in Microsoft's performance of Professional Services. The data protection terms of the Microsoft Data Protection Addendum apply.

(6) Feedback. Either party may provide suggestions, comments, ideas, know-how, or other feedback to the other party. Feedback is voluntary and the receiving party is not required to hold it in confidence. The receiving party will not disclose the source of feedback without the providing party's consent. Feedback may be used for any purpose without obligation of any kind.

(7) Retained Rights. Except as expressly set forth in this agreement, neither party grants the other (by implication, estoppel or otherwise) any right, title, interest, or license, in such party's patents, patent applications, trade secrets, copyrights, mask work rights, trademarks or other intellectual property.

(8) Fixes. Each Fix is licensed under the same terms as the Product to which it applies. If the Fix is not provided for a specific Product, any use terms Microsoft provides with the Fix will apply. If no use terms are provided, Customer shall have a non-exclusive, perpetual, fully paid-up license to use and reproduce the Fix solely for its internal business purposes. Customer may not modify, change the file name or combine any Fix with any non-Microsoft computer code, except as expressly permitted in a licensing agreement.

(9) Services Deliverables. Except as may be otherwise explicitly set forth in a Statement of Services, upon payment in full, Microsoft will assign to Customer a non-exclusive, non-transferable, perpetual license to use, reproduce and modify any Services Deliverables for Customer's internal business purposes only, subject to the terms and conditions in this Agreement.

(10) Affiliates rights. Except as may be otherwise explicitly set forth in a Statement of Services, Customer may sublicense its rights to the Services Deliverables and Sample Code granted hereunder to its Affiliates, but the Affiliate(s) may not further sublicense these rights.

(11) Non-Microsoft software and technology. Customer is solely responsible for any non-Microsoft software or technology that Customer installs or uses with the Products, Fixes or Services Deliverables.

(12) Sample Code. Upon payment in full (if applicable), Microsoft grants Customer a non-exclusive, perpetual, non-transferable license to use and modify any Software code that Microsoft provides for purposes of illustration ("Sample Code") and to reproduce and distribute the object code form of the Sample Code for Customer's internal purposes only and not to any unaffiliated third party.

c. Compliance with applicable laws, privacy, and security.

(1) Customer consents to the processing of personal information by Microsoft and its agents to facilitate the subject matter of this Agreement. Customer will obtain all required consents from third parties (including

Customer's contact, resellers, distributors, administrators, and employees) under applicable privacy and data protection law before providing personal information to Microsoft.

- (2) Personal information collected through Professional Services (i) may be transferred, stored, and processed in the United States or any other country in which Microsoft or its contractors maintain facilities and (ii) will be subject to the privacy terms specified in the Use Rights. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use transfer, retention, and processing of Personal Data from the European Economic Area and Switzerland.

d. Miscellaneous.

- (1) **Insurance while performing Professional Services on Customer's premises.** Microsoft will maintain industry-appropriate insurance coverage at all times when performing Professional Services on Customer's premises under this Agreement via commercial insurance, self-insurance, or any other similar risk financing alternative. Microsoft will provide Customer with evidence of coverage on request.
- (2) **Cost or Pricing Data/Commercial items.** Microsoft will not, under any circumstances, accept work that would require the submission of cost or pricing data as defined by 48 CFR 15.4, or the submission of non-commercial items.
- (3) **Packaged Professional Services Pricing and Payment** Microsoft's Packaged Professional Services are a commercial item service provided on a firm fixed price (FFP) basis. Packaged Professional Services are priced per unit and will be invoiced as each unit is delivered.

Government Community Cloud Services.

- a. **Community requirements.** If Customer purchases Government Community Cloud Services, Customer certifies that it is a member of the Community and agrees to use Government Community Cloud Services solely in its capacity as a member of the Community and, for eligible Government Community Cloud Services, for the benefit of end users that are members of the Community. Use of Government Community Cloud Services by an entity that is not a member of the Community or to provide services to non-Community members is strictly prohibited and could result in termination of Customer's license(s) for Government Community Cloud Services without notice. Customer acknowledges that only Community members may use Government Community Cloud Services.
- b. All terms and conditions applicable to non-Government Community Cloud Services also apply to their corresponding Government Community Cloud Services, except as otherwise noted in the Use Rights. If any terms and conditions applicable to non-Government Community Cloud violates applicable Federal law, then, such terms shall not apply with respect to the Federal Government.
- c. Customer may not deploy or use Government Community Cloud Services and corresponding non-Government Community Cloud Services in the same domain.
- d. **Use Rights for Government Community Cloud Services.** For Government Community Cloud Services, notwithstanding anything to the contrary in the Use Rights:
 - (1) Government Community Cloud Services will be offered only within the United States.
 - (2) Terms regarding compliance with non-US law, such as GDPR, will not apply.
 - (3) References to geographic areas outside the United States for the location of Customer Data at rest do not apply.
 - (4) The compliance control standards and frameworks for Government Community Cloud Services are detailed in the applicable System Security Plan for each service and may differ from those applicable to commercial services (e.g., as set forth in the Data Protection Addendum).
- e. **Commercial Products.** Microsoft may make commercial products available to Customer to use with Customer's Government Community Cloud Services. Such Products will be provisioned in the public commercial cloud and all security controls and data commitments related to these services are described in the applicable Use Rights.

Azure Government Secret and O365 Government Secret Services.

- a. The following terms and conditions apply solely to Azure Government Secret and O365 Government Secret Services and shall take precedence over any conflicting terms in this agreement or any document incorporated herein.
- b. Customer certifies that all Customers using Azure Government Secret and O365 Government Secret Services have the authority to access classified systems at level of classification of the system being accessed.
- c. The existing Service Level Agreements ("SLAs") for Azure and O365 services apply to Azure Government Secret and O365 Government Secret, except that the SLAs are modified as follows:
 - (1) For the purpose of this section, "data centers" as they are referred to in the existing SLAs, shall include any Microsoft data centers, colocation data centers, or security operations centers (SOCs) that support the Azure Government Secret and O365 Government Secret Services provided under this Agreement.
 - (2) The SLA commitment does not apply to any unavailability, suspension, or termination of Services:
 - a. caused by any factor outside of Microsoft's reasonable control, including any force majeure event, which may include, but is not restricted to: limiting access to the facility by the Customer or a third party, limiting access to software, equipment or the space in which software or equipment are located in the facility by the Customer or a third party, limiting Internet access or network access, IP transit provider issues;
 - b. that results from any actions or inactions of the Customer or a third party, including but not limited to failure to process or deploy software patches through any government mandated vetting process or failure to meet agreed upon requirements for scaling of capacity;
 - c. that results from Customer equipment, software or other technology and/or third-party equipment, software or other technology (other than third party equipment within our direct control), encryption devices and related software;
 - d. that results from Microsoft dependencies on Customer or a third-party systems or any components thereof;
 - e. that results from any maintenance as provided for pursuant to any separate Agreement;
 - f. that result from Customer's failure to adhere to any other agreed upon policy or process documentation applicable to the environment;
 - g. that result from customer support issues that cannot be resolved through Microsoft's standard support channels available for Azure Government Secret and O365 Government Secret Services within the standard SLA period available for Azure Government Secret and O365 Government Secret services.

Miscellaneous.

- a. **Independent contractors.** The parties are independent contractors. Customer and Microsoft each may develop products independently without using the other's Confidential Information.
- b. **Agreement not exclusive.** Customer is free to enter into agreements to license, use, and promote the products and services of others.
- c. **No agency.** This Agreement does not create an agency, partnership, or joint venture.
- d. **U.S. export.** Products, Fixes, and Services Deliverables are subject to U.S. export jurisdiction. Customer must comply with all applicable international and national laws, including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end use and destination restrictions by U.S. and other governments related to Microsoft products, services, and technologies.
- e. **Severability.** If any part of this Agreement is held to be unenforceable, the rest of the Agreement will remain in full force and effect.
- f. **Waiver.** Failure to enforce any provision of this Agreement will not constitute a waiver. Any waiver must be in writing and signed by the waiving party.

- g. No third-party beneficiaries.** This Agreement does not create any third-party beneficiary rights except as expressly provided by its terms.
- h. Survival.** All provisions survive termination of this Agreement except those requiring performance only during the term of the Agreement.
- i. Notices.** All notices must be in writing. Except for Notices of Dispute or notices relating to arbitration, notices to Microsoft must be sent to the following address and will be deemed received on the date received at that address:
- Microsoft Corporation
Dept. 551, Volume Licensing
6880 Sierra Center Parkway,
Reno, Nevada 89511, USA
- Notices to Customer will be sent to the individual at the address Customer identifies on its account as its contact for notices. Microsoft may send notices and other information to Customer by email or other electronic form.
- j. Applicable law.** This Agreement will be governed by and construed in accordance with the Federal laws of the United States. The 1980 United Nations Convention on Contracts for the International Sale of Goods and its related instruments will not apply to this Agreement.
- k. Privacy and Compliance with applicable Laws, privacy and security.** Microsoft and Customer will each comply with all applicable laws and regulations (including applicable security breach notification law). However, Microsoft is not responsible for compliance with any laws applicable to Customer that are not also generally applicable to information technology services providers.
- l. Dispute.** Any breach of the Government Contract, including these General Terms, including Customer's obligations set forth herein, shall be handled in accordance with the Contracts Disputes Act (41 U.S.C. §§7101-7109) and FAR 52.233-1, Disputes.
- m. FAR 52.212-4 and GSAR 552.212-4.** If the Government Contract is subject to the Federal Acquisition Regulation, then these General Terms constitute the tailored version of FAR 52.212-4 and GSAR 552.212-4, as permitted by FAR 12.302 and 512.301(e).
- n. Order of precedence.** The Government Contract shall take precedence over these General Terms. Any inconsistencies shall be resolved by following the order of precedence in 552.212-4(s). These General Terms will take precedence over any conflicting terms in other documents that are incorporated into this Agreement that are not expressly resolved in those documents, except that conflicting terms in the Use Rights take precedence over these General Terms as to the applicable Products. Terms in an amendment control over the amended document and any prior amendments concerning the same subject matter.
- o. Microsoft Affiliates and contractors.** Microsoft may perform its obligations under this Agreement through its Affiliates and use contractors to provide certain services. Microsoft remains responsible for their performance.
- p. Government procurement rules.** By accepting this agreement, Customer represents and warrants that (i) it has complied and will comply with all applicable government procurement laws and regulations; (ii) it is authorized to enter into this Agreement; and (iii) this Agreement satisfies all applicable procurement requirements.
- q. Voluntary Product Accessibility Templates.** Microsoft supports the government's obligation to provide accessible technologies to its citizens with disabilities as required by Section 508 of the Rehabilitation Act of 1973, and its state law counterparts. The Voluntary Product Accessibility Templates ("VPATs") for Products and the Microsoft technologies used in providing the Online Services can be found at Microsoft's VPAT page. Further information regarding Microsoft's commitment to accessibility can be found at <https://www.microsoft.com/en-us/accessibility>.
- r.** If any document incorporated by reference into these General Terms, including the Use Rights and terms included and/or referenced or incorporated herein and/or therein, contains a provision (a) allowing for the automatic termination of Customer's license rights; (b) allowing for the automatic renewal of services and/or fees; (c) requiring the governing law to be anything other than Federal law; and/or (d) otherwise

violates applicable Federal law, then, such terms shall not apply with respect to Customer. If any document incorporated by reference into these General Terms, including the Use Rights and terms included and/or referenced or incorporated herein and/or therein contains an indemnification provision, such provision shall not apply as to the United States indemnifying Microsoft or any other party.

- s. **Section headings.** All section and subsection headings used in this agreement are for convenience only and shall not affect the interpretation of this agreement.
- t. **Azure Marketplace and AppSource.** Microsoft Azure enables Customer to access or purchase products and services which are optimized for use with Azure through the Microsoft Azure Marketplace and/or AppSource (together the "Marketplace"). All transactions through the Marketplace are between the Customer and the Publisher of the individual products or services available in the Marketplace. Customer is responsible for ensuring all products and services acquired through the Marketplace meet Customer's technical and security requirements. Please see the Use Rights for more information.

Definitions.

"Administrator Data" means the information provided to Microsoft or its Affiliates during signup, purchase, or administration of Products.

"Affiliate" means (i) with regard to Government, any other agency, office, bureau, department, or other entity of the United States Government that are allowed to utilize this Agreement. and (ii) with regard to Microsoft, any legal entity that Microsoft controls, which controls Microsoft, or which is under common control with Microsoft. "Control" means, for purposes of this definition, ownership of more than a 50% interest of voting securities in an entity or the power to direct the management and policies of an entity.

"Azure Government Services" means one or more of the services or features Microsoft makes available to Customer under this Agreement and identified at <http://azure.microsoft.com/en-us/regions/#services>, which are Government Community Cloud Services.

"Azure Government Secret and O365 Government Secret Services" means one or more of the services or features Microsoft makes available to Customer in the Azure Government Secret and O365 Government Secret environment under this Agreement. The full catalog of Azure and O365 Government Secret Services will be listed in the customer portals for the Azure Government Secret cloud and the O365 Government Secret cloud or at some other location specified by Microsoft.

"Community" means the community consisting of one or more of the following: (1) a Government, (2) a Customer using eligible Government Community Cloud Services to provide solutions to a Government or a qualified member of the Community, or (3) a Customer with Customer Data that is subject to Government regulations for which the Customer determines and Microsoft agrees that the use of Government Community Cloud Services is appropriate to meet the Customer's regulatory requirements. Membership in the Community is ultimately at Microsoft's discretion, which may vary by Government Community Cloud Service.

"Control" means ownership of more than a 50% interest of voting securities in an entity or the power to direct the management and policies of an entity.

"Confidential Information" is defined in the "Confidentiality" section.

"Customer" means the entity identified as such on the account associated with this Agreement.

"Customer Data" means all data, including all text, sound, software, image or video files that are provided to Microsoft or its Affiliates by, or on behalf of, Customer and its Affiliates through use of Online Services. Customer Data does not include Support and Consulting Data.

"day" means a calendar day, except references that specify "business day".

"End User" means any person Customer permits to use a Product or access Customer Data.

"Federal Agency" means a bureau, office, agency, department or other entity of the United States Government.

"Fixes" means Product fixes, modifications or enhancements or their derivatives that Microsoft releases generally (such as Product service packs), or provides to Customer to address a specific issue.

"Government" means a Federal Agency, State/Local Entity, or Tribal Entity acting in its governmental capacity.

"Government Community Cloud Services" means Microsoft Online Services that are provisioned in Microsoft's multi-tenant data centers for exclusive use by or for the Community and offered in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-145. Microsoft Online Services that are Government Community Cloud Services are designated as such in the Use Rights and Product Terms.

"Government Contract" means the agreement between Customer and Microsoft which incorporates these General Terms.

"License" means Customer's right to use the quantity of a Product ordered. For certain Products, a License may be available on a subscription basis ("Subscription License"). Licenses for Online Services will be considered Subscription Licenses under these Additional Use Right and Restrictions.

"Licensing Site" means <http://www.microsoft.com/licensing/contracts> or a successor site.

"Microsoft" means Microsoft Corporation.

"Non-Microsoft Product" means any third-party-branded software, data, service, website or product, unless incorporated by Microsoft in a Product.

"Office 365 Service Descriptions" means the Service Descriptions for Office 365 GCC High, published by Microsoft at <https://technet.microsoft.com/en-us/library/mt774581.aspx> (for the product superset, Office 365 US Government) and <https://technet.microsoft.com/enus/library/mt774968.aspx> (for the product subset, Office 365 GCC High), or at successor sites Microsoft later identifies.

"Office 365 US Government" means the Government Community Cloud Service described by the Office 365 Service Descriptions, and purchased by Customer pursuant to the terms and conditions of the Agreement.

"Office 365 GCC High" means the Government Community Cloud Service described by the Office 365 Service Descriptions, and purchased by Customer pursuant to the terms and conditions of the Agreement.

"Online Services" means Microsoft-hosted services to which Customer subscribes under this Agreement. It does not include software and services provided under separate license terms.

"Online Services Benefits" means those Professional Services, made available to eligible customers at no additional charge as part of an Online Services subscription to advise and assist with onboarding, migration, training and use of those Online Services. Additional terms and conditions may be required to receive some Online Services Benefits. Eligibility will be determined on a per-service basis and may vary depending on availability. Microsoft reserves the right to change the availability of Online Service Benefits at any time in its sole discretion.

"Packaged Professional Services" means cloud training, advisory, and assistance services that Microsoft provides on a firm fixed unit price basis.

"Personal Data" means any information relating to an identified or identifiable natural person.

"Pre-Existing Work" means computer code or other written materials developed or otherwise obtained independently of the efforts of a party under this Agreement.

"Product" means all Software and Online Services identified in the Product Terms that Microsoft offers under this Agreement, including previews, prerelease versions, updates, patches and bug fixes from Microsoft. Product availability may vary by region. "Product" does not include Non-Microsoft Products.

"Product Terms" means the document that provides information about Products available under this Agreement. The Product Terms document is published on the Licensing Site and is updated from time to time.

“Professional Services” means all Product support services and Microsoft research or engineering services, training, advice, consulting or other services provided as an Online Services Benefit or Packaged Professional Service to assist with onboarding, migration, training and use of Online Services or otherwise related to any Online Service. The precise scope of the Professional Services may be specified in a Statement of Services.

“Publisher” means a provider of a Non-Microsoft Product.

“Representatives” means a party’s employees, Affiliates, contractors, advisors and consultants. “SLA” means Service Level Agreement, which specifies the minimum service level for the Online Services and is published on the Licensing Site.

“Services Deliverables” means any computer code or materials, other than Products or Fixes that Microsoft leave with Customer at the conclusion of Microsoft’s performance of services.

“Software” means licensed copies of Microsoft software identified in the Product Terms. Software does not include Online Services, but Software may be part of an Online Service.

“Statement of Services” means any statement of work, performance work statement, or other description of Professional Services issued into or under a Government Contract that incorporates this Agreement.

“Support and Consulting Data” means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by, or on behalf of, Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Professional Services covered under this Agreement. Support and Consulting Data may include Personal Data.

“Trade Secret” means information that is not generally known or readily ascertainable to the public, has economic value as a result, and has been subject to reasonable steps under the circumstances to maintain its secrecy.

“Tribal Entity” means a federally-recognized tribal entity performing tribal governmental functions and eligible for funding and services from the U.S. Department of Interior by virtue of its status as an Indian tribe.

“use” means to copy, download, install, run, access, display, use or otherwise interact with.

“Use Rights” means the license terms and terms of service for each Product published on the Licensing Site and updated from time to time. The Use Rights include the Product-Specific License Terms, the License Model terms, the Universal License Terms, the Data Protection Terms, and the Other Legal Terms. The Use Rights supersede the terms of any end user license agreement that accompanies a Product.

2. GSA Schedule Addendum

Notwithstanding anything else contained in the Microsoft Customer Agreement, the following terms and conditions shall apply to the Software and Online Services provided under the GSA Schedule. Microsoft agrees that, in the event of any conflict or inconsistency between the terms in this Addendum and other terms within the Use Rights, the terms of this Addendum will supersede and be controlling.

- 1) Commercial supplier agreements unenforceable clauses – All terms are subject to GSAR 552.212-4 (FAR Deviation).
- 2) Amendments: Any amendment to this Agreement must be executed by both parties, except that Microsoft may change the Use Rights and Product Terms from time to time, provided that:
 - a. Updates to terms are made available on the Licensing Site; and
 - b. Any term unilaterally revised subsequent to award that is inconsistent with any material term or provision of the Agreement is not enforceable against the Government. Terms included by reference using electronic means (e.g. via web links, click and accept, etc.) shall be enforceable only to the extent that:
 - (1) When included by reference using electronic means, the terms are readily available at the referenced locations; and
 - (2) Terms do not materially change Government obligations; and
 - (3) Terms do not decrease overall level of services; and
 - (4) Terms do not limit any other Government right addressed elsewhere in the Agreement.

3. Use Rights

Microsoft Use Rights are included as Attachment 1.

Attachment 1 – Use Rights

Publication Date: June 01, 2022

Program: MCA

Table of Contents

INTRODUCTION	3
ABOUT THIS DOCUMENT	3
UNIVERSAL LICENSE TERMS	4
FOR ONLINE SERVICES	4
FOR ALL SOFTWARE	8
PRIVACY & SECURITY TERMS	12
WINDOWS DESKTOP OPERATING SYSTEM	15

MICROSOFT AZURE	22
MICROSOFT POWER PLATFORM	40
GLOSSARY	44
CAL AND ML EQUIVALENCY LICENSES	51
NOTICES	56
PROGRAM AGREEMENT SUPPLEMENTAL TERMS	57
STORAGE ARRAY, AZURE DATA BOX, AZURE STACK EDGE, AND AZURE STACK HUB RUGGEDIZED TERMS	57

Introduction

About this Document

This copy of the Use Rights has been downloaded from <https://www.microsoft.com/licensing/terms> for the date and program indicated on the title page and based on the selected products or configurations.

The terms formerly contained in the "Online Services Terms" have been moved into the "Product Terms" and no longer exist as standalone terms. The unified Product Terms are incorporated by reference into agreements governing Customer's use of Microsoft Products and Professional Services.

Access to versions of the Product Terms and Online Services Terms published prior to February 2021 are available [here](#). Updates that Microsoft makes from time to time to Use Rights apply to Customer as set forth in Customer's agreement.

IF ANY DOCUMENT INCLUDED AND/OR REFERENCED, OR INCORPORATED BY REFERENCE INTO THESE "ATTACHMENT 1 - USE RIGHTS" CONTAINS A PROVISION REQUIRING THE GOVERNING LAW TO BE ANYTHING OTHER THAN THE FEDERAL LAW OF THE UNITED STATES; AND/OR OTHERWISE VIOLATES THE APPLICABLE FEDERAL LAW OF THE UNITED STATES, INCLUDING, BUT NOT LIMITED TO GSAR 552.212-4(w), THEN, SUCH TERMS SHALL NOT APPLY WITH RESPECT TO THE FEDERAL GOVERNMENT. ALL PRICES AND PRICING MODELS IN THESE USE RIGHTS SHALL BE IN ACCORDANCE WITH THE GSA SCHEDULE CONTRACT AND GSA SCHEDULE PRICELIST AND TO THE EXTENT THAT PRICES REFERENCED IN THESE USE RIGHTS ARE INCONSISTENT WITH THE GSA SCHEDULE CONTRACT AND GSA SCHEDULE PRICELIST THEN THE GSA SCHEDULE CONTRACT AND GSA SCHEDULE PRICELIST SHALL SUPERSEDE PRICES REFERENCED IN THESE USE RIGHTS.

Universal License Terms

For Online Services

Definitions

Terms used here but not defined in the [Glossary](#) will have the definitions provided in Customer's licensing agreement.

Data Processing and Security

The parties agree that these terms govern Customer's use of the Online Services and that the [DPA](#) (defined in the [Glossary](#)) sets forth their obligations with respect to the processing and security of [Customer Data](#) and [Personal Data](#) by the Online Services. The parties also agree that, unless a separate Professional Services agreement exists, these terms govern the provision of Professional Services, including but not limited to the terms in the [Professional Services](#) section and terms in the [DPA](#) for the processing and security of Professional Services Data and [Personal Data](#) in connection with that provision. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products (as defined below). In the event of any conflict or inconsistency between the [DPA](#) and any other terms in Customer's licensing agreement (including these terms), the DPA shall prevail.

Service Level Agreements

Many Online Services offer a Service Level Agreement (SLA). For more information regarding the Online Services SLAs, please refer to <https://www.microsoft.com/licensing/product-licensing/products>.

Applicable Product Terms and Updates for Online Services

When Customer renews or purchases a new subscription to an Online Service, the then-current terms will apply and will not change during Customer's subscription for that Online Service. When Microsoft introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), Microsoft may provide terms or make updates to the terms that apply to Customer's use of those new features, supplements or related software.

Electronic Notices

Microsoft may provide Customer with information and notices about Online Services electronically, including via email, through the portal for the Online Service, or through a web site that Microsoft identifies. Notice is given as of the date it is made available by Microsoft.

Licensing the Online Services

Customer must acquire and assign the appropriate subscription licenses required for its use of each Online Service. Each user that accesses the Online Service must be assigned a User SL or access the Online Service only through a device that has been assigned a Device SL, unless specified otherwise in the Online Service-specific Terms. [Subscription License Suites](#) describes SL Suites that also fulfill requirements for User SLs. Customer has no right to use an Online Service after the SL for that Online Service ends.

License Reassignment

Most, but not all, SLs may be reassigned. Except as permitted in this paragraph or in the Online Service-specific Terms, Customer may not reassign an SL on a short-term basis (i.e., within 90 days of the last assignment). Customer may reassign an SL on a short-term basis to cover a user's absence or the unavailability of a device that is out of service. Reassignment of an SL for any other purpose must be for the remaining term of that License. When Customer reassigns an SL from one device or user to another, Customer must block access and remove any related software from the former device or from the former user's device.

Multiplexing

Hardware or software that a Customer uses to:

- pool connections or reduce the number of [OSE's](#), devices, or users a Product directly manages;
- reduce the number of devices or users that directly or indirectly access or use a Product;

- or access data a Product itself processes or generates;

does not reduce the number of Licenses of any type that Customer needs.

Online Services Step-up Availability and License Assignment

Some licensing programs allow customers to step-up an existing online service to a higher edition any time during the agreement and enrollment (if any) term. Such higher edition licenses may be acquired using Step-up SKUs with the following requirements:

- A higher edition license acquired using a Step-up SKU can only be assigned to a licensed user of a qualifying base license of the same online service or a suite license that includes the same qualifying base online service,
- Once the higher edition license is acquired, customers may not separate it from the qualifying base online service license,
- Step up SKUs must be purchased under the same licensing agreement and enrollment (if any), under which the qualifying base online service User SL was acquired.

Using the Online Services

Customer may use the Online Services and related software as expressly permitted in Customer's licensing agreement. Microsoft reserves all other rights.

Acceptable Use Policy

Neither Customer, nor those that access an Online Service through Customer, may use an Online Service:

- in a way prohibited by law, regulation, governmental order or decree;
- to violate the rights of others;
- to try to gain unauthorized access to or disrupt any service, device, data, account or network;
- to spam or distribute malware;
- in a way that could harm the Online Service or impair anyone else's use of it;
- in any application or situation where failure of the Online Service could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage, except in accordance with the High-Risk Use section below; or
- to assist or encourage anyone to do any of the above.

Violation of the Acceptable Use Policy in this section may result in temporary suspension of the Online Service. If Microsoft suspends the Online Service, Microsoft will suspend only to the extent reasonably necessary. Unless Microsoft believes an immediate suspension is required, Microsoft will provide reasonable notice before suspending an Online Service for the reasons stated above.

High-Risk Use

WARNING: Modern technologies, and especially platform technologies, may be used in new and innovative ways, and Customer must consider whether its specific use of these technologies is safe. The Online Services are not designed or intended to support any use in which a service interruption, defect, error, or other failure of an Online Service could result in the death or serious bodily injury of any person or in physical or environmental damage (collectively, "High-Risk Use"). Accordingly, Customer must design and implement every application such that, in the event of any interruption, defect, error, or other failure of the Online Service, the safety of people, property, and the environment are not reduced below a level that is reasonable, appropriate, and legal, whether in general or for a specific industry. Customer's High-Risk Use of the Online Services is at its own risk. Microsoft shall have no responsibility for any damages or costs associated with a High Risk Use of the Online Services. Customer shall be responsible for any damages or costs associated with a High Risk Use of Online Services.

Medical Device Disclaimer

Customer acknowledges that the Online Services (1) are not designed, intended or made available as a medical device(s), and (2) are not designed or intended to be a substitute for professional medical advice, diagnosis, treatment, or judgment and should not be used to replace or as a substitute for professional medical advice, diagnosis, treatment, or judgment. Customer is solely responsible for displaying and/or obtaining appropriate consents, warnings, disclaimers, and acknowledgements to end users of Customer's implementation of the Online Services.

Data Protection and Security

Microsoft Product Terms (English, Jun 01 2022, MCA)

6

The terms of the [DPA \(http://aka.ms/DPA\)](http://aka.ms/DPA) apply to Online Services except for Online Services listed in the [Privacy & Security Terms](#). For Core Online Services, Online Service-specific details on security practices and location of [Customer Data](#) at rest are also located in the [Privacy & Security Terms](#).

Use of Software with the Online Service

Customer may need to install certain Microsoft software to use the Online Service. If so, the following terms apply:

Microsoft Software License Terms

Customer may install and use the software only for use with the Online Service. The Online Service-specific Terms may limit the number of copies of the software Customer may use or the number of devices on which Customer may use it. Customer's right to use the software begins when the Online Service is activated and ends when Customer's right to use the Online Service ends. Customer must uninstall the software when Customer's right to use it ends. Microsoft may disable it at that time.

Validation, Automatic Updates, and Collection for Software

Microsoft may automatically check the version of any of its software. Devices on which the software is installed may periodically provide information to enable Microsoft to verify that the software is properly licensed. This information includes the software version, the end user's user account, product ID information, a machine ID, and the internet protocol address of the device. If the software is not properly licensed, its functionality will be affected. Customer may only obtain updates or upgrades for the software from Microsoft or authorized sources. By using the software, Customer consents to the transmission of the information described in this section. Microsoft may recommend or download to Customer's devices updates or supplements to this software, with or without notice. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications) ("Apps"). The Apps may collect diagnostic data (as defined in the Product Documentation) about the use and performance of the Apps, which may be transmitted to Microsoft, to the extent any [Personal Data](#) is contained therein, and used for the purposes described in the [DPA](#).

Third-party Software Components

The software may contain third party software components. Unless otherwise disclosed in that software, Microsoft, not the third party, licenses these components to Customer under Microsoft's license terms and notices.

Reserved

Technical Limitations

Customer must comply with, and may not work around, any technical limitations in an Online Service that only allow Customer to use it in certain ways. Customer may not download or otherwise remove copies of software or source code from an Online Service except as explicitly authorized.

Import/Export Services

Customer's use of any Import/Export Service is conditioned upon its compliance with all instructions provided by Microsoft regarding the preparation, treatment and shipment of physical media containing its data ("storage media"). Customer is solely responsible for ensuring the storage media and data are provided in compliance with all laws and regulations. Microsoft has no duty with respect to the storage media and no liability for lost, damaged or destroyed storage media. All storage media shipped to Microsoft must be shipped DAP Microsoft DCS Data Center (INCOTERMS 2010). Storage media shipped to Customer will be shipped DAP Customer Dock (INCOTERMS 2010).

Font Components

While Customer uses an Online Service, Customer may use the fonts installed by that Online Service to display and print content. Customer may only embed fonts in content as permitted by the embedding restrictions in the fonts and temporarily download them to a printer or other output device to print content.

Changes to and Availability of the Online Services

Microsoft may make commercially reasonable changes to each Online Service from time to time. Microsoft may modify or terminate an Online Service in any country where Microsoft is subject to a government regulation, obligation or other requirement that (1) is not generally applicable to businesses operating there, (2) presents a hardship for Microsoft to continue operating the Online Service without modification, and/or (3) causes Microsoft to believe these terms or the Online Service may conflict with any such requirement or obligation. If Microsoft terminates an Online Service for regulatory reasons, Customers will receive a credit for any amount paid in advance for the period after termination.

Availability, functionality, and language versions for each Online Service may vary by country. For information on availability, Customer may refer to <https://go.microsoft.com/fwlink/?linkid=870295>.

Dataverse

Dataverse structures a variety of data and business logic to support interconnected applications and processes. Dataverse Instances provided with Microsoft 365 licenses includes various features and integrates data that may or may not be available for the product or service Customer is licensed with. Access to Dataverse, through an individual product or service, does not grant access to unrelated products, services, features, or data that users are not licensed for. Users only have rights to access data, services, and features within Dataverse for which they are properly licensed for.

Other

Non-Microsoft Products

Microsoft may make Non-Microsoft Products available to Customer through Customer's use of the Online Services (such as through a store or gallery, or as search results) or a Microsoft online store (such as the Microsoft Store for Business or Microsoft Store for Education). If Customer installs or uses any Non-Microsoft Product with an Online Service, Customer may not do so in any way that would subject Microsoft's intellectual property or technology to obligations beyond those expressly included in Customer's licensing agreement. For Customer's convenience, Microsoft may include charges for certain Non-Microsoft Product as part of Customer's bill for Online Services. Microsoft, however, assumes no responsibility or liability whatsoever for any Non-Microsoft Product. Customer is solely responsible for any Non-Microsoft Product that it installs or uses with an Online Service or acquires or manages through a Microsoft online store. Customer's use of any Non-Microsoft Product shall be governed by the license, service, and/or privacy terms between Customer and the publisher of the Non-Microsoft Product (if any).

Previews

PREVIEWS ARE PROVIDED "AS-IS," "WITH ALL FAULTS," AND "AS AVAILABLE," as described herein. Unless otherwise noted in a separate agreement, Previews are not included in the SLA for the corresponding Online Service, and may not be covered by customer support. We may change or discontinue Previews at any time without notice. We may also choose not to make a Preview service generally commercially available.

Providing "Feedback" (suggestions, comments, feedback, ideas, or know-how, in any form) to Microsoft about Preview services is voluntary. Microsoft is under no obligation to post or use any Feedback. By providing Feedback to Microsoft, Customer (and anyone providing Feedback through Customer) irrevocably and perpetually grant to Microsoft and its Affiliates, under all of its (and their) owned or controlled intellectual property rights, a worldwide, non-exclusive, fully paid-up, royalty-free, transferable, sub-licensable right and license to make, use, reproduce, prepare derivative works based upon, distribute, publicly perform, publicly display, transmit, and otherwise commercialize the Feedback (including by combining or interfacing products, services or technologies that depend on or incorporate Feedback with other products, services or technologies of Microsoft or others), without attribution in any way and for any purpose.

Customer warrants that 1) it will not provide Feedback that is subject to a license requiring Microsoft to license anything to third parties because Microsoft exercises any of the above rights in Customer's Feedback; and 2) it owns or otherwise controls all of the rights to such Feedback and that no such Feedback is subject to any third-party rights (including any personality or publicity rights).

Azure Active Directory, Free Edition

As described in <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is>, most Online Services include an instance of Azure Active Directory, a cloud-based user authentication capability ("Azure AD Free"). After Customer configures and uses the first such Online Service, that instance of Azure AD Free, as configured by Customer for its users, may power the user authentication features for each later-acquired subscription of an Online Service.

Customer's instance of Azure AD Free will also enable authenticated users to interact with Microsoft or a third party in contexts outside of the Online Services ("Other AD-dependent Services"), specifically where Microsoft or that third party requires an Azure Active Directory user account. With respect to the operation of Azure AD Free for Other AD-dependent Services, Microsoft remains a data processor, and this use of Azure AD Free constitutes Customer's authoritative instruction to Microsoft that such use is permitted. With respect to the operation of the Other AD-dependent Service, refer to its applicable agreement and privacy policy to determine the role of the provider of the Other AD-dependent Service.

Competitive Benchmarking

If Customer offers a service competitive to an Online Service, by using the Online Service, Customer agrees to waive any restrictions on competitive use and benchmark testing in the terms governing its competitive service. If Customer does not intend to waive such restrictions in its terms of use, Customer is not allowed to use the Online Service.

Government Customers

If Customer is a government entity, then the following terms apply to any Online Service provided at no charge to Customer:

1. Microsoft waives any and all entitlement to compensation from Customer for the Online Service.
2. In compliance with applicable laws and regulations, Microsoft and Customer acknowledge that the Online Services are for the sole benefit and use of Customer and not provided for the personal use or benefit of any individual government employee.

Waiver of end-user consumer protection provisions

Customer agrees to waive any and all entitlements that would otherwise be applicable under the European Electronic Communications Code (Directive 2018/1972) Article 102 paragraphs 1, 3, and 5; Article 105 paragraph 1; and Article 107 paragraphs 1 and 3.

Online Services Regional Availability

Visit <https://www.microsoft.com/en-us/microsoft-365/business/international-availability> for a list of countries and regions in which the Online Services are available.

Online Services Purchasing Rules

The following purchasing rules apply to purchasing Online Services:

- Subscription terms vary by purchasing program. Under the Enterprise Agreement program, the subscription terms for Online Services other than Microsoft Azure must be coterminous, ending on the date of Customer's Enrollment end date.
- If Customer makes additional purchases of an Online Service, the end of the subscription term of the additional purchase must align with Customer's existing subscription term for the same Online Service. This provision does not apply to Azure reservations.
- Customer may not reduce the number of users or devices covered by its Online Services subscription during the term of their Online Services subscription except as permitted in Customer's licensing agreement.
- Add-on and Step-up User SLs must be purchased under the same licensing agreement as their Qualifying License or base User SL. Add-ons expire upon the earlier of the expiration of the SA coverage for the Qualifying License or the Add-on User SL. Step-ups expire upon the earlier of the expiration of the Step-up User SL or base User SL.
- User SLs are priced monthly.

Online Services Renewal

Online services subscriptions for government and academic customers will not be automatically renewed unless there is an active funded order and Customer chooses the auto-renewal option, and executes a written order for the renewal period of the Online Services.

For all Software

Universal License Terms

Universal License Terms apply to all [software Products](#) licensed through Microsoft Volume Licensing (except where specifically noted in the License Model Terms and/or the Product-Specific License Terms).

Definitions

Terms used in the Product Terms but not defined in the [Glossary](#) will have the definition provided in Customer's volume licensing agreement.

Customer's Use Rights

If Customer complies with its volume licensing agreement, it may use the software as expressly permitted in the Product Terms. Customer needs a [License](#) for each Product and separately licensed functionality used on a device or by a user.

Rights to Use Other Versions and Lower Editions

For any permitted copy or [Instance](#), Customer may create, store, install, run or access in place of the version licensed, a copy or [Instance](#) of a prior version, different permitted language version, different available platform version (for example, 32 bit or 64 bit) or a permitted lower edition. The use rights for the licensed version still apply. [Licenses](#) for prior versions and lower editions do not satisfy the licensing requirements for a Product.

Third Party Software

The software may contain third party proprietary or open source programs or components that are licensed under separate terms that are presented to Customer during installation or in the "ThirdPartyNotices" file accompanying the software. The software may also contain third party open source programs that Microsoft, not the third party, licenses to Customer under Microsoft's license terms.

Pre-Release Code, Updates or Supplements, Additional Functionality

Microsoft may offer updates or supplements to the Products. Customer may use the updates or supplements to the Products, pre-release code, additional functionality and optional add-on services to the Products, subject to specific terms (if any) that accompany them. Some Products require automatic updates, as described in the Product-Specific License Terms.

Restrictions

Customer may not (and is not licensed to) use the Products to offer commercial hosting services to third parties, work around any technical limitations in the Products or restrictions in Product documentation, or separate the software for use in more than one [OSE](#) under a single License (even if the [OSEs](#) are on the same physical hardware system), unless expressly permitted by Microsoft. Rights to access the software on any device do not give Customer any right to implement Microsoft patents or other Microsoft intellectual property in the device itself or in any other software or devices.

Software Assurance

SA coverage may grant additional use rights to Customer. These additional rights end at the expiration of the SA coverage for the [License](#), unless otherwise noted in the benefit description.

Outsourcing Software Management

Customer may install and use licensed copies of the software on [Servers](#) and other devices that are under the day-to-day management and control of [Authorized Outsourcers](#), provided all such Servers and other devices are and remain fully dedicated to Customer's use. Customer is responsible for all of the obligations under its volume licensing agreement regardless of the physical location of the hardware upon which the software is used. Except as expressly permitted here or elsewhere in these Product Terms, Customer is not permitted to install or use licensed copies of the software on [Servers](#) and other devices that are under the management or control of a third party.

License Assignment and Reassignment

Before Customer uses software under a License, it must assign that License to a device or user, as appropriate. Customer may reassign a License to another device or user, but not less than 90 days since the last reassignment of that same License, unless the reassignment is due to (i) permanent hardware failure or loss, (ii) termination of the user's employment or contract or (iii) temporary reallocation of CALs, Client Management Licenses and user or device SLs to cover a user's absence or the unavailability of a device that is out of service. Customer must remove the software or block access from the former device or to the former user. SA coverage and any Licenses that are granted or acquired in connection with SA coverage may be reassigned only with the underlying qualifying License. Additional terms apply to the reassignment of Windows desktop operating system per device licenses, as detailed in the Windows Product Entry.

Technical Measures

Microsoft may use technical measures to enforce terms that restrict Customer's use of certain versions of Product and may verify compliance with those terms as provided in Customer's volume license agreement. Some Products are protected by technological measures and require activation or validation, as well as a product key, to install or access them.

Activation and validation

Customer shall use the appropriate product key provided by Microsoft for activation and validation of the software Product being installed by the Customer. Customer's right to use the software after the time specified in the software Product may be limited unless it is activated. Customer is not licensed to continue using the software if it has unsuccessfully attempted to activate. Each device that has not activated by a Key Management Service (KMS) must use a Multiple Activation Key (MAK) or Azure AD-based Activation. Customer may not circumvent activation or validation.

Product Keys

An assigned product key is required for licensed use of the software. All product keys are Confidential Information of Microsoft. Notwithstanding anything to the contrary in Customer's volume licensing agreement, Customer may not disclose product keys to third parties. Customer may not provide unsecured access to its key management service (KMS) machines over an uncontrolled network. In the event of unauthorized use or disclosure of product keys or KMS keys, Microsoft may prevent further activations, deactivate or block product keys from activation or validation, and take other appropriate action.

Notices

Where indicated in the Use Rights section of each Product Entry, the following notices apply:

Internet-based Features

Software Products may contain features that connect and send information over the Internet, without additional notice to Customer, to Microsoft's systems and those of its Affiliates and service providers. Use of that information is described in the terms accompanying the internet-based features, Product documentation, and Microsoft Privacy Statement (aka.ms/privacy). Unless stated otherwise, Microsoft is a controller of Personal Data processed in connection with Customer's use of Internet-based features in software Products. When Microsoft is a controller for Internet-based features, Microsoft will handle the Personal Data in accordance with the Microsoft Privacy Statement (aka.ms/privacy), and the Data Protection Addendum terms do not apply.

Bing Maps

The Product may include use of Bing Maps. Any content provided through Bing Maps, including geocodes, can only be used within the product through which the content is provided. Customer's use of Bing Maps is governed by the Bing Maps End User Terms of Use available at <http://go.microsoft.com/?linkid=9710837> and the Microsoft Privacy Statement available at <http://go.microsoft.com/fwlink/?LinkID=248686>.

H.264/AVC Visual Standard, the VC-1 Video Standard, and the MPEG-4 Part 2 Visual Standard

This software may include H.264/AVC, VC-1, and MPEG-4 Part 2 visual compression technology. MPEG LA, L.L.C. requires this notice: THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1, THE MPEG-4 PART 2 VISUAL PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE ("VIDEO STANDARDS") AND/OR (ii) DECODE AVC, VC-1, MPEG-4 PART 2 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE www.mpegla.com. For clarification purposes, this notice does not limit or inhibit the use of the software for normal

business uses that are personal to that business which do not include (i) redistribution of the software to third parties, or (ii) creation of content with the VIDEO STANDARDS compliant technologies for distribution to third parties.

Malware protection

Microsoft cares about protecting customers' devices from malware. The software will turn on malware protection if other protection is not installed or has expired. To do so, other antimalware software will be disabled or may have to be removed.

Font Components, Images, and Sounds

While Customer runs the software, it may access and use icons, images, sounds and media included with the software only from a Licensed Device and may use the fonts included with or installed by that software to display and print content. Customer may only embed fonts in content as permitted by the embedding restrictions in the fonts; and temporarily download them to a printer or other output device to print content.

Included Technologies

Products may include other Microsoft technology components subject to their own license terms, as indicated in the Use Rights section of each Product Entry. If separate terms for these components are not addressed in the Product-Specific License Terms, they may be found in a separate folder in the Product's installation directory or through the Product's unified installer.

Benchmark Testing

Customer must obtain Microsoft's prior written approval to disclose to a third party the results of any benchmark test of any Server Product or Microsoft Desktop Optimization Pack.

Multiplexing

Hardware or software that a Customer uses to:

- pool connections or reduce the number of OSE's, devices, or users a Product directly manages;
- reduce the number of devices or users that directly or indirectly access or use a Product;
- or access data a Product itself processes or generates;

does not reduce the number of Licenses of any type that a customer needs.

Administrative and Support Rights

Customer may allow access to server software running in any permitted OSE by two users without CALs solely for administrative purposes. Customer may also allow remote access to other Products solely for purposes of providing technical product support to Licensed Users or on Licensed Devices.

Distributable Code

Refer to the Product Entries for software that contains code and text files Customer is permitted to distribute "Distributable Code". The code and text files listed below are also Distributable Code that may be used as described below. In the case of a conflict between the following terms and Distributable Code terms published in the Product Entry, the terms in the Product Entry govern Customer's use of Distributable Code.

Right to Use and Distribute

The code and text files listed below are "Distributable Code."

- REDIST.TXT Files: Customer may copy and distribute the object code form of code listed in REDIST.TXT files and in OTHER-DIST.TXT files, as well as any code marked as "Silverlight Libraries", Silverlight "Client Libraries" and Silverlight "Server Libraries".
- Sample Code, Templates, and Styles: Customer may modify, copy, and distribute the source and object code form of code marked as "sample", "template", "simple styles" and "sketch styles."
- Third Party Distribution: Customer may permit distributors of its programs to copy and distribute the Distributable Code as part of those programs.

- Image Library: Customer may copy and distribute images, graphics and animations in the Image Library as described in the software documentation.

Distribution Requirements

If Customer distributes any Distributable Code. Customer must:

- Only distribute it with Customer's programs, where Customer's programs provide significant primary functionality to the Distributable Code;
- require distributors and external end users to agree to terms that protect the Distributable Code at least as much as Customer's volume licensing agreement, including the Product Terms;
- indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of Customer's programs, except to the extent that any claim is based solely on the Distributable Code included in Customer's programs.

Distribution Limitations

Customer may not:

- alter any copyright, trademark or patent notice in the Distributable Code;
- use Microsoft's trademarks in Customer's programs' names or in a way that suggests its programs come from or are endorsed by Microsoft;
- distribute Distributable Code in or with any malicious or, deceptive programs or in an unlawful manner; or
- modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that the code be disclosed or distributed in source code form, or that others have the right to modify it.

Software Plus Services

Microsoft may provide services with Products through software features that connect with Microsoft or service provider computer systems over the Internet. It may change or cancel the services at any time. Customer may not use the services in any way that could harm them or impair anyone else's use of them. Customer may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

Processing of Personal Data; GDPR

To the extent Microsoft is a processor or subprocessor of Personal Data in connection with a software Product, Microsoft makes the commitments in the Data Protection Addendum, including for any processing for business operations incident to providing the software Product. When Microsoft is a controller, Microsoft will handle Personal Data in accordance with the Product documentation and Microsoft Privacy Statement (aka.ms/privacy), and the Data Protection Addendum terms do not apply. Please see the Product documentation for details on any processing of Personal Data in connection with software Products and Customer's configuration options.

Privacy & Security Terms

The Privacy & Security Terms were formerly contained in Attachment 1 to the Online Services Terms.

The Data Protection Addendum, or DPA (defined in the Glossary) sets forth the parties obligations with respect to the processing and security of Customer Data, Professional Services Data, and Personal Data by the Products. The Data Protection Addendum can be downloaded here <https://aka.ms/DPA>. In the event of any conflict or inconsistency between the DPA and any other terms in Customer's licensing agreement (including these terms), the DPA shall prevail.

Online Services excluded from the DPA

Except as provided in the [Product-Specific Terms](#), the terms of the [DPA](#) do not apply to: Bing Maps Mobile Asset Management Platform, Bing Maps Transactions and Users, Bing Search Services, Cognitive Services in containers installed on Customer's dedicated hardware, GitHub Offerings, LinkedIn Sales Navigator, Azure Defender for IoT (excluding any cloud-connected features), Azure SQL Edge, Azure Stack HCI, Azure Stack Hub, Microsoft Graph data connect for ISVs, Microsoft Genomics, and Visual Studio App Center Test. Each of these Online Services are governed by the privacy and security terms in the applicable [Product-Specific Terms](#).

Software Products excluded from the DPA

Except as provided in the [Product-Specific Terms](#), the terms of the [DPA](#) do not apply to: Internet based features in Software Products, Windows Desktop Operating System, Windows Server, and these Software Products as part of other Products. Each of these Products are governed by the privacy and security terms in the applicable [Product-Specific Terms](#).

Non-Microsoft Products

Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products (as defined in the [Universal License Terms for Online Services](#)).

DPA Terms Geography Exclusions

For Dynamics 365 and Power Platform online services, the specific terms of the [DPA](#) as noted in Appendix A stating "Microsoft stores copies of [Customer Data](#) and data recovery procedures in a different place from where the primary computer equipment processing the [Customer Data](#) is located." do not apply to the following geographies: United Arab Emirates and South Africa.

Core Online Services

The term "Core Online Services" applies only to the services in the table below, excluding any Previews.

Online Services	
Microsoft Dynamics 365 Core Services	The following services, each as a standalone service or as included in a Dynamics 365 branded plan or application: Dynamics 365 Customer Service, Dynamics 365 Customer Insights, Dynamics 365 Customer Service Insights, Dynamics 365 Field Service, Dynamics 365 Business Central, Dynamics 365 Supply Chain Management, Dynamics 365 Finance, Dynamics 365 Marketing, Dynamics 365 Commerce, Dynamics 365 Human Resources, and Dynamics 365 Sales. Dynamics 365 Core Services do not include (1) Dynamics 365 Services for supported devices or software, which includes but is not limited to Dynamics 365 for apps, tablets, phones, or any of these; (2) LinkedIn Sales Navigator; or (3) except as expressly defined in the licensing terms for the corresponding service, any other separately-branded service made available with or connected to Dynamics 365 Core Services.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Cortana, Customer Lockbox, Exchange Online Archiving, Exchange Online Protection, Exchange Online, Microsoft Bookings, Microsoft Forms, Microsoft MyAnalytics, Microsoft Planner, Microsoft StaffHub, Microsoft Stream, Microsoft Teams (including Bookings, Lists, and Shifts), Microsoft To-Do, Microsoft Defender for Office 365, Office 365 Video, Office for the web, OneDrive for Business, Project, SharePoint Online, Skype for Business Online, Sway, Whiteboard, Yammer Enterprise and, for Kaizala Pro, Customer's organizational groups managed through the admin portal and chats between two members of Customer's organization. Office 365 Services do not include Microsoft 365 Apps for enterprise, any portion of a PSTN service that operates outside of Microsoft's control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded "for Office 365."
Microsoft 365 Compliance Services	The following services, each as a standalone service or as included in a Microsoft 365-branded plan or suite: Compliance Manager, Microsoft Information Protection, Microsoft Information Governance, Insider Risk Management, Communication Compliance, eDiscovery and Audit.
Microsoft Azure Core Services	Anomaly Detector, API Management, App Service (API Apps, Logic Apps, Mobile Apps, Web Apps), Application Gateway, Application Insights, Automation, Azure Active Directory (including Multi-Factor Authentication), Azure API for FHIR, Azure App Configuration, Azure Bot Services, Azure Cache for Redis, Azure Cognitive Search, Azure Container Registry (ACR), Azure Container Service, Azure Cosmos DB (formerly DocumentDB), Azure Data Explorer, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Databricks, Azure DevOps Services, Azure DevTest Labs, Azure DNS,

Online Services	
	Azure Event Grid, Azure Firewall, Azure Health Data Services, Azure Information Protection (including Azure Rights Management), Azure Kubernetes Service, Azure NetApp Files, Azure Purview, Azure Resource Manager, Azure Spring Cloud, Azure Time Series Insights, Azure Video Analyzer for Media, Backup, Batch, BizTalk Services, Cloud Services, Computer Vision, Content Moderator, Custom Vision, Data Catalog, Data Factory, Data Lake Analytics, Data Lake Store, Event Hubs, Express Route, Face, Functions, HDInsight, Import/Export, IoT Hub, Key Vault, Language Understanding, Load Balancer, Log Analytics (formerly Operational Insights), Azure Machine Learning Studio, Media Services, Microsoft Azure Portal, Notification Hubs, Personalizer, Power BI Embedded, QnA Maker, Scheduler, Security Center, Service Bus, Service Fabric, SignalR Service, Site Recovery, Speech Services, SQL Data Warehouse, SQL Database, SQL Managed Instance, SQL Server Stretch Database, Storage, StorSimple, Stream Analytics, Synapse Analytics, Text Analytics, Traffic Manager, Translator, Virtual Machines, Virtual Machine Scale Sets, Virtual Network, and VPN Gateway
Microsoft Defender for Cloud Apps	The cloud service portion of Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security).
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365.
Microsoft Power Platform Core Services	The following services, each as a standalone service or as included in an Office 365 or Microsoft Dynamics 365 branded plan or suite: Microsoft Power BI, Microsoft Power Apps, and Microsoft Power Automate, and Microsoft Power Virtual Agents. Microsoft Power Platform Core Services do not include any client software, including but not limited to Power BI Report Server, the Power BI, PowerApps or Microsoft Power Automate mobile applications, Power BI Desktop, or Power Apps Studio.
Microsoft Defender for Endpoint Services	The cloud services portion of Microsoft Defender for Endpoint.
Microsoft 365 Defender	The cloud service portion of Microsoft 365 Defender.

Security Practices and Policies for Core Online Services

In addition to the security practices and policies for Online Services in the [DPA](#), each Core Online Service also complies with the control standards and frameworks shown in the table below and implements and maintains the security measures set forth in Appendix A of the [DPA](#) for the protection of [Customer Data](#).

Online Service	SSAE 18 SOC 1 Type II	SSAE 18 SOC 2 Type II
Office 365 Services	Yes	Yes
Microsoft 365 Compliance Services	Yes	Yes
Microsoft Dynamics 365 Core Services	Yes	Yes
Microsoft Azure Core Services	Varies*	Varies*
Microsoft Defender for Cloud Apps	Yes	Yes
Microsoft Intune Online Services	Yes	Yes
Microsoft Power Platform Core Services	Yes	Yes
Microsoft Defender for Endpoint Services	Yes	Yes
Microsoft 365 Defender	Yes	Yes

*Current scope is detailed in the audit report and summarized in the Microsoft Trust Center.

Location of Customer Data at Rest for Core Online Services

For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as follows except as otherwise provided in the Online Service-specific terms:

- **Office 365 Services.** If Customer provisions its tenant in Australia, Brazil, Canada, the European Union, France, Germany, India, Japan, Norway, South Africa, South Korea, Sweden, Switzerland, the United Kingdom, the United Arab Emirates, or the United

States, Microsoft will store the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, and (3) files uploaded to OneDrive for Business.

- **Microsoft Intune Online Services.** When Customer provisions a Microsoft Intune tenant account to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft Intune Trust Center.
- **Microsoft Power Platform Core Services.** When Customer provisions a Power Platform Core Service to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo, except as described in the Microsoft Power Platform Trust Center.
- **Microsoft Azure Core Services.** If Customer configures a particular service to be deployed within a Geo then, for that service, Microsoft will store Customer Data at rest within the specified Geo. Certain services may not enable Customer to configure deployment in a particular Geo or outside the United States and may store backups in other locations. Refer to the Microsoft Trust Center (which Microsoft may update from time to time, but Microsoft will not add exceptions for existing Services in general release) for more details.
- **Microsoft Defender for Cloud Apps.** If Customer provisions its tenant in the European Union or the United States, Microsoft will store Customer Data at rest only within that Geo, except as described in the Microsoft Defender for Cloud Apps Trust Center.
- **Microsoft Dynamics 365 Core Services.** When Customer provisions a Dynamics 365 Core Service to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo, except as described in the Microsoft Dynamics 365 Trust Center.
- **Microsoft Defender for Endpoint Services.** When Customer provisions a Microsoft Defender for Endpoint tenant to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft Defender for Endpoint Trust Center.
- **Microsoft 365 Defender.** When Customer provisions a Microsoft 365 Defender tenant to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft 365 Defender Trust Center.

Windows Desktop Operating System

Availability

Product	Program Attribute
Microsoft Defender for Endpoint Plan 1 (User SL)	
Microsoft Defender for Endpoint Plan 2 (User SL)	
Windows 10 Home Academic Legalization Get Genuine	
Windows 10 Pro Legalization Get Genuine	
Windows 11 Education (Per Device)	
Windows 11 Education E3 (SL)	
Windows 11 Education E5 (Per User)	
Windows 11 Enterprise (Per Device)	
Windows 11 Enterprise A3 (SL)	
Windows 11 Enterprise A5 (Per User)	
Windows 11 Enterprise E3 (SL)	
Windows 11 Enterprise E3 From SA (SL)	
Windows 11 Enterprise E3 Per User Add-on (to Enterprise per device) (SL)	
Windows 11 Enterprise E5 (SL)	
Windows 11 Enterprise E5 From SA (SL)	
Windows 11 Enterprise E5 Per User Add-on (to Enterprise per device) (SL)	
Windows 11 Home to Pro Right Licensing (Per Device)	
Windows 11 Home to Pro Upgrade for Microsoft 365 Business Premium	
Windows 11 Pro (Per Device)	
Windows 7 ESU 2021 (Per Device)	
Windows 7 ESU 2021 For M365 (Per Device)	
Windows 8.1 Enterprise Sideload (Per Device)	

Microsoft Product Terms (English, Jun 01 2022, MCA)

16

Windows Embedded 8 Standard Enterprise Kit (100 Pack)	
Windows Enterprise LTSC 2021 (Per Device)	
Windows VDA E3 (SL)	
Windows VDA E5 (SL)	
Windows VDA per device (SL)	

Product Conditions:

Provides additional information related to acquiring the Product, such as prerequisites for purchase, prior versions, and the applicable Product Pool.

Product Conditions - General	
Prior Version	Windows 10 Enterprise LTSC 2016 (10/16), Windows Embedded 8.1 Industry (4/14)
Product Pool	System
Promotions	None

Product Conditions - Program Specific	
Student Use Benefit	Refer to Student Use Benefits and Academic Programs

License Assignment for Windows Desktop Operating System Licenses

Per User License Assignment Eligibility (Excluding Virtual Desktop Access)

The Licensed User must be the Primary User of at least one device licensed with a Qualifying OS. This one device must also be the Primary User's primary work device.

Per Device License Assignment Eligibility (Excluding Virtual Desktop Access)

The Licensed Device must be licensed with a Qualifying OS, and the Qualifying OS must be installed on the Licensed Device. Per Device license assignment is permanent unless Customer has Software Assurance for that device.

Virtual Desktop Access (VDA) License Assignment Eligibility

VDA Per Device and Per User licenses may be assigned to any user or device.

Qualifying Operating Systems

Windows software acquired through a volume licensing agreement may only be installed or activated on devices licensed to run one of the qualifying operating systems (OS) below.

Qualifying OS for Per User Licenses and Virtual Desktop Access Per Device/User Licenses

Qualifying Operating Systems	Enterprise Agreement, Microsoft Products and Services Agreement, Select, Select Plus	Microsoft Cloud Agreement and Microsoft Customer Agreement
Windows 10/11		
Enterprise, IoT Enterprise, Pro, Pro for Workstations	X	X
Education, Home		X (Academic licenses only)
Windows 8/8.1 ¹		
Enterprise, Pro, Windows Embedded 8/8.1 Pro/Industry Pro	X	

¹ Windows 7 Operating Systems covered by an Extended Security Update (ESU) license are Qualifying Operating Systems during the device's active ESU coverage period. Windows 7 Enterprise, Professional, Ultimate and Professional/Ultimate for Embedded Systems editions are equivalent to Windows 8 Pro edition eligibility.

Qualifying OS - Per Device Licenses (Excluding Virtual Desktop Access Licenses)

Unless Customer has Software Assurance for the device, Customer must remove the Qualifying OS from the device before installing Windows software acquired through a volume licensing agreement on a Licensed Device.

Qualifying Operating Systems	New Enterprise Agreement (EA)/Open Value Company Wide (OV-OW) ¹	Existing Enterprise Agreement (EA)/Open Value Company Wide (OV-OW)	Microsoft Products and Services Agreement (MPSA)/Select Plus/Open	Microsoft Cloud Agreement and Microsoft Customer Agreement	Academic and Charity
Windows 10/11					
Enterprise, Pro, Pro for Workstations	X	X	X	X	X
Education, Home				X (Academic licenses only)	X
Windows 8/8.1 ²					
Enterprise, Pro	X	X	X		X
Windows 8/8.1					X
Apple					
macOS ³	X		X		X
Windows Embedded Operating Systems					
Windows 10/11 IoT Enterprise	X	X	X	X	X
Windows 2000 Professional for Embedded Systems	X		X		X
Windows XP Professional for Embedded Systems	X		X		X
Windows Vista Business/Ultimate for Embedded Systems	X		X		X
Windows 7 Professional/Ultimate for Embedded Systems	X	X	X		X
Windows Embedded 8/8.1 Pro/Industry Pro	X	X	X		X

¹ Also applicable to Qualified Devices acquired through merger or acquisition.

² Windows 7 Operating Systems covered by an Extended Security Update (ESU) license are Qualifying Operating Systems during the device's active ESU coverage period. Windows 7 Enterprise, Professional, and Ultimate editions are equivalent to Windows 8 Pro edition eligibility. Windows 7 Home Premium, Home Basic, and Starter Edition editions are equivalent to Windows 8 edition eligibility.

³ macOS must be preinstalled by the authorized manufacturer prior to the initial sale of the device.

Third Party Re-imaging

Before a third party may re-image a Customer's devices, Customer must provide the third party with written documentation showing it has the requisite licenses for the installation.

Purchase Eligibility for Windows 11 Home to Pro Upgrade for Microsoft 365 Business Premium

Customers in Australia, Canada, Iceland, Japan, New Zealand, Norway, South Africa, Switzerland, United Kingdom, USA, or any country in the European Union may license the Windows 11 Home to Pro Upgrade for Microsoft 365 Business Premium in any quantity up to the

number of its Microsoft 365 Business Premium subscriptions. Notwithstanding the Qualifying OS license requirements, Customer may install Windows 11 Home to Pro Upgrade for Microsoft 365 Business Premium software on devices licensed with Windows Home version 7 or later.

Automatic Updates

Customer authorizes Microsoft to download and install updates automatically on devices running Windows 10/11 unless they have been configured to prevent automatic updates using supported methods. All updates are licensed under the same terms as the Product to which they apply.

Windows 7 ESU (Extended Security Updates)

Customer may acquire Windows 7 ESU licenses on a per device basis. Devices running a local OSE covered by ESU or accessing virtual OSEs covered by ESU must be licensed with Windows 7 ESU for the respective year of coverage. Devices do not need an ESU license to access Windows 7 OSEs covered by ESU running on Azure Virtual Desktop. If Customer has one or more ESU licenses, devices do not need an ESU license to run or access Windows 7 OSEs covered by ESU when the OSE is licensed through a Visual Studio Subscription for development or test purposes. Windows 7 ESU 2020/2021/2022 for M365 licenses may only be assigned to devices with active Software Assurance or used exclusively by users with Windows Enterprise, VDA, or M365 SLs (that include Windows Enterprise). Windows 7 ESU 2020/2021/2022 licenses may be assigned to any device. Windows 7 ESU 2021 & 2022 and Windows 7 ESU 2021 & 2022 for M365 licenses may only be assigned to devices also licensed with ESU(s) for the prior year(s).

Academic and Charity Programs

License Assignment

Per User License Assignment

The Licensed User must be the Primary User of at least one device that satisfies the Qualifying OS Per Device License requirements.

Per Device License Assignment

The Licensed Device must satisfy the Qualifying OS Per Device license requirements, and the Qualifying OS must be installed on the Licensed Device. Per Device license assignment is permanent unless Customer has Software Assurance for that device.

Academic Program Windows Edition Rights

Windows Education licenses include rights to install or activate Windows Enterprise in lieu of Windows Education.

Lab and Library Use

Institutions with Windows Education E3/E5, or Windows Education (per device) assigned to all faculty and staff, Education Qualified Users or Knowledge Workers may install Windows Education, Windows Enterprise, or Windows Pro Academic on any open access lab or library within the Institution's Organization. Use of the software is otherwise subject to the License terms for Windows Education. This provision does not apply to User SLs acquired under the Microsoft Cloud Agreement and Microsoft Customer Agreement.

Shared Devices

Institutions with Windows Education E3/E5 assigned to all Knowledge Workers or Education Qualified Users are licensed to run Windows Education, Windows Enterprise, or Windows Pro Academic on any shared device with a qualifying operating system within the Institution's Organization. For the purposes of this subsection, shared device means a device not used by any one person more than 50% of the time during a single work day period, and not assigned to any Primary User as their primary work device. Use of Windows on shared devices does not count as use of an Education Platform Product under the Enrollment for Education Solutions. Use of the software is otherwise subject to the License terms for Windows Education.

Graduation Benefit

Institutions with an active Agreement may, at any time during the Agreement term, transfer a Student's Windows Education license to such Student when they become a Graduate if the Student installs or activates Windows Education on a Student owned device while

enrolled at the institution. Institution must provide each such Graduate with a license agreement in the form provided by Microsoft. Upon the Graduate's acceptance of the terms of the license agreement, the Graduate receives a perpetual right to run Windows Education locally on the same device. This entitlement is nontransferable to any other device.

Get Genuine Windows Licenses

- Customers may acquire Get Genuine Windows (also known as "GGWA") licenses for the full version of the Windows desktop operating system for devices that require valid Windows licenses. Because Get Genuine Windows licenses are full licenses for Windows, they do not have a Qualifying OS requirement.
- Get Genuine Windows licenses are available only as a one-time purchase per Customer, where all units must be placed under a single order. Get Genuine Windows licenses may not be assigned to devices without a Qualifying OS if such devices are obtained after the Customer's order.

Use Rights

Identifies the License Terms for each Software Product, including the Universal License Terms, the applicable License Model, and any Product-Specific License Terms. References in Customer's volume licensing agreement to "Use Rights" refer to the terms included in the Use Rights section of each Software Product Entry.

Use Rights	
License Terms	Universal License Terms for all Software (see Additional License Terms for Online Services section below)
Down Editions	Enterprise to Pro
External User Access Requirements	None
Included Technologies	None
Notices	H.264/MPEG-4 AVC and/or VC-1 - refer to Notices

Additional License Terms for Online Services

Certain Windows software licenses include some Online Services which are governed by the [Universal License Terms for Online Services](#), including but not limited to, Microsoft Defender for Endpoint, Windows Update Compliance, Windows Update for Business deployment service, and Desktop Analytics.

Windows diagnostic data processor configuration

For Windows 10/11 Enterprise, Pro and Education editions (version 1809 with July 2021 update or newer), Microsoft is the processor for Windows diagnostic data collected from a device where the Windows diagnostic data processor configuration is set by joining an Azure Active Directory account to the device and enabling group policy as described in the Product documentation. Except as provided above, Microsoft will continue to be a controller of Personal Data processed in connection with your use of Windows, including data processed by Microsoft in connection with Customer's use of service-based capabilities. When Microsoft is a controller, Microsoft will handle the Personal Data in accordance with the Microsoft Privacy Statement (aka.ms/privacy), and the [Data Protection Addendum](#) (aka.ms/DPA) terms do not apply.

Windows Local Use

Customer may run Windows software acquired through a volume licensing agreement as one Physical OSE locally on Licensed Devices. This local use right applies to VDA per device licenses only if the Licensed Device is also licensed with a Qualifying Operating System. Licensed Users may run Windows software acquired through a volume licensing agreement as one Physical OSE locally on devices licensed with a Qualifying Operating System.

Windows Azure AD-Based Activation

[Licensed Users](#) using Azure AD-based activation may activate the software in the [Physical OSE](#) on up to five concurrent devices running either Windows 10 Pro Anniversary Update or Windows 10 Enterprise Creator's Update or a later version.

Microsoft Defender for Endpoint

Eligible Licensed Users may use Microsoft Defender for Endpoint on up to five concurrent devices.

Windows Apps

Unless other terms are displayed to Customer or presented in the app's settings, Customer agrees the services that it accesses from the Windows app is governed by the Microsoft Services Agreement at <http://go.microsoft.com/fwlink/?linkid=246338> or for Windows apps that access Xbox services, the Xbox.com terms of use at <http://xbox.com/legal/livetou>.

Microsoft Customer Agreement Activation Use Rights

For Customers licensed under a Microsoft Cloud Agreement or Microsoft Customer Agreement,

- Notwithstanding Windows Azure AD-Based Activation and Windows 11 Upgrade Benefit requirements, each user may activate no more than five concurrent instances of the software across physical and virtual OSEs.
- For subscription licenses only, notwithstanding the Universal License Terms for all Software or volume licensing agreement, upgrade subscription licenses do not include rights to run or install a prior version, different language version, different platform version, or a lower edition of Windows, including Windows Enterprise LTSC. Users may, however, apply their edition upgrades to Windows 10 devices without updating to Windows 11 if they chose.
- Software Assurance Benefits do not apply.

Windows 11 Upgrade Benefit

The following User SLs include a Windows 11 upgrade benefit (version upgrade only, edition remains the same) for device(s) licensed with Windows 8, 8.1, 10:

- Windows 11 Enterprise/Education (all)
- Microsoft 365 (all that include Windows 11 Enterprise)

Windows 11 Multitenant Hosting

Customers with Windows 11 Enterprise Per User SLs (excluding local only), Windows 11 Education Per User SLs, or VDA Per User SLs using Azure AD-based activation on supported editions may install the Windows 10 Creators Update or later version software on a virtual machine running in Customer's Microsoft Azure accounts (notwithstanding anything to the contrary in the Outsourcing Software Management clause) or a shared server with a Qualified Multitenant Hosting Partner ("QMTH") identified at <https://aka.ms/QMTHAuthorizedPartnerList>. Rights to install and use the software with a QMTH do not apply if the QMTH is using a Listed Provider as a Data Center Provider. Each Licensed User may access up to four instances of the software. Azure Government customers may use KMS activation in lieu of Azure AD-based activation. When configuring the image(s) on Microsoft Azure, Customers must indicate their use of the multitenant hosting for Windows and adhere to other software configuration requirements available at <https://docs.microsoft.com/en-us/windows/deployment/vda-subscription-activation>. This section does not apply to Students receiving access to software through Student Use Benefit.

Azure Virtual Desktop for Windows

Azure Virtual Desktop for Windows

Users licensed with Microsoft 365 E3/E5/F3/Business Premium/A3/A5/Student Use Benefit, Windows Enterprise E3/E5, Windows Education A3/A5, or Windows VDA E3/E5 may access Azure Virtual Desktop Windows virtual machines running in Customer's Microsoft Azure accounts. Azure Virtual Desktop virtual machines do not count against a user's device activation count limit.

Azure Virtual Desktop for Development and Test

Users licensed with Visual Studio subscriptions and MSDN Platforms with active SA ("Authorized Users") may access Azure Virtual Desktop Windows, and Windows Server virtual machines running in Customer's Microsoft Azure accounts for development and test purposes. Customer's end users may also access Azure Virtual Desktop Windows, and Windows Server virtual machines initiated by Authorized Users to perform acceptance tests or provide feedback.

Azure Virtual Desktop Per User Access Operating System

Universal Terms. The following Universal License Terms for all Software do not apply to the Azure Virtual Desktop per user access operating system software: Rights to Use Other Versions and Lower Editions; Software Assurance; Outsourcing Software Management.

Windows 365 Operating System

Universal Terms. The following Universal License Terms for all Software do not apply to the Windows 365 operating system software: Rights to Use Other Versions and Lower Editions; Software Assurance; Outsourcing Software Management.

License Model

Desktop Operating Systems

Device License

1. Customer may install one copy of the software on a Licensed Device or within a local virtual hardware system on a Licensed Device for each License it acquires.
2. Customer may use the software on up to two processors.
3. Local use is permitted for any user.
4. Remote use is permitted for the Primary User of the Licensed Device and for any other user from another Licensed Device or a Windows VDA Licensed Device.
5. Only one user may access and use the software at a time.
6. Customer may connect up to 20 devices to the Licensed Device for file sharing, printing, Internet Information Services, Internet Connection Sharing or telephony services.
7. An unlimited number of connections are allowed for KMS activation or similar technology.

Adobe Flash Player

The software may include a version of Adobe Flash Player. Customer agrees that its use of the Adobe Flash Player is governed by the license terms for Adobe Systems Incorporated at <http://go.microsoft.com/fwlink/?linkid=248532>. Adobe and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Microsoft Azure

Availability

Product	Program Attribute
Azure Active Directory Premium Plan 1 (User SL)	
Azure Active Directory Premium Plan 2 (User SL)	
Azure Active Professional Direct Support*	
Azure Active Standard Support*	
Azure Information Protection Premium Plan 1 (User SL)	
Azure Site Recovery (to Customer Owned Site)	
Azure SQL Edge (per Device)	
Microsoft Azure Services	
Microsoft Defender for Identity (User SL)	
Microsoft Defender for Identity Client Management License Add-on (User SL)	
Microsoft Translator API	

*Also available through Microsoft Customer Agreement and Reduction Eligible when acquired under that agreement.

Product Conditions:

Provides additional information related to acquiring the Product, such as prerequisites for purchase, prior versions, and the applicable Product Pool.

Microsoft Azure	
Terms of Service	Universal License Terms for Online Services (For Azure Virtual Desktop per user access, Windows operating system is governed by the Universal License Terms for all Software and includes specific terms in Windows Desktop Operating System terms)
Product Pool	Server
Promotions	None

Product Conditions - Program Specific	
Student Use Benefit	Refer to Student Use Benefits and Academic Programs

Product Categories

This table highlights which Azure products fall under the categories of Microsoft Azure Infrastructure Plans, Microsoft Azure User Plans, Microsoft Azure Support Plans, and Microsoft Azure Services:

Product Category	Product
Microsoft Azure Infrastructure Plans	Microsoft Azure StorSimple Plan 8100 & 8600 Renewal (no device), Microsoft Azure StorSimple Plan with Device (8100 & 8600 device)
Microsoft Azure User Plans	Azure Active Directory Premium Plan 1 & 2(User SL), Azure Information Protection Premium Plan 1 (User SL), Azure Information Protection Premium Plan 1 Add-on (User SL), Microsoft Defender for Identity (User SL), Microsoft Defender for Identity Client Management License Add-on (User SL)
Microsoft Azure Support Plans	Azure Active Professional Direct Support, Azure Active Standard Support, Microsoft Azure StorSimple Premium & Standard Support, Microsoft Azure StorSimple Standard Support to Premium Support
Microsoft Azure Services	Azure SQL Edge (per Device), Microsoft Translator API, Microsoft Azure Services

Microsoft Azure Services Plans

If subscribed to by Customer as a [Microsoft Azure Services Plan](#), individual Microsoft Azure Services may have different program availability or be subject to different terms. Other than Azure Stack Hub, Services purchased as a [Microsoft Azure Services Plan](#) are not eligible for the Azure Customer Solution clause in the General Service Terms for Azure.

Subscription Term

Azure is licensed on a subscription basis for a fixed term. Usage is metered, and charges are applied periodically based on usage. Some subscriptions require prepayment or an upfront commitment and others are billed after the services are used ("pay-as-you-go"). Pay-as-you-go subscriptions automatically renew after each billing period unless cancelled before the end of the billing period. For plans that require an upfront commitment (such as Azure reservations), the term of the subscription is the same as the commitment period. At the end of the term, such subscriptions may be renewed automatically on a pay-as-you go basis provided that there is an active funded order.

The table below highlights the subscription terms for the options to purchase Microsoft Azure Services that a customer is eligible for:

Options	Subscription Term
Consumption	Subscription term is the same as the billing period.
Microsoft Azure Services Plan	Subscription term is the same as the billing period.
Azure reservations	Subscription term is the same as the Azure reservation commitment term.

Purchasing Microsoft Azure Services

Microsoft Azure Services may be purchased in one or a combination of the following ways:

Consumption: Customer pays based on the amount of Microsoft Azure Services consumed during a billing period. Certain features of the Microsoft Azure Services may only be available for purchase on a consumption basis.

Microsoft Azure Services Plan: Customer may be able to subscribe to a Microsoft Azure Service as a [Microsoft Azure Services Plan](#).

Azure reservations: [Azure reservations](#) are purchased for specified terms of up to three years with equal monthly payments.. [Azure reservations](#) expire at the end of the specified term. Customer may cancel an Azure reservation and receive a prorated refund based on a remaining Azure reservation term, up to a pro-rated amount of \$50,000 per year.

Pricing

Microsoft may offer lower prices to Customer (or Customer's reseller) for individual Microsoft Azure Services during Customer's Agreement term on a permanent or temporary (promotional) basis.

Azure reservations: Notwithstanding the terms in Customer's volume licensing agreement, fixed pricing does not apply to [Azure reservations](#). Azure reservation pricing will be based on the available pricing at the time of each purchase in accordance with the GSA Schedule Pricelist.

Payment and Fees

This table highlights which Azure Product categories are eligible for the Payment and Fees options below. Please reference the Product Category table above for eligible products.

Payment and Fees options	Eligible Products*
1. Reserved	
2. Reserved	
3. Reserved	
4. Consumption Invoicing	Microsoft Azure Services
5. Azure Services Plan Invoice	Microsoft Azure Infrastructure Plans, Microsoft Azure Support Plans, Microsoft Azure User Plans
6. Azure reservations	Microsoft Azure Services

*Some Products may not be eligible for certain Payment and Fees scenarios. Please refer to the Azure Portal or Pricing Calculator (<https://azure.microsoft.com/pricing/calculator/>) for more information on availability.

- **Consumption Invoicing:** If Customer provisions Microsoft Azure Services it will be invoiced monthly at Consumption Rates.
- **Azure Services Plan Invoice:** The purchase of a Microsoft Azure Services Plan will be invoiced to Customer either on an upfront or annual basis, according to the terms of Customer's volume licensing agreement governing payment terms for the order of Online Services generally.
- **Azure reservations:** Azure reserved instances for a virtual machine or Azure SQL Database services cover compute only (the base rate) and do not include the cost of the software (e.g., Windows Server or SQL Server), storage or back-up. Conversely, Azure reserved instances for software do not include the cost of compute.

Azure Reservation Options

The following options apply to Azure reservations Customer has purchased.

1. **Exchange:** is an option that allows Customer to apply the monetary value of a remaining Azure reservation term to the purchase of one or more new Azure reservations of equal or greater monetary value for the same service.
2. **Cancel:** is an option that allows Customer to receive a prorated refund based on a remaining Azure reservation term, up to a pro-rated amount of \$50,000 per year).
3. **Assignment:** allows Customer to apply an Azure reservation to a single (scoped) subscription of the Agreements/account(shared).

Azure Hybrid Benefit

Microsoft Azure Hybrid Benefit for Windows Server

Under the Microsoft Azure Hybrid Benefit for Windows Server, Customer may use Windows Server Virtual Machines in Customer's Microsoft Azure service accounts and pay for the cost of compute only (the "Base Instance"). Customer must indicate that it is using Windows Server under the Azure Hybrid Benefit for Windows Server when creating or configuring a virtual machine on Azure. The Online Services Terms govern use of Windows Server under this benefit. Customer may not concurrently allocate Windows Server Licenses to Azure Hybrid Benefit and assign the same Licenses to its Licensed Servers, except on a one-time basis, for a period not to exceed 180 days, to allow Customer to migrate the same workloads to Azure. On the earlier of completion of migration to Azure or 180 days from the start of migration, Licenses will be deemed "assigned to Azure". Customer may later reassign Licenses back to its Licensed Servers, provided Licenses remain assigned to Azure for a minimum of 90 days.

Except as provided below for Windows Server Datacenter Licenses allocated as described in "Unlimited Virtualization Rights, each Windows Server processor License with SA, and each set of 16 Windows Server core Licenses with SA, entitles Customer to use Windows Server on Microsoft Azure on up to 16 Virtual Cores allocated across two or fewer Azure Base Instances. Each additional set of 8 core Licenses with SA entitles use on up to 8 Virtual Cores on one Base Instance. Customer may use Standard or Datacenter software.

Special Use Rights for Windows Server Datacenter Licenses

As exceptions to the general terms governing allocation of licenses and use of Windows Server under the Azure Hybrid Benefit for Windows Server:

- **Unlimited Virtualization Rights.** Customer may use Windows Server in any number of Base Instances on an Azure Dedicated Host or other dedicated physical host in Azure, provided Customer allocates Windows Server Datacenter Licenses with SA for all of the Physical Cores available to Customer on that Azure server. Concurrent use on Azure Dedicated Host or other dedicated physical host in Azure and Customer's Licensed Servers is limited to the same 180 day migration period.
- **Dual Use Rights.** When exercised in connection with Datacenter Licenses with SA, the Azure Hybrid Benefit for Windows Server provides rights to simultaneously deploy and use the software on Azure and on Licensed Servers in Customer's data centers. Dual use rights do not apply in the case of Licenses allocated as described in "Unlimited Virtualization Rights."

Microsoft Azure Hybrid Benefit for SQL Server

Under the Microsoft Azure Hybrid Benefit for SQL Server, for each SQL Server License covered with SA ("Qualified License"), Customer may consume in its Microsoft Azure services accounts the Microsoft Azure Data Services identified in the table below in the indicated

ratios. If a customer wishes to use Azure Hybrid Benefit for SQL Server to consume two or more Azure Data Services, one or more Licenses must be allocated for each service.

Qualified License	Microsoft Azure Data Service ¹	Ratio of Qualified Licenses to Azure vCores
SQL Server Enterprise (Core)	Azure Arc-enabled SQL Managed Instance - General Purpose	1 Core License:4 vCores
	Azure SQL Database (Elastic Pool and Single Database)/Azure SQL Managed Instance - General Purpose	1 Core License:4 vCores
	Azure SQL Database (Elastic Pool and Single Database)/Azure SQL Managed Instance - Business Critical	1 Core License:1 vCore
	Azure SQL Database (Single Database)/Azure SQL Managed Instance - Hyperscale	1 Core License:4 vCore
	Azure Data Factory SQL Server Integration Services (Enterprise)	1 Core License:1 vCore
	Azure Data Factory SQL Server Integration Services (Standard)	1 Core License:4 vCores
	SQL Server Enterprise Virtual Machines	1 Core License ² :1 vCPU
	SQL Server Standard Virtual Machines	1 Core License:4 vCPUs
SQL Server Standard (Core)	Azure Arc-enabled SQL Managed Instance - General Purpose	1 Core License:1 vCore
	Azure SQL Database (Elastic Pool and Single Database)/Azure SQL Managed Instance - General Purpose	1 Core License:1 vCore
	Azure SQL Database (Elastic Pool and Single Database)/Azure SQL Managed Instance - Business Critical	4 Core License:1 vCore
	Azure SQL Database (Single Database)/Azure SQL Managed Instance - Hyperscale	1 Core License:1 vCore
	Azure Data Factory SQL Server Integration Services (Standard)	1 Core License: 1 vCore
	Azure Data Factory SQL Server Integration Services (Enterprise)	4 Core Licenses:1 vCore
	SQL Server Standard Virtual Machines	1 Core License ² :1 vCPU
	SQL Server Enterprise Virtual Machines	4 Core Licenses ² :1 vCPU

¹Azure Hybrid Benefit is not available in the serverless compute tier of Azure SQL Database.

²Subject to a minimum of four Core Licenses per Virtual Machine.

With Azure Hybrid Benefit for SQL Server, Customers will not be charged for the usage of an Azure Data Service, but it will pay for the cost of compute (i.e., the base rate), storage, and back-up, as well as I/O associated with their use of the services (as applicable). Customers must indicate that it is using the applicable Azure Data Service under Azure Hybrid Benefit for SQL Server when configuring workloads on Azure.

Customer may not concurrently allocate a License to Azure Hybrid Benefit for SQL Server and assign the same License to (a) shared servers under License Mobility through Software Assurance or (b) a Licensed Server, except on a one-time basis, for a period not to exceed 180 days, to allow Customer to migrate those workloads to Azure.

On the earlier of completion of migration to Azure or 180 days from the start of migration, Licenses will be deemed "assigned to Azure". Customer may later reassign Licenses back to its Licensed Servers or to shared servers under License Mobility through Software Assurance, provided Licenses remain assigned to Azure for a minimum of 90 days.

Fail-over Rights for SQL Server Standard/Enterprise Virtual Machines

When allocating SQL Server Licenses for use with a SQL Server Standard/Enterprise Virtual Machine under the Azure Hybrid Benefit for SQL Server, Customer is entitled to:

- One Fail-over OSE for any purpose, including high availability; and
- One Fail-over OSEs specifically for disaster recovery purposes.

Customer may also run Primary Workload and its disaster recovery Fail-over OSE simultaneously for brief periods of disaster recovery testing every 90 days, and around the time of a disaster, for a brief period, to assist in the transfer between them. Customer may perform the following maintenance-related operations for any permitted Fail-over OSE:

- Database consistency checks or Checkdb
- Log Back-ups
- Full Back-ups
- Monitoring resource usage data

Fail-over OSEs permitted for disaster recovery must be asynchronous and manual. The number of Licenses that otherwise would be required for a Fail-over OSE must not exceed the number of Licenses required for the corresponding Primary Workload. Fail-over OSEs may not serve SQL Server data to users or devices or otherwise run active SQL Server workloads.

Customer is entitled to one additional Fail-over OSE for high availability for each of its Primary Workloads that runs on the Linux platform and serves as the SQL Server master instance when used in conjunction with Customer's use of Big Data Clusters. These additional Fail-over OSEs are subject to the same Fail-Over Rights limitations.

SQL Server Enterprise Core Unlimited Virtualization Rights

As an exception to the general terms governing allocation of Licenses and use of SQL Server under the Azure Hybrid Benefit for SQL Server, Customer may use SQL Server in any number of Virtual Machines on an Azure Dedicated Host or other dedicated physical host in Azure in one of its Microsoft Azure service accounts, provided Customer allocates SQL Server Enterprise Core Licenses with SA for all of the Physical Cores available to Customer on that Azure Dedicated host. Concurrent use on Azure Dedicated Host or other dedicated physical host in Azure and Customer's Licensed Servers is limited to the same 180 day migration period.

Limited Hosting Rights for Azure Arc-enabled SQL Managed Instance

When using Azure Hybrid Benefit, paragraph 3 of the Service Specific terms for Azure Arc-enabled SQL Managed Instance does not apply. Customer is entitled only to run its Azure Arc-enabled SQL Managed Instance containers on Microsoft Azure, its own Servers, or Servers under the day-to-day management and control of Authorized Outsourcers, regardless of whether those Servers are dedicated to Customer or not.

Azure Virtual Desktop

Azure Virtual Desktop Conditions

The Azure Virtual Desktop control plane may only be used to manage Azure Virtual Desktop VMs running on Azure. Windows Enterprise multi-session is limited for use on Azure Virtual Desktop VMs running on Azure only.

Azure Virtual Desktop for Windows

Users licensed with Microsoft 365 E3/E5/F3/Business Premium/A3/A5/Student Use Benefit, Windows Enterprise E3/E5, Windows Education A3/A5, or Windows VDA E3/E5 may access Azure Virtual Desktop Windows virtual machines running in Customer's Microsoft Azure accounts. Azure Virtual Desktop virtual machines do not count against a user's device activation count limit.

Azure Virtual Desktop for Windows Server

Users licensed with RDS User CALs with SA or RDS User Subscription Licenses or using devices licensed with RDS Device CALs with SA may access Azure Virtual Desktop Windows Server virtual machines running in Customer's Microsoft Azure accounts.

Azure Virtual Desktop for Development and Test

Users licensed with Visual Studio subscriptions and MSDN Platforms with active SA ("Authorized Users") may access Azure Virtual Desktop Windows, and Windows Server virtual machines running in Customer's Microsoft Azure accounts for development and test purposes. Customer's end users may also access Azure Virtual Desktop Windows, and Windows Server virtual machines initiated by Authorized Users to perform acceptance tests or provide feedback.

Azure Dev/Test Pricing

Customer may be eligible for Azure dev/test pricing for Azure Services accessed by (i) its Qualified Licensed Users solely for development and test purposes, and (ii) its users performing acceptance tests and providing feedback related to those development and test activities. "Qualified Licensed Users" means users allocated Visual Studio subscriptions or MSDN Platform subscriptions with active Software Assurance. See Azure.com (<https://azure.microsoft.com/pricing/dev-test/>) for eligibility criteria and applicable services.

General Service Terms

Restriction on U.S. Police Department Use of Azure Facial Recognition Services

Customer may not use Azure Facial Recognition Services if Customer is, or is allowing use of such services by or for, a police department in the United States. Violation of any of the restrictions in this section may result in immediate suspension of Customer's use of the service.

Notices

The Bing Maps, Professional Services, Azure Media Services H.265/HEV Encoding, Adobe Flash Player, H.264/AVC Visual Standard, VC-1 Video Standard, and MPEG-4 Part 2 Visual Standard and MPEG-2 Video Standard in Notices apply.

Service Level Agreement

Refer to <http://azure.microsoft.com/support/legal/sla/>.

Limitations

Customer may not

- resell or redistribute the Microsoft Azure Services, or
- allow multiple users to directly or indirectly access any Microsoft Azure Service feature that is made available on a per user basis (e.g., Active Directory Premium). Specific reassignment terms applicable to a Microsoft Azure Service feature may be provided in supplemental documentation for that feature.

Retirement of Services or Features

Microsoft will provide Customer with 12 months' notice before removing any material feature or functionality or discontinuing a service, unless security, legal or system performance considerations require an expedited removal. This does not apply to Previews.

Data Retention after Expiration or Termination

The expiration or termination of Customer's Online Service subscription will not change Customer's obligation to pay for hosting of Customer Data during any Extended Term.

Azure Customer Solution

Use Rights and Conditions for Use

Customer may create and maintain a Customer Solution. Despite anything to the contrary in Customer's licensing agreement, Customer may permit third parties to access and use the Microsoft Azure Services solely in connection with the use of that Customer Solution.

Customer is responsible for ensuring that third parties who access, use or distribute the Customer Solution comply with these terms, the terms and conditions of Customer's licensing agreement, and all applicable laws.

Use of Software within Microsoft Azure

For Microsoft software available within a Microsoft Azure Service, Microsoft grants Customer a limited license to use the software only within the Microsoft Azure Service.

Data Center Availability

Usage of data centers in certain regions may be restricted to Customers located in or near that region. For information on service availability by region, please refer to <http://azure.microsoft.com/en-us/regions>.

Sharing

The Microsoft Azure Services may provide the ability to share a Customer Solution and/or Customer Data with other Azure users and communities, or other third parties. If Customer chooses to engage in such sharing, Customer agrees that it is giving a license to all authorized users, including the rights to use, modify, and repost its Customer Solution and/or the Customer Data, and Customer is allowing Microsoft to make them available to such users in a manner and location of its choosing.

Marketplace

Microsoft Azure enables Customer to access or purchase products and services which are optimized for use with Azure through features such as the Microsoft Azure Marketplace and the Virtual Machine Gallery, subject to separate terms available at <http://azure.microsoft.com/en-us/support/legal/store-terms>.

Service Specific Terms

Subscription License Suites

In addition to User SLs, refer to Subscription License Suites for other SLs that fulfill requirements for Azure Active Directory Premium, Microsoft Defender for Identity, Azure Information Protection, and Microsoft Intune.

API Terms for Security & Compliance Applications

"Compliance Application" means a software program or service built exclusively to ensure that an organization is complying with their security-related requirements.

"Security Application" means a software program or service built exclusively to protect and defend the information and technology assets of an enterprise.

"End User" refers to the end-user of the S&C Application.

"Customer" refers to the registered owner of the Azure subscription where the S&C application is registered with Azure Active Directory.

The following terms and conditions apply to an S&C Application's use of the S&C APIs:

- The End User must have one of the following Microsoft 365 E5 eligible licenses: Microsoft 365 E5/A5/G5, Microsoft 365 E5 Security, Microsoft 365 E5 Compliance, Microsoft 365 E5 Information Protection and Governance, or Microsoft 365 E5 Information Protection & Data Loss Prevention.
- Microsoft will bill Customer for all commercial consumption of API messages that exceed the included monthly seeded allowance per End User tenant. Refer to <https://docs.microsoft.com/en-us/graph/teams-licenses> to understand and review the seeded allowances and pricing details for the S&C APIs.
- S&C Applications must query the S&C APIs with model=Aquery parameter.

The following terms and conditions apply to an application's use of the S&C APIs (other than an S&C Application):

- Microsoft will bill Customer for all commercial consumption of API messages, including, but not limited to, use with the following applications:
 - **Backup and Restore:** Applications that allows users to create or restore backups of messages or files and create and restore system images to repair data in the event of data corruption, or data loss.
 - **Sentiment analysis:** Applications that use natural language processing, text analysis, computational linguistics, biometrics, and other techniques to systematically identify, extract, quantify, and study affective states and subjective information.
 - **Analytics and Insights:** Applications offering continuous iterative exploration and investigation of information to gain.
- Applications that do not qualify as an S&C Application must query the S&C APIs with model=Bquery parameter.

These terms and conditions supersede any terms and conditions contained elsewhere, including the Microsoft APIs Terms of Use [<https://docs.microsoft.com/en-us/legal/microsoft-apis/terms-of-use>].

Azure Active Directory Basic

Customer may, using Single Sign-On, pre-integrate up to 10 SAAS Applications/Custom Applications per User SL. All Microsoft as well as third party applications count towards this application limit.

Azure Active Directory Premium

Customer may, using Single Sign-On, pre-integrate SaaS Applications/Custom Applications. Customer may not copy or distribute any data set (or any portion of a data set) included in the Microsoft Identity Manager software that is included with a Microsoft Azure Active Directory Premium (P1 and P2) User SL.

External User Allowance

For each User SL (or equivalent Subscription License Suite) Customer assigns to a user, Customer may also permit up to five additional External Users to access the corresponding Azure Active Directory service level. This option is not available to new customers nor customers using (or who have used) the service under a Monthly Active User count. Only External Users can use the Azure Active Directory External Identities pricing based on Monthly Active User count.

Azure Arc-enabled SQL Managed Instance

Use Rights

1. Azure Arc-enabled SQL Managed Instance licenses are not assigned to any given Server and are therefore not subject to the License Assignment and Reassignment clause.
2. Licenses are billed according to the terms of the license meter. Customer must connect to Azure at least once every 30 days via direct connected mode or indirect export mode to report usage data.
3. Notwithstanding the Outsourcing Software Management clause, Customer may run Azure Arc-enabled SQL Managed Instance containers on Microsoft Azure, its own Servers, or Servers under the day-to-day management and control of third parties, regardless of whether those Servers are dedicated to Customer or not.

The terms of the DPA do not apply to processing of data in Azure Arc enabled SQL Managed Instance running in an environment outside of Microsoft's control, except to the extent any Personal Data is collected to enable Azure management services and to meter usage for billing purposes.

Azure Communication Services

Customer Responsibility

Azure Communication Services is a developer product and an input to customers' applications. Customers are solely liable for their applications or offerings that incorporate Azure Communication Services capabilities and services.

Notices

The H.264/AVC Visual Standard notice in Notices section applies.

PSTN Services

Azure Communication Services provides services for calling and text messaging to and from the public switched telephone network ("PSTN"). Azure Communication Services PSTN services are provided by the Microsoft Affiliate or other service provider authorized to administer them. Pricing for PSTN services may include applicable taxes and fees. PSTN services terms may vary from country to country. All included taxes, fees and country-specific terms of use are disclosed in the terms of use available on the Volume Licensing site at <https://aka.ms/CommunicationServicesTerms>.

Microsoft Teams Interoperability

Interoperability between Azure Communication Services and Microsoft Teams enables your applications and users to participate in Teams calls, meetings, and chat. It is your responsibility to ensure that the users of your application are notified when recording or transcription are enabled in a Teams call or meeting. Microsoft will indicate to you via the Azure Communication Services API that

recording or transcription has commenced and you must communicate this fact, in real time, to your users within your application's user interface.

License Terms Precedence

Some Azure Communication Services, including private previews and Previews, may be provided under a separate license, such as an open-source license. In the event of a conflict between these terms and any separate license, the separate license will prevail with respect to the Azure Communication Service that is the subject of such separate license. Each party reserves all rights (and no one receives any rights) not expressly granted by the foregoing licenses.

End User Information

Except in instances required by law or regulation, Microsoft does not retain information that identifies individual end users. Customer acknowledges that, should it delete or de-link end user identifying information in its possession, Microsoft shall have no responsibility to reconstitute the information.

Defense of Claims

In accordance with the procedures set forth in the Contract Disputes Act, You agree to be responsible for all direct damages caused by a material breach to these terms by you or your subcontractors, agents, employees, or customers

Messaging Policy

Customer and its end users shall comply with the Azure Communication Services Messaging Policy. The Messaging Policy applies to SMS and MMS communications. Microsoft reserves the right to suspend or remove access to Azure Communication Services for Customer or its end users that do not comply with the Messaging Policy. The Messaging Policy is available at <https://docs.microsoft.com/en-us/azure/communication-services/concepts/telephony-sms/messaging-policy>.

Azure Defender for IoT

Customer may use Azure Defender for IoT solely to monitor devices based on its current commitment level. Customer agrees to update its commitment level for the next billing period based on actual usage. Commitment levels (updated if necessary) auto-renew from billing period to billing period.

Azure DevOps

Use for Development and Testing

Customer may only access and use Azure DevOps to develop and test Customer's application(s). Only one Licensed User may access a virtual machine provided by Azure DevOps at any time.

Authorized Developer

Customer appoints Microsoft as its authorized developer with respect to Apple software included in Azure DevOps. Microsoft is responsible for complying with the terms for any such software included in Azure DevOps and will keep confidential any confidential information of Apple accessed as part of Azure DevOps.

Third Party Repository Service Access

If Customer grants Microsoft access to its third-party repository service account(s), Customer authorizes Microsoft to scan the account(s), including the contents of Customer's public and private repositories.

Azure DevTest Labs

Secrets in DevTest Labs

Azure DevTest Labs automatically creates a key vault when a user saves a secret for the first time. Customer may not use this key vault to store anything other than DevTest Lab related passwords, SSH keys, or personal access tokens.

Azure Health Bot Service

Customer Obligations

Customer is solely responsible for: (1) the accuracy and adequacy of information and Data furnished through use of the Azure Health Bot Service; (2) implementing a secure application-to-application authentication method between the Customer Health Bot Application and the Azure Health Bot Service; (3) obtaining appropriate consent from end users in connection with their use of the Customer Health Bot Application; and (4) displaying appropriate warnings, disclaimers, and acknowledgements to end users in connection with their use of the Customer Health Bot Application, including, as applicable, those set forth in the following form.

Azure Information Protection Premium

Notices

The Bing Maps Notices apply. Any deployment services provided to Customer are subject to the Professional Services Notice. (refer to Notices)

Azure Kubernetes Service on Azure Stack HCI and Azure Kubernetes Service Runtime on Windows Server

Use Rights and Conditions for Use

Customer may use Azure Kubernetes Service on Azure Stack HCI (AKS on HCI) and Azure Kubernetes Service Runtime on Windows Server (AKS on WS) (collectively, AKS) only (i) on Azure Stack HCI (with respect to AKS on HCI) or Windows Server (with respect to AKS on WS) running on servers dedicated to Customer's use and (ii) to host, manage, and service validly licensed containers running validly licensed applications.

Customer may use AKS as long as it is registered with Customer's valid Azure subscription in order to enable additional AKS functionality and to meter and invoice Customer.

Included Microsoft Applications

AKS may include other Microsoft applications. These license terms apply to those included applications, if any, unless other license terms are provided with the other Microsoft applications.

Third Party Software

AKS may include third party components with separate legal notices or governed by other agreements, as may be described in the ThirdPartyNotices file(s) accompanying AKS or within AKS itself.

License Restrictions

Customer may not work around any mandatory registration or sign-up process for AKS.

Customer Support

Any support for AKS is provided "as is", "with all faults", and without warranty of any kind.

Updates

AKS may automatically download and install updates for you. You agree to receive these automatic updates without any additional notice. Updates may not include all existing software features, services, or peripheral devices.

Azure Lab Services

While Microsoft provides Azure Lab Services to Customer, as between Customer and Microsoft, Customer is the sole provider of related services to Customer's end users and shall have sole and exclusive responsibility to end users, including any support obligations. Customer's end users are not a party to any agreement with Microsoft regarding the services.

Notification; Liability; Bar on Actions Against Microsoft

Customer will notify Microsoft promptly of any incidents that could have an impact on Microsoft such as a data breach, password issues, end user complaint(s), loss of user data, or intellectual property or privacy claims.

Customer acknowledges and agrees that Microsoft has no obligation or liability to Customer or any end user for the end user's usage of the service.

By using the service, an end user may not bring any action against Microsoft in relation to the services. If any end user does bring an action against Microsoft, the Indemnification provision in this section applies.

Indemnification

You agree to be responsible for all direct damages associated with any claim by an end user, third party, and/or regulatory authority in connection with the service provided to the end users.

End User Terms

In order to provide the services to end users, Customer must validly agree to a binding, written agreement that contain the substance of the following requirements:

Statement of Relationship: Customer is the sole provider of the services. Customer is responsible for providing any support to end users. The services will be provided by Customer to Customer's end users under your terms of use and privacy policy.

Compliance; Acceptable Use: Customer is solely responsible for ensuring compliance with all applicable laws, including, but not limited to GDPR, with respect to Customer's provision and end users' use of the service. In addition, for clarity and without limiting the Acceptable Use Policy, Customer and Customer's end users may not use Azure Lab Services to facilitate or engage in cryptocurrency mining. Violation of this prohibition may result in suspension of the service, as set forth in the Acceptable Use Policy.

Disclaimer of Warranties: Customer will disclaim any and all warranties in connection with the services, and Customer will disclaim the same with respect to Microsoft.

Limitation of Liability and Exclusion of Damages: Customer will disclaim liability and exclude damages in a way that is consistent with the provisions of any applicable agreement(s) between Customer and Microsoft.

Updates

Customer is responsible for updating the virtual machines (VMs) in Customer's portfolio. Notwithstanding the foregoing, Microsoft may, but is not obligated to, take any action it deems reasonable in its business judgment with respect to the VMs in your portfolio, including applying any updates or other changes generally applicable to the services.

Azure Machine Learning service

NVIDIA Components

Azure Machine Learning service may include NVIDIA Corporation's CUDA Toolkit, Tesla drivers, cuDNN, DIGITS, NCCL, and TensorRT (the "NVIDIA Components"), Customer agrees that its use of NVIDIA Components is governed by the NVIDIA Cloud End User License Agreement for Compute at <https://go.microsoft.com/fwlink/?linkid=874330>.

Azure Maps

Navigation restrictions

Customer may not use Azure Maps to enable turn-by-turn navigation functionality in any application.

Database restrictions

Customer may not use Azure Maps or any part thereof to create a competing database or service, or a derived database populated wholly or partially with Customer's data and/or data supplied or created by any third party.

Customer will not use the data delivered by the Azure Maps in combination with any other third-party database, except that Customer may layer onto the data of a type not already included within the Service (such as your proprietary content) or of which Microsoft otherwise licenses.

API Results

Customer may not cache or store information delivered by the Azure Maps API including but not limited to geocodes and reverse geocodes, map data tiles and route information (the "Results") for the purpose of scaling such Results to serve multiple users, or to circumvent any functionality in Azure Maps.

Caching and storing Results is permitted where the purpose of caching is to reduce latency times of Customer's application. Results may not be stored for longer than: (i) the validity period indicated in returned headers; or (ii) 6 months, whichever is the shorter. Notwithstanding the foregoing, Customer may retain continual access to geocodes as long as Customer maintains an active Azure account.

Customer may not display any Results, except geocodes and/or Azure Maps Weather service results, solely as described in these Terms, on any third-party content or geographical map database.

Mobility API

Customer may not cache nor store information delivered by the Mobility API including but not limited to Agency Information, Stop Keys and Transit Type (the "Mobility Results") for the purpose of scaling such Mobility Results to serve multiple users, or to circumvent any functionality in Azure Maps.

Caching and storing Mobility Results is permitted where the purpose of caching is to reduce latency times of Customer's application. Mobility Results may not be stored for longer than: (i) the validity period indicated in returned headers; or (ii) 6 months, whichever is shorter. Notwithstanding the foregoing, Customer may retain continual access to Stop Name, ID, and Position as long as Customer maintains an active Azure Maps account.

Map Data

Use of content displaying the TomTom copyright notice must be in accordance with restrictions set forth in the TomTom Licensing Third Party Product Terms and EULA (https://www.tomtom.com/en_GB/thirdpartyproductterms/).

Imagery Data

Azure Maps uses imagery from Microsoft Bing and Airbus. Use of imagery content is subject to the following:

- Bing Imagery is subject to the Bing Maps Notice in the [Notices](#) section.
- Airbus imagery is prohibited for customers from the following countries: Afghanistan, Belarus, Cambodia, Central African Republic, China, Cuba, Congo (Democratic Republic of), Crimea region (Ukraine), Cyprus, Eritrea, Ethiopia, Haiti, Hong Kong, Iran, Iraq, Lebanon, Libya, Myanmar (Burma), North Korea, Pakistan, Russian Federation, Saudi Arabia, Somalia, South Sudan, Sudan, Syrian Arab Republic, Turkey, Ukraine, Venezuela, and Yemen.
- For regions where access to Airbus imagery is restricted, Azure Maps will leverage imagery from other sources. Customers may not use any means to subvert the restrictions listed above and gain access to imagery content.

User region parameter

User region parameter in Azure Maps must be used in compliance with applicable laws, including those regarding mapping, of the country where maps, images and other data and third-party content that Customer is authorized to access via Azure Maps is made available.

No warranty for accuracy

Microsoft and its suppliers make no warranty that the maps, images, data or any content delivered by Azure Maps will be accurate or complete.

Copyright

Customers may not remove, obscure, mask or change any logo and/or copyright notice placed on or automatically generated by Azure Maps. In addition, customers using the Azure Maps Render V2 API must use the "Get Map Attribution service" to obtain the copyright attribution text and display it in their applications.

Azure Stack HCI

Privacy Notice

Microsoft will be a controller of Personal Data when customers turn on collection of Windows diagnostic data as described in product documentation. When Microsoft is a controller, Microsoft will handle this Personal Data in accordance with the Microsoft Privacy Statement at aka.ms/privacy, and the Data Protection Addendum terms do not apply.

Use Rights and Conditions for Use

Customer may use the Azure Stack HCI software only (i) on servers dedicated to Customer's internal use and (ii) as a host operating system to manage and service validly licensed virtual machines running validly licensed applications. Any dedicated server that is under the management or control of an entity other than Customer or one of its Affiliates is subject to the Outsourcing Software Management clause. Customer may use the Azure Stack HCI software as long as it is (i) registered with Customer's valid Azure subscription in order to enable additional Azure Stack HCI functionality and to meter and invoice Customer and (ii) connected to Customer's Azure subscription over the Internet at least once every thirty (30) consecutive calendar days.

License Restrictions

Customer may not (i) work around any mandatory registration or sign-up process for Azure Stack HCI or (ii) run any applications, operating system roles, and/or other workloads directly on the Azure Stack HCI software except for (A) utilities and operating system roles and (B) virtualized machines running Azure Stack HCI, both (A) and (B) as necessary to enable Azure Stack HCI to host, manage, and service validly licensed virtual machines running validly licensed applications.

Customer Support

Any customer support for Azure Stack HCI that may be available from Microsoft requires that Azure Stack HCI runs on server hardware that is pre-validated and listed in the Azure Stack HCI catalog or any successor.

Azure Stack Hub

Privacy Notice

Microsoft will be a controller of Personal Data when customers turn on collection of Windows diagnostic data as described in the Product documentation. When Microsoft is a controller, Microsoft will handle this Personal Data in accordance with the Microsoft Privacy Statement at aka.ms/privacy, and the Data Protection Addendum terms do not apply.

If a Microsoft Cloud Agreement or Microsoft Customer Agreement Customer uses Azure Stack Hub software or services that are hosted by a Reseller, such use will be subject to Reseller's privacy practices, which may differ from Microsoft's.

Use of Azure Stack Hub

Customer may use Azure Stack Hub only on the hardware on which it is preinstalled.

Use of the Default Provider Subscription

The subscription created for the system administrator during the Azure Stack Hub deployment process (the default provider subscription) may be used solely to deploy and manage the Azure Stack Hub infrastructure; it may not be used to run any workload that does not deploy or manage Azure Stack Hub infrastructure (e.g. it may not be used to run any application workloads).

Azure Stack Hub Plan

Customer may use Microsoft Azure Stack Hub on a Licensed Server, provided it acquires a number of SLs equal to the number of Physical Cores on that Server. Licenses are reduction eligible; however, ongoing use remains subject to the requirement to retain licenses equal to the Physical Cores on the Server.

Azure SQL Edge

IoT Device

Any IoT Device that is under the management or control of an entity other than Customer or one of its Affiliates is subject to the Outsourcing Software Management clause.

Use of Azure SQL Edge

Customer may install and use any number of copies of the Azure SQL Edge software on an IoT Device dedicated to Customer's use and to which a License is assigned. Notwithstanding anything to the contrary in Universal Terms for Online Services, Customer may reassign a License at any time to other IoT Devices dedicated to its use. If Customer installs any features or functionalities other than the Azure SQL Edge software (whether derived from Microsoft or third party software) on the IoT Device, then those other features or functionalities may be used only to support the IoT Program.

The terms of the DPA do not apply to Azure SQL Edge installed on Customer's IoT Device, except to the extent any Personal Data is collected to enable Azure management services and to meter usage for billing purposes, because the operating environment of such IoT Devices is not under Microsoft's control.

Azure Virtual Desktop Per User Access

Definitions

"End User" means a third-party individual that acquires Azure Virtual Desktop Customer Solution from Customer for End User's own internal use (without the right to resell or redistribute it).

"Azure Virtual Desktop Customer Solution" means an application or any set of applications that adds primary and significant functionality to the Azure Virtual Desktop.

Use Rights

Azure Virtual Desktop per user access licenses are only available for Customer's external commercial purposes to serve Azure Virtual Desktop Customer Solutions to third parties on Azure. Customer may not use the licenses acquired under this model for internal purposes. Customer may assign no more than one million user identities licensed under this model to its Azure Virtual Desktop session hosts.

To access Azure Virtual Desktop for internal business purposes Customer may acquire select Windows Enterprise and Microsoft 365 licenses. Please see the relevant product sections for more details.

End User Entitlements

End Users may connect to up to five Azure Virtual Desktop session hosts at once.

Hosting Entitlement

The General Service Terms Azure Customer Solution clause does not apply. Notwithstanding the general restrictions in Customer's agreement that preclude reselling, redistributing, or using the Products to offer commercial hosting services to third parties, Customer may, subject to the conditions set forth below:

Combine Azure Virtual Desktop per user access licenses with applications owned or licensed by Customer or a third party to create an Azure Virtual Desktop Customer Solution solely for use on Microsoft Azure, and permit End Users to access and use Azure Virtual Desktop per user access licenses in connection with the use of that Azure Virtual Desktop Customer Solution on a rental, subscription or services basis (whether or not a fee for such use is paid).

Additional Terms

Indemnification. You agree to be responsible for all direct damages associated with any claim by an end user, third party, and/or regulatory authority in connection with the service provided to the end users.

Support. Microsoft is not obligated to provide support services to Customer or its End Users in connection with the Azure Virtual Desktop Customer Solution. Customer alone is responsible for providing technical support to End Users for all aspects and components of the Azure Virtual Desktop Customer Solution, either itself or by obtaining and continuously maintaining support for its End Users through Microsoft or a third party. Customer must inform End Users of this fact. Any support from Microsoft for questions or issues that arise as part of Customer's support of the Azure Virtual Desktop Customer Solution must be obtained under a separate support services agreement.

END USER AGREEMENT REQUIREMENTS

Company must:

- Notify each End User before or at the time of purchase (in the appropriate language versions for the locations in which Company will deliver the Azure Virtual Desktop Customer Solution) that the Azure Virtual Desktop Customer Solution contains Microsoft technology that is subject to certain license terms and that the End User must agree to the license terms before using the Product.
- Include the following acknowledgment in the credit screen or about screen and documentation of any Azure Virtual Desktop Customer Solution: "© Copyright 2021 Microsoft Corporation. All rights reserved."
-

TERMS AND CONDITIONS REGARDING USE OF MICROSOFT SOFTWARE & ONLINE SERVICES

This document governs the use of software and online services ("Software Services") that [insert Service Provider's name] ("Service Provider") provides to you on a rental, subscription or services basis, and that include Microsoft software and online services ("Microsoft Products"). Service Provider does not own the Microsoft Products and the use thereof is subject to certain rights and limitations of which Service Provider must inform you. Your right to use the Microsoft Products is subject to the terms of your agreement with Service Provider, and to your understanding of, compliance with, and consent to the following terms and conditions, which Service Provider does not have authority to vary, alter, or amend.

- **OWNERSHIP OF MICROSOFT PRODUCTS.** The Microsoft Products are licensed to Service Provider from an affiliate of the Microsoft Corporation (collectively "Microsoft"). Microsoft Products are protected by copyright and other intellectual property rights. Microsoft Products and related elements including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Microsoft Products are owned by Microsoft or its suppliers. You may not remove, modify or obscure any copyright trademark or other proprietary rights notices that are contained in or on the Microsoft Products. The Microsoft Products are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Your possession, access, or use of the Microsoft Products does not transfer any ownership of the Microsoft Products or any intellectual property rights to you.
- **USE OF SOFTWARE SERVICES.** You may use the Software Services only in accordance with your agreement with Service Provider and these terms. These terms permanently and irrevocably supersede the terms of any Microsoft End User License Agreement that may be presented in electronic form during the installation and/or use of the Software Services.
- **COPIES.** You may not make any copies of the Products.
- **LIMITATIONS ON REVERSE ENGINEERING, DECOMPILE AND DISASSEMBLY.** You may not reverse engineer, decompile, or disassemble the Products, except and only to the extent that applicable law, notwithstanding this limitation, expressly permits such activity.
- **NO RENTAL.** You may not rent, lease, lend, pledge, or directly or indirectly transfer or distribute the Products to any third party, and may not permit any third party to have access to and/or use the functionality of the Products except for the sole purpose of accessing the functionality of the Products in the form of Software Services in accordance with the terms of this agreement and any agreement between you and Service Provider.
- **TERMINATION.** Without prejudice to any other rights, Service Provider may terminate your rights to use the Products in accordance with the **Disputes Clause (Contract Disputes Act)** if you fail to comply with these terms and conditions. In the event of termination or cancellation of your agreement with Service Provider or Service Provider's agreement with Microsoft under which the Products are licensed, you must stop using and/or accessing the Products, and destroy all copies of the Products and all of their component parts within thirty (30) days of the termination of your agreement with Service Provider.
- **NO WARRANTIES, LIABILITIES OR REMEDIES BY MICROSOFT.** Microsoft disclaims, to the extent permitted by applicable law, all warranties and liability for damages by Microsoft or its suppliers for any damages and remedies whether direct, indirect or consequential, arising from the Software Services. Any warranties and liabilities are provided solely by Service Provider and not by Microsoft, its affiliates or subsidiaries.
- **PRODUCT SUPPORT.** Any support for the Software Services is provided to you by Service Provider or a third party on Service Provider's behalf and is not provided by Microsoft, its suppliers, affiliates or subsidiaries.
- **NOT FAULT TOLERANT.** The Products are not fault-tolerant and are not guaranteed to be error free or to operate uninterrupted. You must not use the Products in any application or situation where the Product(s) failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage ("High Risk Use").
- **EXPORT RESTRICTIONS.** The Products are subject to U.S. export jurisdiction. You must comply with all applicable laws including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. For additional information, see <http://www.microsoft.com/exporting/>.

- **LIABILITY FOR BREACH.** In addition to any liability you may have to the Service Provider, Customer agrees that Customer will also be legally responsible directly to Microsoft for any breach of these terms and conditions.
- **INFORMATION DISCLOSURE.** You must permit Service Provider to disclose any information requested by Microsoft under the Service Provider's Agreement. Microsoft will be an intended third-party beneficiary of your agreement with Service Provider, with the right to enforce provisions of your agreement with Service Provider and to verify your compliance.
- **PRIVACY AND DATA PROTECTION.** The Software Service will be provided by Service Provider you under its privacy policy.

Azure VMware Solution

Professional Services Data Transfer to VMware

If customer contacts Microsoft for technical support relating to Azure VMware Solution and Microsoft must engage VMware for assistance with the issue, Microsoft will transfer the Professional Services Data and the Personal Data contained in the support case to VMware. The transfer is made subject to the terms of the Support Transfer Agreement between VMware and Microsoft, which establishes Microsoft and VMware as independent processors of the Professional Services Data. Before any transfer of Professional Services Data to VMware will occur, Microsoft will obtain and record consent from customer for the transfer.

VMware Data Processing Agreement

Once Professional Services Data is transferred to VMware (pursuant to the above section), the processing of Professional Services Data, including the Personal Data contained the support case, by VMware as an independent processor will be governed by the VMware Data Processing Agreement for Microsoft AVS Customers Transferred for L3 Support ([https://rc.portal.azure.com/verifyLink?href=https%3A%2F%2Fwww.vmware.com%2Fvmware-dpa-for-avs-customers.html&id=Microsoft Azure Marketplace](https://rc.portal.azure.com/verifyLink?href=https%3A%2F%2Fwww.vmware.com%2Fvmware-dpa-for-avs-customers.html&id=Microsoft%20Azure%20Marketplace)). Customer also gives authorization to allow its representative(s) who request technical support for Azure VMware Solution to provide consent on its behalf to Microsoft for the transfer of the Professional Services Data to VMware.

Deployment and Usage Information

Customer authorizes Microsoft to share with VMware its status as a customer of Azure VMware Solution and associated Azure VMware Solution deployment and usage information.

Cognitive Services and Applied AI Services

For the purposes of this section, "Services" means collectively Cognitive Services and Applied AI Services.

Product documentation

Microsoft may provide technical documentation regarding the appropriate operation applicable to the Services (including the applicable developer guides), which is made available online by Microsoft and updated from time to time. Customer acknowledges and agrees that it has reviewed this documentation and will use the Services in accordance with such documentation, as applicable.

Some Services are intended to process Customer Data that includes Biometric Data (as may be further described in product documentation) which Customer may incorporate into its own systems used for personal identification or other purposes. Customer acknowledges and agrees that it is responsible for complying with the Biometric Data obligations contained in the Online Services DPA (<https://aka.ms/DPA>).

Limit on Customer use of service output

Customer will not, and will not allow third parties to use the Services or data from the Services to create, train, or improve (directly or indirectly) a similar or competing product or service.

Limited Access Services

Certain Services may require registration and limit access based on Microsoft's eligibility and use criteria ("Limited Access Services"). Customer agrees that it will only use the Services for the uses specified in its registration form and/or in its Enrollment or agreement and in accordance with relevant service terms. Microsoft may require Customer to re-verify the information submitted to Microsoft regarding the Limited Access Services remains accurate, complete and up to date; and is using the Limited Access Services in accordance with information submitted and these terms. Microsoft may suspend or terminate Customer's access to these Limited Access Services for non-compliance, only to the extent reasonably necessary. Customer shall respond to requests for re-verification from Microsoft within ten business days of receiving a request (requests may be provided via self- certification Azure tools). If Microsoft

needs additional information to assure compliance with these terms, Customer will reasonably cooperate with Microsoft to provide such information within 30 business days of request. To apply for access and use of Limited Access Services, Customer must provide current, complete, and accurate information in the registration form and any re-verification requests from Microsoft.

Customized TTS Services and use of Synthetic Voices

Permissions. Customer represents, warrants and certifies that (i) it has explicit written permission from the voice owner(s) contained within its audio files ("Voice Talent") to use their personal data, including his/her voice likeness to create voice model(s) ("Synthetic Voice(s)"), (ii) Customer's agreement(s) contemplate the duration of use of the Synthetic Voice and any content limitations and (iii) Customer has shared Microsoft's disclosure guidance for voice talent (<https://aka.ms/disclosure-voice-talent>) with Voice Talent directly or through Voice Talent's authorized representative that describes how synthetic voices are developed and operate in conjunction with text to speech services. Microsoft reserves the right to require Customer to provide audio files containing acknowledgements by Voice Talent(s). Customer acknowledges and agrees that Microsoft may use this to perform speaker verification against Customer's audio training files; however, Microsoft's retention of audio files does not create or imply an obligation that Microsoft will perform speaker verification.

Permitted uses. In addition to compliance with the Acceptable Use Policy, the code of conduct (available at <https://aka.ms/custom-neural-code-of-conduct>) sets the minimum requirements that all TTS implementations must adhere to in good faith. Customer shall have the exclusive right to use the Synthetic Voice(s) created by Customer and made available through use of the Services. Notwithstanding the foregoing or anything to the contrary in the DPA, Customer acknowledges and agrees that Microsoft may retain a copy of each Synthetic Voice created by Customer and may, but is not obligated to, use the Synthetic Voice(s) to investigate and respond to any alleged violations of the service terms. Customer agrees and grants Microsoft a limited nonexclusive irrevocable worldwide license to retain acknowledgment audio voice consent file(s) and a copy of the Synthetic Voice(s) for the limited purposes above. Customer is required to secure and maintain all rights necessary for Microsoft to retain and use the acknowledgment audio files and Synthetic Voice(s) as described in this section without violating the rights of Voice Talent(s) or any other third party or otherwise obligating Microsoft to Customer, Voice Talent or any other third party. This paragraph will survive termination or expiration of Customer's agreement.

Microsoft Translator Attribution

When displaying automatic translations performed by Microsoft Translator, Customer will provide reasonably prominent notice that the text has been automatically translated by Microsoft Translator.

Services in Containers

Services features that are available in containers are designed to connect to a billing endpoint. The containers and the billing endpoint are licensed to Customer under this agreement as Online Services, and the containers are also subject to the terms for Use of Software with the Online Service in this agreement. Customer must configure the containers it uses to communicate with the billing endpoint so that the billing endpoint meters all use of those containers. Provided Customer enables such metering and subject to any applicable transaction limits, Customer may install and use any number of containers (1) on Customer's hardware devices that are dedicated to Customer's exclusive use, and (2) in Customer's Microsoft Azure Service accounts. Any dedicated hardware that is under the management or control of an entity other than Customer or one of its Affiliates is subject to the Outsourcing Software Management clause of the [Universal License Terms for All Software](#).

The containers include material that is confidential and proprietary to Microsoft. Customer agrees to keep that material confidential and to promptly notify Microsoft if Customer becomes aware of any possible misappropriation or misuse.

The terms of the [DPA](#) do not apply to containers installed on Customer's dedicated hardware, except to the extent a) any Personal Data is collected in connection with the billing endpoint, or b) custom model training is required prior to download of the Service operating in the container, because the operating environment of those containers is not under Microsoft's control.

Inactive Services Configurations and Custom Models

For the purposes of data retention and deletion, a Services configuration or custom model that has been inactive may at Microsoft's discretion be treated as an Online Service for which the Customer's subscription has expired. A configuration or custom model is inactive if for 90 days (1) no calls are made to it; (2) it has not been modified and does not have a current key assigned to it and; (3) Customer has not signed in to it.

Express Route Global Reach

Express Route Global Reach is an Azure Service offering data transport capabilities to Express Route users in certain locations. Express Route Global Reach is provided by the Microsoft Affiliate authorized in a given country to administer it. Pricing for Express Route Global Reach may include applicable taxes and fees. Express Route Global Reach terms may vary from country to country. All included taxes, fees and country-specific terms of use are disclosed in the terms of use available at <https://aka.ms/CommunicationServicesTerms>.

Extended Use Rights for Microsoft Defender for Identity Customers

Customer may also install and use Advanced Threat Analytics locally to manage client OSEs (or Server OSEs used as client OSEs) that are used solely by users to whom licenses are assigned. This right expires when Customer's subscription expires.

Microsoft Azure StorSimple Plan Offerings

For each StorSimple Plan with Device purchased, Customer will receive a Storage Array device. Geographic availability and the terms and conditions governing the Storage Array, including warranty, shipping and handling, and duties, are set forth in the Storage Array and Azure Data Box Terms. Each StorSimple Plan purchased by Customer will be associated with a single Storage Array; any additional Storage Arrays used by Customer will be billed at Consumption Rates. Microsoft Azure StorSimple 8100 and 8600 plans can be reduced at the next anniversary following 12 months of continuous usage.

Microsoft Genomics

Microsoft Genomics Privacy

The Microsoft Privacy Statement located at <https://aka.ms/privacy> and attached hereto applies to Customer's use of Microsoft Genomics, except that this Microsoft Genomics section controls to the extent it conflicts with the Microsoft Privacy Statement.

Broad License Terms

Microsoft Genomics includes access to the Genetic Analysis Toolkit (GATK) from the Broad Institute, Inc. ("Broad"). Use of the GATK and any related documentation as part of Microsoft Genomics is also subject to Broad's GATK End User License Agreement ("Broad EULA" located here <https://software.broadinstitute.org/gatk/eula/index?p=Azure>).

Microsoft may collect and share with Broad certain statistical and technical information regarding Customer's usage of the GATK. Customer authorizes Microsoft to report to Broad Customer's status as a user of the GATK in Microsoft Genomics.

No Medical Use

Microsoft Genomics is not a medical device and outputs generated from its use are not intended to be statements of fact, nor are they to be used as a substitute for medical judgment, advice, diagnosis or treatment of any disease or condition.

Multi-Cloud Scanning Connectors for Azure Purview

To enable interoperability with Customer's deployments with other cloud providers, Microsoft may operate within such other clouds certain optional, discrete data scanner functionality for Customer's data hosted in such other clouds (the "Multi-Cloud Scanning Connectors for Azure Purview"). Microsoft will disclose in its documentation how Customer may enable and use the Multi-Cloud Scanning Connectors for Azure Purview. For clarity, the Multi-Cloud Scanning Connectors for Azure Purview is a separate add-on to Azure Purview. The Multi-Cloud Scanning Connectors for Azure Purview is not a Microsoft Azure Core Service and the following sections of the DPA do not apply to the Multi-Cloud Scanning Connectors for Azure Purview: "Educational Institutions", "CJIS Customer Agreement", "HIPAA Business", and "Appendix A - Security Measures".

With respect solely to the Multi-Cloud Scanning Connectors for Azure Purview, the following modifications to the DPA apply:

- Data Access: Microsoft employs least privilege access mechanisms to control access to Customer Data (including any Personal Data therein). Microsoft employs role-based access controls to ensure that Microsoft's access to Customer Data required for service operations is for an appropriate purpose and approved with management oversight.
- Auditing Compliance: Microsoft's commitments in the Auditing Compliance section of the DPA do not extend to third-party computers, computing environments or physical data centers used by the Multi-Cloud Scanning Connectors for Azure Purview.

Standard data protection terms offered by those other cloud providers govern your use of the Multi-Cloud Scanning Connectors for Azure Purview while the add-on is hosted in such other clouds.

Visual Studio App Center

Visual Studio App Center Test Privacy and Security Terms

The privacy statement located at <https://aka.ms/actestprivacypolicy> applies to Customer's use of Visual Studio App Center Test. Customer may not use Visual Studio App Center Test to store or process Personal Data. Please refer to the Product documentation for more information.

Use for Development and Testing

Customer may only access and use Visual Studio App Center to develop and test Customer's application(s). Only one Licensed User may access a virtual machine provided by Visual Studio App Center at any time.

Authorized Developer

Customer appoints Microsoft as its authorized developer with respect to Apple software included in Visual Studio App Center. Microsoft is responsible for complying with the terms for any such software included in Visual Studio App Center and will keep confidential any confidential information of Apple accessed as part of Visual Studio App Center.

Third Party Repository Service Access

If Customer grants Microsoft access to its third-party repository service account(s), Customer authorizes Microsoft to scan the account(s), including the contents of Customer's public and private repositories.

Add-ons

Customer may acquire Add-ons subject to the following conditions:

1. Customer must have active SA or an active User SL for the corresponding Qualifying Licenses
2. Customer may acquire one Add-on SL for each Qualifying License(s), unless provided otherwise in these terms
3. Customer may acquire add-on SLs between true-up dates in advance of the acquisition of the Qualifying Licenses

Add-ons expire upon the earlier of the expiration of the SA coverage for the Qualifying License or the Add-on SL term, unless provided otherwise in these terms. Add-ons may only be reassigned to users or devices with Qualifying Licenses.

Microsoft Azure User Plans

Qualifying License(s)	Add-on User Subscription License(s)
Enterprise CAL Suite	Azure Information Protection Premium Plan 1 Add-on (User SL)
Advanced Threat Analytics 2016 Client Management License per User	Microsoft Defender for Identity Client Management License Add-on (User SL)

Microsoft Power Platform

Availability

Product	Program Attribute
AI Builder capacity add-on	
Dataverse Database Capacity	
Dataverse File Capacity	
Dataverse Log Capacity	
Power Apps Per App	
Power Apps per app plan	
Power Apps plan (User SL)	
Power Apps portals login capacity add-on	
Power Apps portals page view capacity add-on	

Microsoft Product Terms (English, Jun 01 2022, MCA)

41

Power Automate per flow plan	
Power Automate per user (User SL)	
Power Automate per user with attended RPA plan (User SL)	
Power Automate unattended RPA Add-on (SL)	
Power BI Premium (User SL)	
Power BI Premium Add-On (User SL)	
Power BI Premium P1	
Power BI Premium P2	
Power BI Premium P3	
Power BI Premium P4	
Power BI Premium P5	
Power BI Pro	
Power Platform Requests add-on	
Power Virtual Agents	

Product Conditions - General	
Terms of Service	Universal License Terms for all Online Services
Product Pool	Server
Promotions	None

Power BI Report Server – Running Instances

For each Microsoft Power BI Premium P subscription license, Customer may run any number of [Instances](#) of the Power BI Report Server software in a [Physical OSE](#) or [Virtual OSE](#) on a Server dedicated to Customer's user or a [Virtual OSE](#) on shared servers on Microsoft Azure Services only. Dedicated [Servers](#) used for this purpose, that are under the management or control of an entity other than Customer or one of its Affiliates, are subject to the [Outsourcing Software Management](#) clause. Customer may run the Power BI Report Server software in a Physical or [Virtual OSE](#) with up to the number of cores included under its Power BI Premium P plan. If any [Virtual Core](#) is at any time mapped to more than one Hardware Thread, Customer needs an additional subscription license for each additional [Hardware Thread](#) mapped to that [Virtual Core](#).

Power BI Report Server - Sharing Content

A Power BI Pro User SL is required to publish shared Power BI reports using the Power BI Report Server.

SQL Server Technology

Customer may run any number of [Instances](#) of any SQL Server database software (SQL Server Standard) included in Power BI Report Server in one [OSE](#) on a [Server](#) dedicated to Customer's use for the limited purpose of supporting Power BI Report Server and any other product that includes SQL Server database software. Dedicated [Servers](#) used for this purpose, that are under the management or control of an entity other than Customer or one of its Affiliates, are subject to the [Outsourcing Software Management](#) clause.

Azure availability

Certain Power Platform services may be available for purchase as an Azure meter which allows customers to pay as you go for certain services as outlined in the [Azure Purchasing Services and the Azure Payment and Fees sections](#). The individual licensing terms for these products are applicable for these Power Platform services, in addition to the [Azure Purchasing Services and the Azure Payment and Fees sections](#).

Professional Direct Support

Customer must acquire enough Professional Direct Support licenses to cover each Dynamics 365 and Power Platform license on its agreement, up to a maximum of 250 licenses.

License Prerequisites

User License	User License Prerequisites
Power Automate unattended RPA add-on	Power Automate per user with attended RPA plan, or

Microsoft Product Terms (English, Jun 01 2022, MCA)

42

User License	User License Prerequisites
	Power Automate per flow plan
Power BI Premium Add-On	Power BI Pro, or Microsoft 365 A5/E5, or Office 365 A5/E5

Purchasing Minimums - All Programs

Purchases of the following products require a minimum purchase of the Licenses listed in the table below. These minimums must be maintained through the term of the customers Agreement or Enrollment:

Product	Minimum QTY
Power Apps portals login capacity add-on	Tier 1: 1 Tier 2: 10 Tier 3: 50
Power Apps plan (2000 Seat Minimum) (User SL)	2000
Power Automate per flow plan	5
Professional Direct Support	20 (250 maximum - once met, all remaining users are covered with no additional licenses required)

Power Apps Portals – Extended Use rights

Purchases of the following products provide internal users the use rights for Power Apps Portals

Product	Custom Power Apps Portals use rights
Dynamics 365 Enterprise license ¹	Power Apps Portals that map to licensed Dynamics 365 application context and, Power Apps Portals that map to the same environment as the licensed Dynamics 365 application
Power Apps per app	1 Power Apps portal
Power Apps per user	Unlimited Power Apps portals

¹Dynamics 365 Sales Enterprise, Dynamics 365 Customer Service Enterprise, Dynamics 365 Field Service, Dynamics 365 Project Operations, Dynamics 365 Finance, Dynamics 365 Supply Chain Management, Dynamics 365 Commerce, Dynamics 365 Human Resources, Dynamics 365 Business Central.

Prerequisites for Power Apps and Power Automate capacity add-on

Purchases of Power Apps and Power Automate capacity add-on require an underlying license purchase of Power Apps, Power Automate, Office/Microsoft 365, or Dynamics 365 licenses.

Service Specific Terms

Notices

The Bing Maps, H.264/AVC Visual Standard, VC-1 Video Standard, MPEG-4 Part 2 Visual Standard, and MPEG-2 Video Standard Notices apply. (refer to [Notices](#))

Inactive Dataverse Instances provided with Microsoft 365 licenses

If a Customer allows its Dataverse instance that is provided with Microsoft 365 licenses to go inactive, Microsoft may, at its discretion, disable the inactive instance and delete the Customer Data and Personal Data within it. Such Dataverse instance is inactive if for 90 days 1) no user logged into the instance, 2) no apps, bots, reports or flows have accessed the data contained in the instance, 3) no new apps, bots, reports, or flows were installed on or imported into the instance, and 4) no other actions or activities are registered in this instance through API or background processing jobs.

Microsoft Power BI

Definitions

"Customer Application" means an application or any set of applications that adds primary and significant functionality to the Embedded Capabilities and that is not primarily a substitute for any portion of Microsoft Power BI services.

"Embedded Capabilities" means the Power BI APIs and embedded views for use by an application.

Hosting Exception for Embedded Capabilities

Customer may create and maintain a Customer Application and, despite anything to the contrary in Customer's volume licensing agreement, combine Embedded Capabilities with Customer Data owned or licensed by Customer or a third party, to create a Customer Application using the Embedded Capabilities and the Customer Data together. Any Power BI content accessed by the Customer Application or its end users must be stored in Microsoft Power BI Premium capacity. Customer may permit third parties to access and use the Embedded Capabilities in connection with the use of that Customer Application. Customer is responsible for that use and for ensuring that these terms and the terms and conditions of Customer's volume licensing agreement are met by that use.

Limitations

Customer may not

- resell or redistribute the Microsoft Power BI services, or
- allow multiple users to directly or indirectly access any Microsoft Power BI feature that is made available on a per user basis.

Access without a User SL

A User SL is not required to view content in Power BI Premium capacity that is shared through the embed APIs or embedded views functionality. With Power BI Premium P series only, a User SL is also not required to view content in Power BI Premium capacity that is shared through the apps or email subscription features, or through Power BI Report Server.

Publish to Web

Customer may use the publish to web functionality to share content only on a publicly available website. Customer may not use this functionality to share content internally. Microsoft may display content published through the publish to web functionality on a public website or gallery.

Microsoft Power Apps

Restricted Tables

Customer may not create, modify, or delete any data from tables of the type designated as "restricted" in product documentation at <https://go.microsoft.com/fwlink/?linkid=868812>. Customer has read-only access to such restricted tables.

Non-Restricted Tables

Users with a Power Apps license may create, read, update, or delete any data from tables of the type that are not designated as "restricted" in product documentation at <https://go.microsoft.com/fwlink/?linkid=868812>.

Distributable Code

Customer may use the "Wrap" feature of Power Apps to generate a software package containing a canvas app combined with certain Power Apps mobile platform components. Customer may distribute the combined package unmodified under the terms set forth in the

Distributable Code section of the [Universal License Terms for Software](#). Customer may not disassemble the combined package or distribute any components separated from the combined package.

Updates

Customer may be required to update the package generated from the "Wrap" feature of Power Apps to ensure packages are running on a supported version of the Power Apps mobile platform. Packages running on unsupported versions may not function.

Glossary

Terms defined in this Glossary apply unless otherwise defined in product specific terms.

Definitions

Academic Program means Academic Purchasing Account on MPSA, Academic Select License, Select Plus for Academic, Campus and School Agreement, or Open Value Subscription - Education Solutions.

Add-on means a license that is purchased in addition to (and associated with) a previously acquired Qualifying License (or set of Qualifying Licenses). An Add-on license is assigned to a single Qualified User (as defined in Customer's Enrollment) or to the same Server or device as the Qualifying License(s). For any Add-on User SL not appearing individually, the license terms applicable to a full User SL for the same service apply.

Additive CAL means a CAL that must be used on conjunction with a base CAL.

Additive External Connector License means an External Connector License that must be used in conjunction with a base External Connector License.

Allocated Annual prepayment means, if Customer elects annual invoicing, the portion of the Azure prepayment allocated annually through the Enrollment term.

Authorized Outsourcer means any third party service provider that is not a Listed Provider and is not using Listed Provider as a Data Center Provider as part of the outsourcing service.

Azure Facial Recognition Services means facial recognition features or functionality included in Azure Services, such as Face; or the facial recognition functionality in Azure Video Analyzer for Media.

Azure Government Services means one or more of the services or features Microsoft makes available to Customer as Government Community Cloud Services in the "US Gov" regions identified at <http://azure.microsoft.com/en-us/regions/#services>.

Azure Prepayment means the total monetary amount a customer commits to pay during the term of the subscription for its use of eligible Microsoft Azure Services.

Azure reservations means an advanced purchase of eligible Microsoft Azure Services for a specified term and region (e.g. Reserved VM Instances, reserved capacity, etc.).

Bing Search Services means the Bing Custom Search, Bing Local Business Search, Entity Search, Image Search, News Search, Video Search, Visual Search, Web Search, Spell Check, and Autosuggest APIs, and any other APIs identified at <https://aka.ms/r1j7jq>.

Bing Search Services Data means Customer Data that are provided to Microsoft by, or on behalf of, Customer through use of the Bing Search Services.

CAL means client access license, which may be assigned by user or device, as appropriate. A user CAL allows access to corresponding version of the server software or earlier versions of the server software from any device by one user. A device CAL allows access to corresponding versions of the server software or earlier versions of the server software from one device by any user. CALs allow access to server software running on Customer's Licensed Servers only.

CAL Equivalent License means a User SL or External Connector License identified in a Product's "Server Software Access" table, or a CAL suite or SL, as identified in [CAL and ML Equivalency Licenses](#), as applicable. A CAL suite is a CAL Equivalent License only if Customer purchased the License after the Server Product's Date Available or if Customer had active SA coverage as of the Date Available.

Client OSE means an OSE running a client operating system.

Clustered HPC Application means a high performance computing applications that solves, in parallel, complex computational problems, or a set of closely related computational problems. Clustered HPC Applications divide a computationally complex problem into a set of jobs and tasks which are coordinated by a job scheduler, such as provided by Microsoft HPC Pack, or similar HPC middleware, which distributes these in parallel across one or more computers operating within an HPC cluster.

Cluster Node means a device that is dedicated to running Clustered HPC Applications or providing job scheduling services for Clustered HPC Applications.

Consumption Rates means the prices for Microsoft Azure Services or, for certain Microsoft Azure Service Plans, any usage in excess of a specified quantity. Consumption Rates may also be referred to as "Overage Rates" or "Overage" in other Microsoft or Microsoft Azure documents.

Core Factor means a numerical value associated with a specific Physical Processor for purposes of determining the number of Licenses required to license all of the Physical Cores on a Server.

Core Online Services means those Online Services listed as Core Online Services in the [Privacy & Security Terms](#) section.

Customer Data means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data.

Customer Health Bot Application means an application or any set of applications that adds primary and significant functionality to the Azure Health Bot Service and that is not primarily a substitute for the Azure Health Bot Service.

Customer Solution means any application that the Customer makes available to its end users consisting of Customer's applications and the [Microsoft Azure Services](#), whereby Customer's application adds primary and significant functionality and is not primarily a substitute to the [Microsoft Azure Services](#). Customer applications that only provide billing, license management, and/or infrastructure services (e.g., virtual machines, containers, storage, or management for such infrastructure services) do not constitute "primary and significant functionality."

Cycle Harvesting Node means a device that is not dedicated to running Clustered HPC Applications or job scheduling services for Clustered HPC Applications.

Data Center Provider means an entity that provides infrastructure or software services, directly or indirectly, to another service provider. Microsoft may also serve as a Data Center Provider through Microsoft Azure.

Data Protection Addendum (DPA) means the Microsoft Products and Services Data Protection Addendum published at <https://aka.ms/DPA>.

Education Qualified User means an employee or contractor (except Students) who accesses or uses an Education Platform Product for the benefit of the Institution.

Embedded Unified Solution means a business application developed by Customer's Reseller that the Reseller licenses to Customer that adds significant and primary functionality to an Embedded SL Product.

External Connector License means a License assigned to a Server dedicated to Customer's use that permits access to the corresponding version of the server software or earlier versions of the server software by External Users.

External Users means users that are not employees, onsite contractors or onsite agents of Customer or its Affiliates.

Fail-over OSE means an OSE (or in the context of Azure Hybrid Benefit, a SQL Server Virtual Machine) in which passive Instances of the server software are running in anticipation of a fail-over event.

Government Community Cloud (U.S. only) means Online Services that are available exclusively to the Community. Use Rights for government community cloud services are equivalent to those of their standard multitenant equivalents unless otherwise noted. Qualifying Online Services are offered as government community cloud services and non-government community cloud services. Customers may be provisioned as one or the other but not a mix of both. Online Services designated as government community cloud may not be deployed in the same domain with specific non-government community cloud services.

Graduate means a Student who has (1) completed a grade or a level in a school or an educational institution in the Organization that qualifies the Student for enrollment into college or university or (2) earned a diploma or degree from a college or university in the Organization.

Hardware Thread means either a Physical Core or a hyper-thread in a Physical Processor.

High Performance Computing (HPC) Workload means a workload where the server software is used to run a Cluster Node and is used in conjunction with other software as necessary to permit security, storage, performance enhancement and systems management on a Cluster Node for the purpose of supporting the Clustered HPC Applications.

Instance means an image of software that is created by executing the software's setup or install procedure or by duplicating an existing Instance.

IoT Device means a computing device that (i) is designed or configured for use primarily with an industry- or task-specific software program that provides the primary functionality of the computing device ("IoT Program"), (ii) uses equal to or less than 16 physical cores, and (iii) is not designed to be marketed or primarily used as a multi-functional Server, or a commercially viable substitute for a multi-functional Server.

Knowledge Worker means any employee (including a Student employee), contractor, or volunteer of or for the Institution who uses a Product or Qualified Device for the benefit of the institution or within the user's relationship with the Institution. This definition does not include users of any listed software product or online service as excluded from the definition of Knowledge Worker.

License means the right to download, install, access and use a Product.

Licensed Device means a single physical hardware system, dedicated to Customer's use, to which a License is assigned. Dedicated devices that are under the management or control of an entity other than Customer or one of its Affiliates are subject to the Outsourcing Software Management clause. For purposes of this definition, a hardware partition or blade is considered to be a separate device.

Licensed Server means a single Server, dedicated to Customer's use, to which a License is assigned. Dedicated Servers that are under the management or control of an entity other than Customer or one of its Affiliates are subject to the Outsourcing Software Management clause. For purposes of this definition, a hardware partition or blade is considered to be a separate Server.

Licensed User means the single person to whom a License is assigned.

License Mobility through Software Assurance Partner means an entity identified at <https://www.microsoft.com/en-us/licensing/licensing-programs/software-assurance-license-mobility> and authorized by Microsoft to host customers' software on shared servers.

Licensing Site means <http://www.microsoft.com/licensing/contracts> or a successor site.

Listed Providers include entities identified by Microsoft at <http://aka.ms/listedproviders>. Microsoft may identify additional Listed Providers at <http://aka.ms/listedproviders> from time to time; however, if Customer is using an outsourcer at the time its Authorized Outsourcer status is terminated, then Customer may temporarily continue to use the same entity in its former Authorized Outsourcer capacity for one year from the date of that change in status.

Management License (ML) means a License that permits management of one or more OSEs by the corresponding version of the server software or any earlier version of the server software. There are two categories of Management Licenses: Server Management License and Client Management License. There are three types of Client Management Licenses: User, OSE and device. A User Management License permits management of any OSE accessed by one user; an OSE Management License permits management of one OSE accessed by any user; a device Management License (Core CAL or Enterprise CAL Suite) permits management of any OSE on one device.

Management License Equivalent License means a User SL identified in a Product's "Management License" table, or a CAL suite or SL, as identified in CAL and ML Equivalency Licenses, as applicable. A CAL suite is a Management License Equivalent License only if Customer purchased the license after the Server Products' Date Available or if Customer had active SA coverage as the Date Available.

Managing an OSE means to solicit or receive data about, configure, or give instructions to the hardware or software that is directly or indirectly associated with the OSE. It does not include discovering the presence of a device or OSE.

Microsoft Azure Services means the Microsoft services and features identified at <http://azure.microsoft.com/services/>, except those identified in the Product Terms as Microsoft Azure Infrastructure Plans, Microsoft Azure User Plans, or Microsoft Azure Support Plans. "Microsoft Azure Services" includes any open source components incorporated by Microsoft in those services and features.

Microsoft Azure Services Plan means a subscription to one of the individual Microsoft Azure Services identified in the Product Terms as Microsoft Azure Infrastructure Plans, Microsoft Azure User Plans, or Microsoft Azure Support Plans.

Microsoft Translator means Translator Text API and/or Translator Speech API offered by Microsoft as a cloud based machine translation service.

Network Server means a physical hardware server solely dedicated to Customer use and provides resource assistant to computers in a network. Any dedicated server that is under the management or control of an entity other than Customer or one of its Affiliates is subject to the Outsourcing Software Management clause in the Universal License Terms.

Non-Microsoft Product means any third-party-branded software, data, service, website or product, unless incorporated by Microsoft in an Online Service.

Online Service means a Microsoft-hosted service to which Customer subscribes under a Microsoft volume licensing agreement, including any service identified in the Online Services section of the Product Terms. It does not include software and services provided under separate license terms (such as via gallery, marketplace, console, or dialog).

Operating System Environment (OSE) means all or part of an operating system Instance, or all or part of a virtual (or otherwise emulated) operating system Instance which enables separate machine identity (primary computer name or similar unique identifier) or separate administrative rights, and instances of applications, if any, configured to run on the operating system Instance or parts identified above. A physical hardware system can have one Physical OSE and/or one or more Virtual OSEs.

Personal Data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Physical Core means a core in a Physical Processor.

Physical OSE means an OSE that is configured to run directly on a physical hardware system. The operating system Instance used to run hardware virtualization software or to provide hardware virtualization services is considered part of the Physical OSE.

Physical Processor means a processor in a physical hardware system.

Previews means preview, beta or other pre-release features, data center locations, and services offered by Microsoft for optional evaluation.

Primary User means the user who uses a Licensed Device more than 50% of the time in any 90 day period.

Primary Workload means either an OSE in which Instances of the server software are running under the "Use Rights" section of a product entry or, in the context of Azure Hybrid Benefit rights, a SQL Server Virtual Machine.

Production Environment means any Physical or Virtual OSE running a production workload or accessing production data, or Physical OSE hosting one or more Virtual OSEs running production workloads or accessing production data.

Professional Services means Microsoft technical support services and Microsoft consulting services (e.g., for data migration) provided to Customer. "Professional Services" does not include Products.

Professional Services Data means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from a Product) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services.

Qualifying Third Party Device means a device that is not controlled, directly or indirectly, by Customer or its Affiliates (e.g., a third party's public kiosk).

Running Instance means an Instance of software that is loaded into memory and for which one or more instructions have been executed. (Customer "Runs an Instance" of software by loading it into memory and executing one or more of its instructions.) Once running, an Instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.

S&C APIs mean the following Microsoft Graph APIs: Change Notifications (aka Webhook) API, Export API, Patch API.

S&C Applications mean collectively the Security Applications and Compliance Applications.

Services Deliverables means any computer code or materials (including without limitation proofs of concept, documentation and design recommendations, sample code, software libraries, algorithms and machine learning models) other than Products or Fixes that Microsoft leaves with Customer at the conclusion of Microsoft's performance of Professional Services.

SL means subscription License that allows access to software or a hosted service for a defined period of time.

Server means a physical hardware system capable of running server software.

Server Farm means a single data center or two data centers each physically located either in time zones not more than four hours apart, or within the EU or EFTA. A data center can be moved from one Server Farm to another, but not on a short-term basis. (EU is European Union; EFTA is European Free Trade Association).

Step-up means a license purchased in addition to (and associated with) a previously acquired base license. For any Step-up User SL not appearing individually in the Product Terms, the license terms applicable to the equivalent full User SL apply.

Student means any individual enrolled in any educational institution that is part of Institution's Organization whether on a full-time or part-time basis.

Student Qualified Device means a Qualified Device owned, leased, or controlled by a Student or owned, leased, or controlled by the Organization and assigned for individual, dedicated use by a Student.

Subprocessor means other processors used by Microsoft to process data.

Virtual Core means the unit of processing power in a virtual hardware system. A Virtual Core is the virtual representation of one or more hardware threads.

Virtual OSE means an OSE that is configured to run on a virtual hardware system.

Web Workload (also referred to as "Internet Web Solutions") are publicly available web pages, websites, web applications, web services, and/or POP3 mail serving. For clarity, access to content, information, and applications served by the software within an Internet Web Solution is not limited to Customer's or its affiliates' employees. Software in Internet Web Solutions is used to run:

- web server software (for example, Microsoft Internet Information Services), and management or security agents (for example, the System Center Operations Manager agent);
- database engine software (for example, Microsoft SQL Server) solely to support Internet Web Solutions; or
- the Domain Name System (DNS) service to provide resolution of Internet names to IP addresses as long as that is not the sole function of that instance of the software.

Windows Server Container with Hyper-V isolation (formerly known as, Hyper-V Container) is a container technology in Windows Server which utilizes a virtual operating system environment to host one or more Windows Server Container(s). Each Hyper-V isolation instance used to host one or more Windows Server Container is considered one Virtual OSE.

Windows Server Container without Hyper-V isolation (formerly known as, Windows Server Container) is a feature of Windows Server software.

Windows Software Components means components of Windows software included in a Product. Microsoft .NET Framework, Microsoft Data Access Components, PowerShell software and certain .dlls related to Microsoft Build, Windows Identity Foundation, Windows Library for JavaScript, Debghelp.dll, and Web Deploy technologies are all Windows Software Components.

Attributes

Attributes are identified in the tables in each Product Entry, and indicate rights or conditions applicable to the Products.

Microsoft Product Terms (English, Jun 01 2022, MCA)

49

Additional Software: Software identified in the Use Rights for Server Products that Customer is permitted to use on any device in conjunction with its use of server software.

Add-ons and From SA: Indicates the Product is available as an Add-on, and/or From SA. For details, refer to the Add-ons and From SA sections for each respective product and online service.

Client Access Requirement: Indicates whether or not a Server Product requires CALs for access by users and devices.

Disaster Recovery: Rights available to SA customers to use software for conditional disaster recovery purposes; refer to Servers – Disaster Recovery Rights section of [Software Assurance Benefits](#).

Down Editions: Permitted lower editions corresponding to specified higher editions. Customer may use the permitted lower edition in place of a licensed higher-level edition, as permitted in the Universal License Terms.

Extended Term Eligible: Online services that are eligible for an extended term as described in the Enterprise and Enterprise Subscription licensing agreement.

External User Access Requirement: Indicates specific license requirements or options for access by External Users.

Fail-Over Rights: An SA benefit that allows Customer to run passive fail-over Instances as described in the Product entry.

Included Technologies: Indicates other Microsoft components included in a Product; refer to the Included Technologies section of Universal License Terms for details.

License Mobility: Rights available to SA customers either to reassign licenses outside the standard timelines or to use Products on multitenant servers outside their own datacenters; refer to License Mobility section of [Software Assurance Benefits](#).

License Terms: Terms and conditions governing deployment and use of a Product.

Migration Rights: Customer may be able to upgrade from prior versions of the software or other Products under special terms published in the Product Entry or Product List as indicated. Customer may also have non-standard downgrade rights to use prior versions of the same or other Products in place of the licensed version.

Notices: Identifies the notices applicable for a Product; refer to the Notices section of the Universal License Terms for details.

Online Subscription Program (OSP): The Product is available in an Online Subscription program.

Prerequisite: Indicates that certain additional conditions must be met in order to purchase Licenses for the Product.

Prerequisite (SA): Indicates that certain additional conditions must be met in order to purchase SA coverage for the Product.

Prior Version: Earlier versions of Product and their Date Available.

Product Pool: Indicates the grouping of Products that the Product belongs to for the purposes of determining pricing discounts. There are three Product pool categories; Application, Server and System.

Product-Specific License Terms, or Product-Specific Terms: Indicates the Product-specific terms and conditions governing deployment and use of the Product in the Product Terms, including those in the product specific sections of the Product Terms.

Promotions: Indicates that limited time offers apply to the Product as described in [Promotions](#).

Qualified User Exemption: Exemption applicable to users who access Products solely under one of these licenses. These users are exempt from being counted as a Qualified User under Customer's volume licensing agreement, notwithstanding anything to the contrary in that agreement.

Reduction Eligible: An Online Service for a customer that has an Enterprise Enrollment, Enterprise Subscription Enrollment, Microsoft Azure Enrollment or Enrollment for Education Solutions can report a reduction in licenses or Allocated Annual prepayment.

Reduction Eligible (SCE): Products for which a Server & Cloud Enrollment customer can report a reduction in subscription licenses or future Allocated Annual prepayment after 12 continuous months.

Roaming Rights: An SA benefit that permits the Primary User of a Licensed Device certain access and use rights. The Primary User may use a Qualifying Third Party Device to (i) remotely access and use permitted Instances or copies of the software running on Servers

dedicated to Customer's use, (ii) locally use a permitted Instance or copy in a Virtual OSE, or (iii) locally access a permitted Instance or copy of the software on a USB drive via Windows to Go, in each case solely for work-related purposes while the user is not on Customer's premises. No other user may use the software under the same License at the same time. Despite anything to the contrary in Customer's volume licensing agreement, Qualified Desktops and Devices do not include any Qualifying Third Party Devices from which Customer's users access and use the software and any (other) enterprise product solely under Roaming Rights.

SA Benefits Pool: Indicates the category of the Product for purposes of determining SA Benefits broadly applicable to that Product Pool, as listed in [Software Assurance Benefits](#).

SA Equivalent Rights: Software SLs acquired under a Server and Cloud Enrollment or Microsoft Products and Services Agreement provide the same SA rights and benefits during the term of the Subscription as Licenses with SA coverage.

Self Hosting: An SA benefit that permits use of Products for conditional hosting purposes; refer to the Servers – Self Hosted Applications section of [Software Assurance Benefits](#).

Student Use Benefit: The option for Institutions that license a qualifying Product for their Organization-wide count to license a Product for use by their Students at a ratio of 1:15 or 1:40 Students per Education Qualified User or Knowledge Worker (or staff/faculty user) at no additional cost. The qualifying Products and the Products eligible for the Student use, and the applicable ratios are identified in [Student Use Benefits and Academic Programs](#). Such Student Licenses may not be counted toward minimum order requirements. The License Terms for the Products licensed under the Student Use Benefit govern Students' use. Rights to use Products under the Student Use Benefit expire when Student is no longer affiliated with the Institution.

Suite: A Product that is comprised of components that are also licensed separately. A suite is licensed under a single License that is assigned to a single user or device, and allows use of all of its components on the single device or by a single user to which it is assigned. The components of the Suite may not be separated and used on separate devices or by separate users.

True-Up Eligible: An Online Service subscription License that an Enterprise or Enterprise Subscription customer can order via the true-up or annual order process rather than monthly.

UTD Discount: An Up to Date Discount is a discount available to Open Value Subscription customers ordering licenses for Product during the first year of their agreement if they have a License for the corresponding qualifying Product.

Cell Values

Cell Values are used in the Program Availability table in each of each Product Entry to identify how the Product is offered in each program. The volume licensing program agreements define these offering types.

A = Additional Product: The Product is offered as an Additional Product.

AF = Additional Product Faculty: The Product is offered as an Additional Product for the School program and must be licensed on an Organization-wide basis covering all Faculty and Staff.

AO = Additional Product Organization Wide: The Product is offered as an Additional Product and must be ordered organization-wide.

AP = Additional Product in EES 2017: The Product is offered as an Additional Product for the Enrollment for Education Solutions (with a publication date on or after October 2017).

AS = Additional Product School: The Product is offered as an Additional Product for the School program only.

E = Enterprise Product: The Product is offered as an Enterprise Product, but not a desktop.

ED = Education Desktop: The Product is offered as an education desktop platform product with either Enterprise CAL Suite or Core CAL Suite under Enrollment for Education Solutions (with a publication date prior to October 2017) and Open Value Subscription - Education Solutions and must be licensed on an Organization-wide basis covering all Faculty and Staff.

EO = Enterprise Online Service: The Online Service is offered as an enterprise Online Service or platform Online Service and satisfies the Enterprise Product requirements. EO for Core CAL and Enterprise CAL Suite require the corresponding CAL Suite Bridge.

EP = Education Platform Product: The Product is offered as an Education Platform Product under the Enrollment for Education Solutions (with a publication date on or after October 2017) and must be licensed on an Organization-wide basis covering all Education Qualified Users or Knowledge Workers or for the full Student Count.

Microsoft Product Terms (English, Jun 01 2022, MCA)

51

OM = Open Minimum: Each License counts solely as 5 Licenses for purposes of the initial order minimum in Open License and Open Value.

OW = Organization-wide: Available under the Organization-wide option.

P = Non-Organization Wide in Open Value: The Product is offered on a non-Organization Wide basis in Open Value.

S = Student Offering School Only: The Product is offered as a Student Offering under School Program only and must be ordered for the full Student Count.

SD = School Desktop Platform Product: The Product is offered as a school desktop platform product with either Enterprise CAL Suite or Core CAL Suite under School Program. An SD is counted as three units.

ST = Student Offering: The Product is offered as a Student Offering and must be ordered for the full Student Count.

SP = Server and Tools Product: The Product is a server and tools product offered under the Server and Cloud Enrollment.

UC = United States Government Community Cloud Service: The Online Service is offered as a Government Community Cloud (U.S. only) Service. For UC availability for Online Service suites, refer to the Program Availability table for each of the suite's components.

CAL and ML Equivalency Licenses

Rights to access server software running on Customer's Licensed Servers or to Manage OSEs are available under CAL suites and Online Services SLs. The tables below show the applicable CAL suite or SL that satisfies the License requirement for access to (or management of) the respective Server Product's base or additive functions. CAL suites must be purchased after the Product's Date Available or have active SA coverage on such date to satisfy access requirements for the current version of the Server Product.

Core CAL

	Core CAL				
Servers	Suite	Bridge O365	BridgeIntune	Bridge O365+Intune	Bridge EMS
Exchange Server 2019 Standard					
Base	X		X		X
Exchange Server 2019 Enterprise					
Base	X		X		X
SharePoint Server Subscription Edition					
Base	X		X		X
Skype for Business Server 2019					
Base	X		X		X
Windows Server 2022 Standard					
Base	X	X	X	X	
Windows Server 2022 Datacenter					
Base	X	X	X	X	
Windows MultiPoint Server 2016 Premium (Academic only)					
Base	X	X	X	X	
Microsoft Endpoint Configuration Manager (formerly, System Center Configuration Manager)					
Management	X	X			
System Center Endpoint Protection 1606					
Management	X	X			

Enterprise CAL

Microsoft Product Terms (English, Jun 01 2022, MCA)

52

Note: A license for the Enterprise CAL Suite with active SA coverage provides rights equivalent to Data Loss Prevention and Exchange Online Protection.

Enterprise CAL					
Servers	Suite	Bridge O365	BridgeIntune	Bridge O365+Intune EMS	Bridge EMS
Exchange Server 2019 Standard					
Base	X		X		X
Additive	X		X		X
Exchange Server 2019 Enterprise					
Base	X		X		X
Additive	X		X		X
SharePoint Server Subscription Edition					
Base	X		X		X
Additive	X		X		X
Microsoft Audit and Control Management Server 2013					
Base	X		X		X
Skype for Business Server 2019					
Base	X		X		X
Additive	X		X		X
Windows Server 2022 Standard					
Base	X	X	X	X	
Additive (RMS)	X	X	X	X	
Windows Server 2022 Datacenter					
Base	X	X	X	X	
Additive (RMS)	X	X	X	X	
Windows MultiPoint Server 2016 Premium (Academic only)					
Base	X	X	X	X	
Additive (RMS)	X	X	X	X	
Advanced Threat Analytics 2016					
Management	X	X		X	
Microsoft Endpoint Configuration Manager (formerly, System Center Configuration Manager)					
Management	X	X			
System Center Endpoint Protection 1606					
Management	X	X			

Enterprise Mobility + Security

Note: With the exception of Advanced Threat Analytics 2016 and Microsoft Endpoint Configuration Manager, users licensed through Student Use Benefits do not satisfy the License requirement for access to (or management of) the Products in this table.

Enterprise Mobility + Security		
Servers	E3	E5
Windows Server 2022 Standard		
Base	X	X
Additive (RMS)	X	X
Additive (MIM)	X	X
Windows Server 2022 Datacenter		
Base	X	X

	Enterprise Mobility + Security	
Servers	E3	E5
Additive (RMS)	X	X
Additive (MIM)	X	X
Windows MultiPoint Server 2016 Premium (Academic only)		
Base	X	X
Additive (RMS)	X	X
Advanced Threat Analytics 2016		
Management	X	X
Microsoft Endpoint Configuration Manager (formerly, System Center Configuration Manager)		
Management	X	X
System Center Endpoint Protection 1606		
Management	X	X
System Center Service Manager		
Management	X	X

Office 365 Enterprise

Note: Office 365 Nonprofit E1 does not satisfy the License requirement for access to (or management of) the Products in this table.

	Office 365 Enterprise		
Servers	E1	E3	E5
Exchange Server 2019 Standard			
Base	X	X	X
Additive		X	X
Exchange Server 2019 Enterprise			
Base	X	X	X
Additive		X	X
SharePoint Server Subscription Edition			
Base	X	X	X
Additive		X	X
Microsoft Audit and Control Management Server 2013			
Base		X	X
Skype for Business Server 2019			
Base	X	X	X
Additive (Enterprise)	X	X	X
Additive (Plus)			X

Office 365 Education

Note: Office 365 A1 does not satisfy the License requirement for access to (or management of) the Products in this table. Users licensed through Student Use Benefits do not satisfy the License requirement for access to (or management of) the Products in this table.

	Office 365 Education	
Servers	A3	A5
Exchange Server 2019 Standard		
Base	X	X
Additive	X	X

Microsoft Product Terms (English, Jun 01 2022, MCA)

54

	Office 365 Education	
Servers	A3	A5
Exchange Server 2019 Enterprise		
Base	X	X
Additive	X	X
SharePoint Server Subscription Edition		
Base	X	X
Additive	X	X
Microsoft Audit and Control Management Server 2013		
Base	X	X
Skype for Business Server 2019		
Base	X	X
Additive (Enterprise)	X	X
Additive (Plus)		X

Microsoft 365

	Microsoft 365		
Servers	F1/F3	E3	E5
Exchange Server 2019 Standard			
Base		X	X
Additive		X	X
Exchange Server 2019 Enterprise			
Base		X	X
Additive		X	X
SharePoint Server Subscription Edition			
Base		X	X
Additive		X	X
Microsoft Audit and Control Management Server 2013			
Base		X	X
Skype for Business Server 2019			
Base		X	X
Additive (Enterprise)		X	X
Additive (Plus)			X
Windows Server 2022 Standard			
Base	X	X	X
Additive (RMS)	X	X	X
Additive (MIM)	X	X	X
Windows Server 2022 Datacenter			
Base	X	X	X
Additive (RMS)	X	X	X
Additive (MIM)	X	X	X
Advanced Threat Analytics 2016			
Management	X	X	X
Microsoft Endpoint Configuration Manager (formerly, System Center Configuration Manager)			
Management	X	X	X
System Center Endpoint Protection 1606			

Microsoft Product Terms (English, Jun 01 2022, MCA)

55

	Microsoft 365		
Servers	F1/F3	E3	E5
Management	X	X	X
System Center Service Manager			
Management	X	X	X

Microsoft 365 Education

Note: Microsoft 365 A1 does not satisfy the License requirement for access to (or management of) the Products in this table. With the exception of Advanced Threat Analytics 2016 and Microsoft Endpoint Configuration Manager, users licensed through Student Use Benefits do not satisfy the License requirement for access to (or management of) the Products in this table.

	Microsoft 365		
Servers	A3 with Core CAL	A3	A5
Exchange Server 2019 Standard			
Base	X	X	X
Additive		X	X
Exchange Server 2019 Enterprise			
Base	X	X	X
Additive		X	X
SharePoint Server Subscription Edition			
Base	X	X	X
Additive		X	X
Microsoft Audit and Control Management Server 2013			
Base		X	X
Skype for Business Server 2019			
Base	X	X	X
Additive (Enterprise)		X	X
Additive (Plus)			X
Windows Server 2022 Standard			
Base	X	X	X
Additive (RMS)		X	X
Additive (MIM)		X	X
Windows Server 2022 Datacenter			
Base	X	X	X
Additive (RMS)		X	X
Additive (MIM)		X	X
Windows MultiPoint Server 2016 Premium (Academic only)			
Base	X	X	X
Additive (RMS)		X	X
Advanced Threat Analytics 2016			
Management	X	X	X
Microsoft Endpoint Configuration Manager (formerly, System Center Configuration Manager)			
Management	X	X	X
System Center Endpoint Protection 1606			
Management	X	X	X
System Center Service Manager			

	Microsoft 365		
Servers	A3 with Core CAL	A3	A5
Management		X	X

Notices

Bing Maps

The Online Service or its included software includes use of Bing Maps. Any content provided through Bing Maps, including geocodes, can only be used within the product through which the content is provided. Customer's use of Bing Maps is governed by the Bing Maps End User Terms of Use available at go.microsoft.com/?linkid=9710837 and the Microsoft Privacy Statement available at go.microsoft.com/fwlink/?LinkID=248686.

Notice about Azure Media Services H.265/HEVC Encoding

Customer must obtain its own patent license(s) from any third party H.265/HEVC patent pools or rights holders before using Azure Media Services to encode or decode H.265/HEVC media.

Notice about Adobe Flash Player

The software may include a version of Adobe Flash Player. Customer agrees that its use of the Adobe Flash Player is governed by the license terms for Adobe Systems Incorporated at <http://go.microsoft.com/fwlink/?linkid=248532>. Adobe and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Notice about H.264/AVC Video Standard, VC-1 Video Standard and MPEG-4 Visual Standard

This software may include H.264/AVC, VC-1, and MPEG-4 Visual technology. MPEG LA, L.L.C. requires this notice:

THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1 AND THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE (VIDEO STANDARDS) AND/OR (ii) DECODE AVC, VC-1 AND MPEG-4 VISUAL VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. REFER TO www.mpegla.com.

For clarification purposes, this notice does not limit or inhibit the use of the software for normal business uses that are personal to that business which do not include (i) redistribution of the software to third parties, or (ii) creation of content compliant with the VIDEO STANDARDS technologies for distribution to third parties.

NVIDIA Components

The software may include components of NVIDIA Corporation's CUDA Toolkit, NVIDIA drivers, CUDA Deep Neural Network Library (cuDNN), NVIDIA Collective Communications Library (NCCL), and NVIDIA TensorRT ("NVIDIA Components"). Customer agrees that its use NVIDIA Components in the software is governed by the following NVIDIA license terms, as applicable: for NVIDIA CUDA Toolkit, <https://docs.nvidia.com/cuda/eula/index.html>; for NVIDIA drivers, <https://www.nvidia.com/content/DriverDownload-March2009/licence.php?lang=us>; for cuDNN it is <http://docs.nvidia.com/deeplearning/sdk/cudnn-sla/index.html>; for NCCL it is <http://docs.nvidia.com/deeplearning/sdk/nccl-sla/index.html>; and for TensorRT it is <https://docs.nvidia.com/deeplearning/sdk/tensorrt-sla/index.html>. As stated in their respective license terms, Customer acknowledges that certain NVIDIA Components as delivered are not tested or certified by NVIDIA for use in connection with the design, construction, maintenance, and/or operation of Critical Applications, that is systems where the use or failure of such system could result in a situation that threatens the safety of human life or results in catastrophic damages. Neither Microsoft nor NVIDIA shall be liable to Customer or any third party, in whole or in part, for any claims or damages arising from Critical Applications uses. Customer agrees to indemnify NVIDIA against all claims, damages, and costs arising from Critical Application uses as stated in the applicable NVIDIA terms. Customer is solely responsible for ensuring that any product or

service developed with the NVIDIA Components as a whole includes sufficient features to comply with all applicable legal and regulatory standards and requirements.

Program Agreement Supplemental Terms

The terms and conditions below apply to Customer's volume licensing agreement, as noted.

Supplemental Terms for Microsoft Customer Agreement

Online Services Renewal for Microsoft Customer Agreement

Online Services. Online services subscriptions for government and academic customers will not be automatically renewed unless there is an active funded order and Customer chooses the auto-renewal option.

Reserved

Coterminosity for Microsoft Customer Agreement

Coterminosity allows a Customer to align the end date (or anniversary date for a multi-year subscription) of a new subscription to an existing subscription. Coterminous subscriptions must all belong to the same Customer. Coterminated end dates can be applied to monthly, annual, and three-year term subscriptions, however, new annual and three-year term subscriptions may not be coterminated with an existing monthly subscription. Charges for the first term of each coterminated subscription will be prorated based on the number of months in the initial term.

Coterminosity may not be applied to third-party, Azure, or trial subscriptions. The coterminosity option does not apply when adding a seat to a current subscription, upgrading a seat to a new or existing subscription, mid-term adjustment of subscription durations, or adjustment of subscription end dates after coterminosity is turned on.

Definition of Management for Qualified Devices

If Customer's volume licensing agreement refers to the Product Terms, the Product List, or the PUR for defining managed Qualified Devices, the following terms apply. Customer "manages" any device on which it directly or indirectly controls one or more operating system environments. For example, Customer manages any device:

- it allows to join its domain, or
- it authenticates as a requirement to use applications while on its premises, or
- it installs agents on (e.g., anti-virus, antimalware or other agents mandated by the Customer's policy), or
- to which it directly or indirectly applies and enforces group policies, or
- on which it solicits or receives data about, and, configures, or gives instructions to hardware or software that is directly or indirectly associated with an operating system environment, or
- it allows to access a virtual desktop infrastructure (VDI) outside of Windows SA, Microsoft Intune (Device) or Windows Virtual Desktop Access Roaming Rights.

A device that accesses a VDI under Roaming Rights only or utilizes Windows To Go on a Qualifying Third Party Device off the Customer's premises only, and is not managed for other purposes as described here, is not considered "managed" for purposes of this definition.

Storage Array, Azure Data Box, Azure Stack Edge, and Azure Stack Hub Ruggedized Terms

This section includes the additional or alternative terms that apply to hardware Products that are identified below. If there is a conflict between the provisions of this section and that of the Product Terms, this section shall govern and control for that hardware Product. Note: any fees related to devices in this section will be proposed and invoiced as Other Direct Costs (ODCs).

Storage Array Terms

Availability

The Storage Array is available for delivery in the following geographies only: Argentina, Australia, Austria, Bahrain, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Egypt, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Kazakhstan, Kenya, Kuwait, Lebanon, Liechtenstein, Macau, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Nigeria, Norway, Pakistan, Peru, Philippines, Poland, Portugal, Puerto Rico, Qatar, Romania, Russia, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, South Korea, Sri Lanka, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Arab Emirates, Ukraine, United Kingdom, United States, Vietnam.

Shipment and Title

Shipping terms for orders placed are: (i) FCA (Incoterms 2010) Supplier Shipping dock; (ii) Microsoft will pre-pay and invoice freight to Customer; and (iii) for shipments outside the United States, Customer is responsible for clearing the goods for import and paying all import costs including duties, taxes, and other clearance charges. Microsoft will supply the Storage Array to the Customer on a No Charge basis and title for the Storage Array and the risk of loss will pass to Customer upon delivery to the carrier and completion of export formalities at the point of origin. All scheduled shipment dates are estimates only. The Storage Array will be shipped to the address provided by Customer using the StorSimple online form (provided separately). For US transactions, Microsoft has remitted sales tax on the value of the Storage Array(s) based upon the ship-to address provided by Customer for the delivery of the Storage Array(s). For US and Canada transactions, the address used for the shipment of the Storage Array(s) is used strictly for purposes of shipping the device to Customer and does not impact any other ship-to (or Tax Address) provided on Customer's volume license agreement used for purposes of charging sales tax to Customer on purchases made under that volume license agreement.

Storage Array Software

Microsoft grants Customer a non-exclusive, non-transferrable, limited license to use the Software that runs in the Storage Array ("Storage Array Software") only in connection with Customer's use of the Storage Array. Customer's use of the Storage Array Software is subject to the terms of Customer's volume license agreement governing Software, and Microsoft reserves all other rights.

Restrictions

Customer may not use the Storage Array Software for comparisons or "benchmarking" except for Customer's internal purposes or publish or disclose the results thereof.

Certain Third Party Open Source Software

The Storage Array Software may be distributed with certain independent code (e.g., firmware) that is licensed under the GNU General Public License ("GPL"), the GNU Library/Lesser General Public License ("LGPL"), the Apache License Version 2.0 ("Apache License") and/or other open-source licenses ("Open-Source Code"). Any such Open-Source Code is identified in the Third Party Software Notices located at: <http://go.microsoft.com/fwlink/?LinkId=627000>, and is licensed to Customer in accordance with the applicable open-source licenses.

Activation/Consent for Internet-based Services

Activation associates the use of the Storage Array Software with a specific device. During activation and subsequent use of the device, the Storage Array Software may send information about the Storage Array Software and device to Microsoft. This information includes the version, language, and product key of the Storage Array Software, Customer's Internet protocol address, operating system, browser and name, the version of the Storage Array Software Customer is using, and the language code of the Storage Array running the Storage Array Software. Microsoft uses this information to make the Internet-based services available to Customer. By using the Storage Array and Storage Array Software, Customer consents to the transmission of this information to Microsoft.

Storage Array Software Updates

The update service for Storage Array Software will allow Customer to download available updates manually, or opt-in to receiving updates automatically. Available updates from Microsoft will be licensed by Microsoft and any third party updates will be licensed by the applicable third party.

Limited Hardware Warranty

Microsoft warrants that the Storage Array hardware will not malfunction due to a defect in materials or workmanship under ordinary commercial use as described in the applicable product documentation for a period of ninety (90) days from the date of delivery to Customer. If it does not and Customer notifies Microsoft within the warranty term, Microsoft will repair or replace it (at Microsoft's election) at no charge. This is the only warranty Microsoft gives for the Storage Array, and Customer waives any breach of warranty claims not made during the warranty period. This warranty does not cover problems caused by accident, abuse or use in a manner inconsistent with Customer's volume license agreement or the product documentation and it is void if the Storage Array is opened or modified, damaged by use with Non-Microsoft Products, or damaged by maintenance or repair performed by anyone other than Microsoft or a Microsoft authorized vendor. **Microsoft provides no other warranties or conditions and disclaims any other express, implied or statutory warranties, including without limitation, warranties of quality, title, non-infringement, merchantability, and fitness for a particular purpose.**

Indemnification. Defense of third party claims

Microsoft will have the right to intervene to defend Customer against any claims made by an unaffiliated third party that a Storage Array infringes its patent, copyright or trademark or makes unlawful use of its Trade Secret, subject to the terms of the Customer's volume license agreement regarding defense of third party claims. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

Limitation of Liability

For any claim related to a Storage Array, each party's maximum, aggregate liability to the other is limited to direct damages finally awarded in an amount not to exceed the amounts Customer was required to pay for the applicable Storage Array. **In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, including loss of use, loss of profits, or interruption of business, however caused or on any theory of liability. No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations; (2) defense obligations; or (3) violation of the other party's intellectual property rights.**

U.S. Export Control Laws

The Storage Arrays are subject to the provisions in Customer's volume licensing agreement regarding U.S. export jurisdiction.

Collection of Diagnostic Information

Microsoft may collect information to help Microsoft diagnose problems related to the Storage Array and provide potential solutions. If Microsoft receives indication of a potential problem, it may collect information from the Storage Array through the Azure StorSimple Management Service. The types of information collected may include files that help describe or identify the problem, such as operational logs, whether the problem occurred in the hardware or software, the type and severity of the problem, and device status. Microsoft will not collect memory dumps, keys, passwords, or data that a Customer stores on the Storage Array. Microsoft uses the information to improve the Storage Array and related services, and may also use it to improve third party hardware and firmware included as part of the Storage Array. To the extent that Microsoft provides its hardware vendor with specific information, Microsoft will only provide the information in an anonymized data format unless Microsoft obtains Customer's explicit consent. Microsoft will provide this information for the purpose of resolving an identified hardware related issue. To learn more about privacy for the Storage Array, refer to <https://www.microsoft.com/en-us/privacystatement>.

Government Use

Customer understands that in exchange for purchasing one or more StorSimple Monetary Commitment Offerings, Microsoft will provide the Storage Array and StorSimple Support to Customer at no additional charge. Microsoft waives any and all entitlement to compensation from Customer for such Storage Array or StorSimple Standard Support. Microsoft intends that the provision of the Storage Array and StorSimple Standard Support to Customer without charge will fully comply with applicable gift, ethics and other laws and regulations related to gratuitous goods and services. Microsoft intends that the provision of Storage Arrays and StorSimple Standard Support shall be for the sole benefit and use of Customer and not for the personal use or benefit of any individual government employee.

Azure Data Box Hardware Terms

Definitions

Azure Storage means the Microsoft-managed cloud service that provides highly available and secure storage.

Azure Storage Account means a secure account that enables Customer to access and store its information using the Azure Storage service.

Data Box Device means a hardware device(s), including Data Box Software, that Microsoft may provide for Customer's temporary use in storing and transporting or transferring data from its premises to an Azure datacenter so it can be uploaded into Customer's Azure Storage Account.

Data Box Software means all software in object code form provided on or in conjunction with a Data Box Device, including all tools, updates, and associated documentation.

Designated Azure Data Center means the Microsoft Azure Data Center designated by Microsoft as the data center to which Customer will return the Data Box Device, and which may be different than the data center where Customer prefers to store its data and/or the location of Customer Azure Storage Account.

Microsoft Azure Data Box Service or **Service** means the Microsoft Azure service that enables customers to store and transfer on the Data Box Device large amounts of data to and from data centers. For clarity, the Service includes without limitation, any associated technology or functionality, information, materials, and Service updates.

Data Box Software

The Data Box Software is licensed, not sold. Microsoft grants Customer a limited, nonexclusive, nontransferable license to use the Data Box Software (in object code) installed on the Data Box Device, or used in connection with the Data Box Device, only for the purpose of transporting or pre-processing (where applicable) data as enabled by the Data Box Device, and for no other purpose. Microsoft reserves all other rights. This license does not give Customer any right to, and Customer may not: (i) use or virtualize features of the Data Box Software separately from the Data Box Device; (ii) publish, copy, rent, lease or lend the Data Box Software; (iii) work around any technical restrictions in the Data Box Software or restrictions in the Data Box Device documentation (if any); (iv) separate and run parts of the Data Box Software on more than one device; (v) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms; or (vi) reverse engineer, decompile, or disassemble the Data Box Software, or attempt to do so, except if applicable law permit this even when these terms do not and, in that case, Customer may do so only as the law allows.

Restrictions

Customer may not use the Data Box Software for comparisons or "benchmarking", except for Customer's internal purposes, nor publish or disclose the results thereof.

Activation/Consent for Internet-based Services

If activation of the Data Box Software is necessary, activation associates the use of the Data Box Software with a specific device. During activation and subsequent use of the device, the Data Box Software may send information about the Data Box Software and device to Microsoft. This information includes the version, language, and product key of the Data Box Software, Customer's Internet protocol address, operating system, browser and name, the version of the Data Box Software Customer is using, and the language code of the Data Box running the Data Box Software. Microsoft uses this information to make the Internet-based services available to Customer. By using the Data Box Device and Data Box Software, Customer consents to the transmission of this information to Microsoft.

Software Updates

The Data Box Device may allow Customer to download available updates manually. If updates are made available, the updates from Microsoft will be licensed by Microsoft and any third-party updates will be licensed by the applicable third party. In order to continue to receive Data Box Device support, Customer agrees that it will stay current with applicable updates by downloading and applying the most recent updates.

Limitations

Customer is not required to use the Data Box Device to transfer data to Azure Storage, nor is Microsoft obligated to continue to make the Data Box Device or any other hardware product available in connection with the Service. The Data Box Device may not be available in certain regions or jurisdictions, and even where it is, it is subject to availability. Microsoft is not responsible for delays related to the Service that are outside of its direct control. Microsoft reserves the right to refuse to offer the Service and corresponding Data Box Device to anyone in its sole discretion and judgment. Microsoft may suspend the Service at its discretion in accordance with the requirements for Microsoft Azure Services under the [Universal License Terms for Online Services](#).

Azure Service Terms

These Azure Data Box Hardware Terms ("Additional Terms") apply to Customer's receipt and use of the Data Box Device as part of the overall Service. Customer's use of the Service is also subject to the Azure Services Terms located at <https://azure.microsoft.com/en-us/support/legal/>. These Additional Terms supplement but do not amend or modify any existing terms in the Azure Services Terms. As set forth in these Additional Terms, Microsoft may charge Customer specified fees in connection with its use of the Data Box Device as part of the Service.

Product Use Rights

Subject to the payment of applicable fees, Microsoft grants Customer permission to use the Data Box Device to transport, transfer (and where applicable, pre-process) such data, provided that Customer implements certain precautions:

1. Back up and protect the data before transferring the data to the Data Box Device and prior to sending to Azure Storage;
2. Do not delete the data from Customer's premises and equipment before Customer has successfully transferred such data from the Data Box Device to a Designated Azure Data Center.
3. Cease using the Data Box Device to transfer data immediately upon notice from Microsoft.

Customer agrees (i) that it is solely responsible for determining the appropriateness of using the Data Box Device as set forth in these Additional Terms, and (ii) that Microsoft shall have no liability to Customer or any other third party for any loss of data or other damages.

Possession and Return of the Data Box Device

As part of the Service, Microsoft allows Customer to possess the Data Box Device for a period of time depending on the Data Box Device type. For Data Box Devices that have a specified time period for possession, Microsoft may charge Customer additional daily fees for possession of the Data Box Device beyond that specified time period.

Shipment and Title; Fees

a. Title and Risk of Loss. All right, title and interest in each Data Box Device is and shall remain the property of Microsoft, and except as expressly set forth in the Additional Terms, no rights are granted to any Data Box Device (including under any patent, copyright, trade secret, trademark or other proprietary rights. Customer will compensate Microsoft for any loss, material damage or destruction to or of any Data Box Device while it is at any of Customer's locations as described in Shipment and Title; Fees, Table 1. Customer is responsible for inspecting the Data Box Device upon receipt from the carrier and for promptly reporting any damages to Microsoft Support at databoxsupport@microsoft.com. Customer is responsible for the entire risk of loss of, or any damage to, the Data Box Device once it has been delivered by the carrier to Customer's designated address until the Microsoft-designated carrier accepts the Data Box Device for delivery back to the Designated Azure Data Center.

b. Fees. As set forth in these terms, Microsoft may charge Customer specified fees in connection with its use of the Data Box Device as part of the Service, with the current schedule of fees set forth at the following: <https://go.microsoft.com/fwlink/?linkid=2052173>. For clarity, Azure Storage and Azure IoT Hub are separate Azure Services, and if used (even in connection with its use of the Service), separate Azure metered fees will apply. For additional clarity, any Azure services Customer uses after completing a transfer of data using the Azure Data Box Service are subject to separate usage fees. For Data Box Devices, Microsoft may charge Customer a lost device fee not to exceed the actual repair and/or replacement cost of the device, as provided in the GSA MAS Price List if (i) the Data Box Device is lost or materially damaged while it is in Customer's care; (ii) Customer does not provide the Data Box Device to the Microsoft-

designated carrier for return within the time period after the date it was delivered to Customer as provided in the table below. Microsoft reserves the right to change the fees charged for Data Box Device types, including but not limited to, by charging different amounts for different device form factors.

c. Shipment and Return of Data Box Device. For those Data Box Devices that are transported or delivered between Customer and a Designated Azure Data Center or a Microsoft entity, Microsoft will provide access to a designated carrier for such shipping and delivery. Customer will be responsible for costs of shipping a Data Box Device from Microsoft or a Designated Azure Data Center to Customer and return shipping of the same, including any metered amounts for carrier charges, any taxes, or applicable customs fees. When returning a Data Box Device to Microsoft, Customer will package and ship the Data Box Device in accordance with Microsoft's instructions, including by using a carrier designated by Microsoft and the packaging materials provided by Microsoft.

d. Transit Risks. Although data on a Data Box Device is encrypted, Customer acknowledges that there are inherent risks in shipping data on and in connection with the Data Box Device, and that Microsoft will have no liability to Customer for any damage, theft, or loss occurring to a Data Box Device or any data stored on one, including without limitation in transit.

e. Self-Managed Shipment. Notwithstanding the foregoing, Customer may elect to use Customer's designated carrier or Customer itself to ship and return the Data Box Device by selecting this option in the Service portal. Once selected, (i) Microsoft will inform the Customer about Data Box Device availability; (ii) Microsoft will prepare the Data Box Device for pick-up by the Customer's designated carrier or Customer itself; and (iii) Customer will coordinate with Microsoft and Designated Azure Data Center personnel for pick-up and return of the Data Box Device by Customer's designated carrier or Customer directly. A Customer's election for self-managed shipment is subject to the following: (i) Customer abides by all other applicable terms and conditions related to the Service and Data Box Device, including without limitation, the Product Terms and the Azure Data Box Hardware Terms; (ii) Customer is responsible for the entire risk of loss of, or any damage to, the Data Box Device (as set forth in the "Shipment and Title; Fees" section, under subsection (a) "Title and Risk of Loss") from the time that Microsoft makes the Data Box Device available for pick-up by Customer's designated carrier or Customer, to the time Microsoft has accepted the Data Box Device from Customer's designated carrier or Customer at the Designated Azure Data Center; (iii) Customer is fully responsible for the costs of shipping a Data Box Device from Microsoft or a Designated Azure Data Center to Customer and return shipping of the same, including carrier charges, any taxes, or applicable customs fees; (iv) When returning a Data Box Device to Microsoft or a Designated Azure Data Center, Customer will package and ship the Data Box Device in accordance with Microsoft's instructions and any packaging materials provided by Microsoft; (v) Customer will be charged applicable fees (as set forth in the "Shipment and Title; Fees" section, under subsection (b) "Fees") which commence from the time the Data Box Device is ready for pick-up at the agreed upon time and location, and will cease once the Data Box Device has been delivered to Microsoft or the Designated Azure Data Center; and (vi) Customer acknowledges that there are inherent risks in shipping data on and in connection with the Data Box Device, and that Microsoft will have no liability to Customer for any damage, theft, or loss occurring to a Data Box Device or any data stored on one, including without limitation in transit when shipped by Customer's designated carrier.

Responsibilities if Customer Moves a Data Box Device between Locations

While Customer is in possession of a Data Box Device, Customer may, at its sole risk and expense, transport the Data Box Device to its different locations to upload its data in accordance with this Section and the requirements of the Additional Terms. Customer is responsible for obtaining, at its own risk and expense, any export license, import license and other official authorization for the exportation and importation of the Data Box Device and associated Software and Customer's data to any such different Customer location. Customer shall also be responsible for customs clearance at any such different Customer location, and will bear all duties, taxes and other official charges payable upon importation as well as any and all costs and risks of carrying out customs formalities in a timely manner. Customer agrees to comply with and be responsible for all applicable import, export and general trade laws and regulations should Customer decide to transport the Data Box Device beyond the country border in which Customer receive the Data Box Device. Notwithstanding the foregoing, if Customer transports the Data Box Device to a different location as set forth in this Section, Customer agrees to cause the Data Box Device to return to the country location where Customer received such device initially, prior to shipping the Data Box Device back to the original point of origin, whether a specified Microsoft entity or a Designated Azure Data Center. If requested, Microsoft may provide a list of companies that may be able to assist Customer in importing or exporting the Data Box Device, but Microsoft does not endorse, support, or represent any of the listed companies, and Microsoft disclaims any liability for any damages or liabilities Customer may incur as a result of those services.

Disclaimer of Warranty

Microsoft provides the Data Box Device, and any assistance by Microsoft in connection with the Data Box Device, "as is" without any warranties or conditions, and disclaims any express, implied or statutory warranties, including without limitation, warranties of quality, title, non-infringement, merchantability, and fitness for a particular purpose. Customer bears the risk of using them.

U.S. Export Control Laws

The Data Box Devices are subject to the provisions in Customer's volume licensing agreement, Azure Subscription Agreement, or other customer agreement regarding U.S. export jurisdiction.

Privacy; Processing of Personal Data

1. **Privacy.** The Microsoft Privacy Statement applies to the Service and the Data Box Device under these Additional Terms.
2. **Terms.** Customer agrees to comply with all data protection laws that apply to its use of the Service, its handling of data with the Data Box Device or in Azure Storage, or its moving the Data Box Device as described in the Responsibilities if Customer Moves a Data Box Device between Locations section above.
3. **Processing of Personal Data.** To the extent Microsoft is a processor or subprocessor of personal data in connection with the software, Microsoft makes the commitments in the European Union General Data Protection Regulation Terms of the Online Services Terms to all customers effective May 25, 2018, at <http://go.microsoft.com/?linkid=9840733>.

Azure Stack Edge Hardware Terms

Definitions

"**Azure Stack Edge Device**" means hardware devices, including Software, that are offered as part of Azure Stack Edge family of devices as described at <https://azure.microsoft.com/en-us/products/azure-stack/edge/>.

Azure Stack Edge Service or "Service" means the Azure service that enables customers to receive, provision, use and manage an Azure Stack Edge Device. For clarity, the Service includes without limitation, any associated technology or functionality (e.g., creating a share), information, materials, and Service updates.

"**Software**" means all software provided on or in conjunction with an Azure Stack Edge Device, including all tools, updates, and associated documentation.

Azure Services Terms; Limitations

Azure Services Terms

These Azure Stack Edge Hardware Terms ("Additional Terms") apply to Customer's receipt and use of the Azure Stack Edge Device as part of the overall Service. Customer's use of the Service is also subject to the Azure Service Agreement and Terms located at <https://azure.microsoft.com/en-us/support/legal/>, which includes without limitation, the Customer's customer agreement and the Product Terms. These Additional Terms supplement but do not amend or modify any existing terms in the Azure Service Agreement and Terms. If there is a conflict between these Additional Terms and any of the terms comprising the Azure Service Agreement and Terms, the Additional Terms will govern and control for purposes of the use of the Azure Stack Edge Device as part of the Service.

Limitations

Customer is not required to use the Azure Stack Edge Device to transfer data to an Azure service or to run any other functionality, nor is Microsoft obligated to continue to make the Azure Stack Edge Device or any other hardware product available in connection with the Service. The Azure Stack Edge Device may not be available in certain regions or jurisdictions, and even where it is, it is subject to availability. Microsoft is not responsible for delays related to the Service that are outside of its direct control. Microsoft reserves the right to refuse to offer the Service and corresponding Azure Stack Edge Device to anyone in its sole discretion and judgment. Microsoft may suspend the Service in its discretion in accordance with the terms for Microsoft Azure services under the [Universal License Terms for Online Services](#).

Use of Azure Stack Edge Device and Software

Conditions for Azure Stack Edge Use

Subject to the payment of applicable fees, Microsoft grants Customer permission to use to the Azure Stack Edge Device, provided that Customer implements the following:

1. **Data Protection.** Customer agrees to develop and implement a data protection strategy that among other things, preserves and backs up customer data residing and remaining locally on the Azure Stack Edge Device in the event of device failure, loss, or destruction.
2. **Customer Determination of Appropriateness.** Customer agrees (i) that it is solely responsible for determining the appropriateness of using the Azure Stack Edge Device as set forth in these Additional Terms, and (ii) that Microsoft shall have no liability to Customer or any other third party for any loss of data or other damages. Customer should assess the capabilities and features of the Azure Stack Edge Device based on Customer's intended workloads and applications to determine if the Azure Stack Edge Device is appropriate to meet Customer's business needs. For example, the Azure Stack Edge Device has Service Level Objectives (see the "Service Level Objectives" Section) but no service level agreement commitments (e.g., for uptime, support issue resolution, etc.) and has the capabilities described at <https://aka.ms/AzureStackEdgeDoc>.
3. **No Transfer or Access.** Customer agrees to not sell, assign, or transfer the Azure Stack Edge Device, and will not directly or indirectly (through a third party) view, open, modify, disassemble, or otherwise tamper with the Azure Stack Edge Device (including the Software).
4. **Accreditation.** To the extent that the Customer is a governmental entity, Microsoft also grants Customer the right to place the Azure Stack Edge Device through its accreditation processes to meet its needs, including without limitation, accreditation requirements and processes for use in an unclassified, secret, or top secret domain.

Software

The Software is licensed, not sold. Microsoft grants Customer a limited, nonexclusive, nontransferable license to use the Software with the Azure Stack Edge Device, and for no other purpose. Microsoft reserves all other rights. This license does not give Customer any right to, and Customer may not: (i) use or virtualize features of the Software separately from the Azure Stack Edge Device; (ii) publish, copy, rent, lease or lend the Software; (iii) work around any technical restrictions in the Software or restrictions in the Azure Stack Edge Device documentation (if any); (iv) separate and run parts of the Software on more than one device; (v) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms; or (vi) reverse engineer, decompile, or disassemble the Software, or attempt to do so, except if applicable law permit this even when these terms do not and, in that case, Customer may do so only as the law allows. If there is a conflict between these Additional Terms and any separate license terms for any separate modules or agents used in connection with the Azure Stack Edge Device, the separate license terms for those modules or agents shall govern and control for the use of such modules or agents.

Restrictions

Customer may not use the Software for comparisons or "benchmarking," except for Customer's internal purposes, nor publish or disclose the results thereof.

Activation/Consent for Internet-based Services

If activation of the Software is necessary, activation associates the use of the Software with a specific device. During activation and subsequent use of the device, the Software may send information about the Software and device to Microsoft, including device properties (e.g., node, chassis and component numbers, software and firmware versions, timestamps of registration, etc.) and Customer environment details (e.g., internet protocol addresses of device, device name, time and update server IP address).

Microsoft uses this information to make the Internet-based services available to Customer. By using the Azure Stack Edge Device and Software, Customer consents to the transmission of this information to Microsoft.

Software Updates

Microsoft may make updates available for the Azure Stack Edge Device. If updates are made available, the updates from Microsoft will be licensed by Microsoft and any third-party updates will be licensed by the applicable third party. In order to continue to receive Azure Stack Edge support, Customer agrees that it will stay current with applicable updates by downloading and applying the most recent updates.

Use of the Azure Stack Edge Device

As part of the Service, Microsoft allows Customer to use the Azure Stack Edge Device for as long as the Customer has an active subscription to the Service. If Customer no longer has an active subscription and fails to return the Azure Stack Edge Device, Microsoft can deem the Azure Stack Edge Device as lost as set forth in the "Title and Risk of Loss; Shipment and Return Responsibilities" Section.

Title and Risk of Loss; Shipment and Return Responsibilities

Title and Risk of Loss

All right, title and interest in each Azure Stack Edge Device is and shall remain the property of Microsoft, and except as expressly set forth in these Additional Terms, no rights are granted to any Azure Stack Edge Device (including under any patent, copyright, trade secret, trademark or other proprietary rights). Customer will compensate Microsoft for any loss, damage or destruction to or of any Azure Stack Edge Device while it is at any of Customer's locations or in the circumstances described in the "Responsibilities if a Government Customer Moves an Azure Stack Edge Device between Customer's Locations" Section, with the exception of expected wear and tear, which includes minor damage (i.e., dings and dents) that do not compromise the structure or functionality of the Azure Stack Edge Device. Customer is responsible for inspecting the Azure Stack Edge Device upon receipt from the carrier and for promptly reporting any damages to Microsoft Support at adbeops@microsoft.com. Customer is responsible for the entire risk of loss of, or any damage to (other than expected wear and tear), the Azure Stack Edge Device once it has been delivered by the carrier to Customer's designated address until the Microsoft-designated carrier accepts the Azure Stack Edge Device for return delivery. If Customer prefers to arrange Customer's own pick-up and/or return of the Azure Stack Edge Device pursuant to the "Shipment and Return of Azure Stack Edge Device" Section below, Customer is responsible for the entire risk of loss of, or any damage to the Azure Stack Edge Device until it has been returned to, and accepted by Microsoft.

Microsoft may charge Customer for a lost device fee for the Azure Stack Edge Device (or equivalent) not to exceed the replacement cost of the device as provided in the GSA MAS Price List (i) if the Azure Stack Edge Device is lost or materially damaged while it is Customer's responsibility as described in the previous sentence, or (ii) if Customer does not provide the Azure Stack Edge Device to the Microsoft-designated carrier for return or return the Azure Stack Edge Device pursuant to the "Shipment and Return of Azure Stack Edge Device" Section below within 30 days from the end of Customer's use of the Service. Microsoft reserves the right to change the fee charged for lost or damaged devices, including but not limited to, by charging different amounts for different device form factors.

Shipment and Return of Azure Stack Edge Device

Customer will be responsible for a one-time metered shipping fee for the shipment of the Azure Stack Edge Device from Microsoft to Customer and return shipping of the same, in addition to any metered amounts for carrier charges, any taxes, or applicable customs fees. When returning an Azure Stack Edge Device to Microsoft, Customer will package and ship the same in accordance with Microsoft's instructions, including by using a carrier designated by Microsoft and the packaging materials provided by Microsoft. If Customer prefers to arrange Customer's own pick-up and/or return of the same, then Customer is responsible for the costs of shipping the Azure Stack Edge Device, including adequate protections against any loss or damage of the Azure Stack Edge Device (e.g., insurance coverage) while in transit. Customer will package and ship the Azure Stack Edge Device in accordance with Microsoft's packaging instructions. Customer is also responsible to ensure that it removes any and all of Customer's data from the Azure Stack Edge Device prior to returning it to Microsoft, including but not limited to, following any Microsoft issued processes for wiping or clearing the Azure Stack Edge Device.

Responsibilities if a Government Customer Moves an Azure Stack Edge Device between Customer's Locations

If a government Customer is in possession of an Azure Stack Edge Device, the government Customer only may, at government Customer's sole risk and expense, transport the Azure Stack Edge Device to government Customer's different locations in accordance with this Section and the requirements of the Additional Terms. Government Customer is responsible for obtaining at government Customer's own risk and expense any export license, import license and other official authorization for the exportation and importation of the Azure Stack Edge Device and associated Software and government Customer's data to any such different government Customer location. Government Customer shall also be responsible for customs clearance at any such different government Customer location, and will bear all duties, taxes and other official charges payable upon importation as well as any and all costs and risks of carrying out customs formalities in a timely manner. Government Customer agrees to comply with and be responsible for all applicable import, export and general trade laws and regulations should government Customer decide to transport the Azure Stack Edge Device beyond the country border in which government Customer receives the Azure Stack Edge Device. Notwithstanding the foregoing, if

government Customer transports the Azure Stack Edge Device to a different location as set forth in this Section, government Customer agrees to cause the Azure Stack Edge Device to return to the country location where government Customer received it initially, prior to shipping the Azure Stack Edge Device to Microsoft. Government Customer acknowledges that there are inherent risks in shipping data on and in connection with the Azure Stack Edge Device, and that Microsoft will have no liability to government Customer for any damage, theft, or loss occurring to an Azure Stack Edge Device or any data stored on one, including without limitation in transit. It is the government Customer's responsibility to obtain the appropriate support agreement from Microsoft in order to meet government Customer's operating objectives for the Azure Stack Edge Device; however, depending on the location to which government Customer intends to move the Azure Stack Edge Device, Microsoft's ability to provide hardware servicing and support may be delayed, or may not be available.

Non-government Customers shall not transport an Azure Stack Edge device to a country that is different from the one to which it was delivered by Microsoft.

Fees

Microsoft will charge Customer specified fees in connection with Customer's use of the Azure Stack Edge Device as part of the Service, with the current schedule of fees for each Azure Stack Edge model and not to exceed the fee set forth in the GSA Schedule Pricelist. For clarity, Customer may use other Azure services in connection with Customer's use of the Service, and Microsoft deems such services as separate services that may be subject to separate metered fees and costs. By way of example only, Azure Storage, Azure Compute, and Azure IoT Hub are separate Azure services, and if used (even in connection with its use of the Service), separate Azure metered services will apply.

Survival

Azure Services Terms, Software, Survival, Disclaimer of Warranty, Privacy Terms and Export Control Laws Section will survive expiration or termination of these Additional Terms.

Disclaimer of Warranty

THE AZURE STACK EDGE DEVICE AND ANY ASSISTANCE BY MICROSOFT PROVIDED PURSUANT TO THESE ADDITIONAL TERMS IS PROVIDED "AS-IS." CUSTOMER BEARS THE RISK OF USING THEM. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. CUSTOMER MAY HAVE ADDITIONAL CONSUMER RIGHTS OR STATUTORY GUARANTEES UNDER LOCAL LAWS WHICH THESE ADDITIONAL TERMS CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER CUSTOMER'S LOCAL LAWS, MICROSOFT EXCLUDES ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

Privacy; Processing of Personal Data

- **Privacy.** The Microsoft Privacy Statement applies to the Service and the Data Box Device under these Additional Terms.
- **Terms.** Customer agrees to comply with all data protection laws that apply to its use of the Service, its handling of data with the Azure Stack Edge Device or in Azure Storage, or if a government Customer moves the Azure Stack Edge Device as described in the "Responsibilities if a Government Customer Moves an Azure Stack Edge Device between Customer's Locations" Section above.
- **Processing of Personal Data.** To the extent Microsoft is a processor or subprocessor of personal data in connection with the software, Microsoft makes the commitments in the European Union General Data Protection Regulation Terms of the Online Services Terms to all customers effective May 25, 2018, at <http://go.microsoft.com/?linkid=9840733>.

Service Level Objectives

The Azure Stack Edge Device has Service Level Objectives (SLO) for (a) delivery of the Azure Stack Edge Device; and (b) replacement of Field Replaceable Units or FRUs. The SLOs or failure to meet the SLOs do not provide any basis for financial recovery or remediation. For clarification purposes, the SLOs are separate and distinct from Azure service level agreement (SLA) commitments, as set forth in the Service Level Agreement for Microsoft Online Services. For additional clarity, the Azure Stack Edge Device does not have any applicable Azure SLAs.

Azure Stack Hub Ruggedized from Microsoft Hardware Terms

Definitions

Documentation means the Ruggedized Azure Stack Hub user documentation set forth in <https://aka.ms/azurestackhub>.

Azure Stack Hub Ruggedized from Microsoft or Appliance means an integrated hardware system, including Software, that Microsoft may offer as part of the Azure Stack family of Appliances as described at <https://azure.microsoft.com/en-us/overview/azure-stack/>, for Customer's use at Customer's designated premises.

Azure Stack Hub Ruggedized Service or Service means the Azure service that enables Customers to receive, provision, use, and manage the Appliance in running Azure services. For clarity, the Service includes without limitation, any associated technology or functionality, information, materials, and Service updates.

Software means all software in object code form provided on or in conjunction with an Appliance, including all tools, updates, and associated documentation.

Azure Service Terms; Limitations

Azure Service Terms

These Ruggedized Azure Stack Hub Appliance Hardware Terms ("Additional Terms") apply to Customer's receipt and use of the Appliance as part of the overall Service. Customer's use of the Service is also subject to the Azure Service Agreement and Terms located at <https://azure.microsoft.com/en-us/support/legal/>, which includes without limitation, the Customer's customer or other license agreement and the Product Terms. These Additional Terms supplement but do not amend or modify any existing terms in the Azure Service Agreement and Terms. If there is a conflict between these Additional Terms and any of the terms comprising the Azure Service Agreement and Terms, the Additional Terms will govern and control for purposes of the use of the Appliance as part of the Service.

Limitations

Microsoft is not obligated to continue to make the Appliance or any other hardware product available in connection with the Service. The Appliance may not be available in certain regions or jurisdictions, and even where it is, it is subject to availability. Microsoft is not responsible for delays related to the Service that are outside of its direct control. Microsoft reserves the right to refuse to offer the Service and corresponding Appliance to anyone in its sole discretion and judgment. Microsoft may suspend the Service in its discretion in accordance with the terms for Microsoft Azure services under the [Universal License Terms for Online Services](#).

Use of the Appliance and Software

Conditions for Appliance Use

Subject to the payment of applicable fees, Microsoft grants Customer permission to use to the Appliance, provided that Customer implements the following:

1. **Data protection.** Customer agrees to take certain precautions regarding its customer data: (i) Back up and protect all data prior to copying to and storing on the Appliance ; (ii) do not delete the data from Customer's premises and equipment before Customer has successfully transferred such data from the Appliance to Microsoft; and (iii) Apply updates as set forth herein and perform preventative maintenance as recommended by Microsoft.
2. **Customer Determination of Appropriateness.** Customer agrees (i) that it is solely responsible for determining the appropriateness of using the Appliance as set forth in these Additional Terms, and (ii) that Microsoft shall have no liability to Customer or any other third party for any loss of data or other damages.
3. **Deployment pre-requisites and facility assessment.** Customer agrees to meet Microsoft's requirements necessary to support the installation, use, maintenance, and removal of the Appliance.
4. **No Transfer or Access.** Customer agrees to not sell, assign, or transfer the Appliance, and will not directly or indirectly (through a third party) view, open, modify, disassemble, or otherwise tamper with the Appliance (including the Software).

Accreditation

To the extent that the Customer is a governmental entity, Microsoft also grants Customer the right to place the Appliance through its accreditation processes to meet its needs, including without limitation, accreditation requirements and processes for use in an unclassified, secret, or top secret domain.

Software

The Software is licensed, not sold. Microsoft grants Customer a limited, nonexclusive, nontransferable license to use the Software with the Appliance, and for no other purpose. Microsoft reserves all other rights. This license does not give Customer any right to, and Customer may not: (i) use or virtualize features of the Software separately from the Appliance; (ii) publish, copy, rent, lease or lend the Software; (iii) work around any technical restrictions in the Software or restrictions in the Appliance documentation (if any); (iv) separate and run parts of the Software on more than one device; (v) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms; or (vi) reverse engineer, decompile, or disassemble the Software, or attempt to do so, except if applicable law permit this even when these terms do not and, in that case, Customer may do so only as the law allows. Subject to the foregoing limitations, Customer's use of the Software is subject to the software license terms presented to or otherwise made available to Customer in connection with the Appliance, and also includes without limitation, any separate license terms for any separate modules or agents to run additional Azure services on or in connection with the Appliance. If there is a conflict between these Additional Terms and any separate license terms for any separate modules or agents used in connection with the Appliance, the separate license terms for those modules or agents shall govern and control for the use of such modules or agents.

Restrictions on Benchmarking

Customer may not use the Software for comparisons or "benchmarking," except for Customer's internal purposes, nor publish or disclose the results thereof.

Activation/Consent for Internet-based Services

If activation of the Software is necessary, activation associates the use of the Software with a specific device. During activation and subsequent use of the device, the Software may send information about the Software and device to Microsoft, as described in the Documentation. Microsoft uses this telemetry to make the Internet-based services available to Customer. By using the Appliance and Software, Customer consents to the transmission of this information to Microsoft.

Software Updates

Microsoft may make Software updates available for the Appliance. If updates are made available, the updates from Microsoft will be licensed by Microsoft and any third-party updates will be licensed by the applicable third party. In order to continue to receive Appliance support, Customer agrees that it will stay current with applicable updates by downloading and applying the most recent updates in compliance with Microsoft's published or provided policy.

Delivery, Deployment, and Use of the Appliance

- **Delivery.** The Service and the Appliance are offered as a Microsoft first party service under these Additional Terms and the Azure Service Agreement and Terms, and by which Microsoft will deliver the Appliance to Customer's specified location ("Customer Specified Location"), subject to Service and Appliance availability.
- **Deployment.** Microsoft will initiate and complete the deployment of the Appliance at the Customer Specified Location, which can typically take up to fifteen (15) days.
- **Use.** As part of the Service, Microsoft allows Customer to use the Appliance for as long as the Customer has an active subscription to the Service, which use includes but is not limited to, use of the hardware, hardware support, and basic software infrastructure services (e.g., storage, compute, including virtual machines and containers). As part of the deployment and use of the Service and the Appliance, Customer agrees to provide assigned resources at the level reasonably requested by Microsoft to address pre-requisite activities, information, items for deployment, and ongoing management.
- **Optional Services.** Customer may use and subscribe to additional, optional services in connection with the Service and Appliance that will be subject to a separate fee or subscription.

*Title and Risk of Loss; Shipment and Return Responsibilities***Title and Risk of Loss**

All right, title and interest in each Appliance is and shall remain the property of Microsoft, and except as expressly set forth in these Additional Terms, no rights are granted to any Appliance (including under any patent, copyright, trade secret, trademark or other proprietary rights). Customer will compensate Microsoft for any loss, damage or destruction to or of any Appliance while it is at any of Customer's locations or in the circumstances described in Section "Responsibilities if a Government Customer Moves the Appliance between Customer's Locations," with the exception of expected wear and tear, which includes minor damage (e.g., dings and dents) that do not compromise the structure or functionality of the Appliance. Customer is responsible for inspecting the Appliance upon receipt from the carrier and for promptly reporting any damages to Microsoft Support at madbeops@microsoft.com. Customer is responsible for the entire risk of loss of, or any damage (other than expected wear and tear) to, the Appliance once it has been delivered by the carrier to Customer's designated address until the Microsoft-designated carrier accepts the Appliance for return delivery.

Microsoft may charge Customer a lost device fee not to exceed the replacement cost of the device as provided in the GSA MAS Price List for the Appliance (i) if the Appliance is lost or materially damaged while it is Customer's responsibility as described in the previous sentence, or (ii) if Customer does not return the Appliance to the Microsoft-designated carrier for return or Microsoft pursuant to Section "Shipment and Return of the Appliance" below, within 30 days from the end of Customer's use of the Service. Microsoft reserves the right to change the fee charged for lost or damaged devices, including but not limited to, by charging different amounts for different device form factors.

Shipment and Return of the Appliance

Customer will be responsible for a one-time, per Appliance metered shipping fee for shipping costs and return logistics ("Logistics Fee"), in addition to any taxes, or applicable customs fees identified on an invoice. The Logistics Fee includes shipping, setup, refurbishment, data destruction, and coverage for loss of the Appliance in transit. When returning an Appliance to Microsoft, Customer agrees to package and ship the Appliance in accordance with Microsoft's instructions, including the use of a carrier designated by Microsoft and the packaging materials provided by Microsoft. Customer is responsible to remove Customer's data from the Appliance prior to returning it to Microsoft, and follow any Microsoft issued processes for wiping or clearing the Appliance.

Disposition at End of Life

Notwithstanding the foregoing, if Microsoft in its sole discretion determines that the Appliance as part of the Service has reached or exceeded its useful lifespan while it is in the possession of Customer, then Microsoft has the right and ability to change the Appliance or any components thereof. Customer agrees to provide Microsoft with limited access to Customer Specified Location and the Appliance for this purpose. Microsoft will discuss logistics and timing of activities related to this change-out of the Appliance or Appliance components with Customer.

Retention of Hardware Components Option

Microsoft may provide Customer with separate fee options to retain specified Appliance components (e.g., hard drives) for destruction by Customer or have Microsoft dispose of said components at the end of the Term or Appliance decommissioning.

Responsibilities if a Government Customer Moves the Appliance between Customer's Locations

If a government Customer is using an Appliance during the government Customer's use of the Service, the government Customer only may, at government Customer's sole risk and expense, transport the Appliance to government Customer's different locations to upload government Customer's data in accordance with Section "Use of the Appliance and Software" above. Subject to Section "Export Control Laws", government Customer is responsible for obtaining at government Customer's own risk and expense any export license, import license and other official authorization for the exportation and importation of the Appliance and associated Software and government Customer's data to any such different location of government Customers. Government Customer is also solely responsible for customs clearance at any such different location of government Customer's, and government Customer will bear all duties, taxes and other official charges payable upon importation as well as any and all costs and risks of carrying out customs formalities in a timely manner. Government Customer agrees to comply with and be responsible for all applicable import, export and general trade laws and regulations should government Customer decide to transport the Appliance beyond the country border in which Customer receives the Appliance. Notwithstanding the foregoing, if government Customer transports the Appliance to a different location as set forth in this Section, government Customer agrees to cause the Appliance to return to the country location where Customer received it initially, prior

to returning the Appliance to Microsoft or a government Customer Specified Location. Government Customer acknowledge that there are inherent risks in shipping data on and in connection with the Appliance, and that Microsoft will have no liability to government Customer for any damage, theft, or loss occurring to an Appliance or any data stored on one, including without limitation in transit. It is Customer's responsibility to obtain the appropriate support agreement from Microsoft in order to meet government Customer's operating objectives for the Appliance; however, depending on the location to which government Customer intends to move the Appliance, Microsoft's ability to provide hardware servicing and support may be delayed, or may not be available.

Non-government Customers shall not transport an Azure Stack Hub Ruggedized device to a country different from the one to which it was delivered by Microsoft.

Fees

Microsoft will charge Customer specified fees in connection with Customer's use of the Appliance as part of the Service in accordance with the fees set forth on the GSA Schedule Pricelist, with the current schedule of fees as provided by Microsoft. For clarity, Customer may use other Azure services in connection with Customer's use of the Service, and Microsoft deems such services as separate and additional services subject to separate subscription or metered fees and costs, as those additional services are installed on the Appliance. By way of example only, Azure Storage, Azure Compute, and Azure IoT Hub are separate Azure services, and if used (even in connection with its use of the Service), separate Azure metered services will apply.

Survival

Sections Azure Services Terms, Software, Survival, Disclaimer of Warranty, Privacy Terms and Export Control Laws will survive expiration or termination of these Additional Terms.

Disclaimer of Warranty

THE APPLIANCE AND ANY ASSISTANCE BY MICROSOFT PROVIDED PURSUANT TO THESE ADDITIONAL TERMS IS PROVIDED "AS-IS." CUSTOMER BEARS THE RISK OF USING THEM. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. CUSTOMER MAY HAVE ADDITIONAL CONSUMER RIGHTS OR STATUTORY GUARANTEES UNDER LOCAL LAWS WHICH THESE ADDITIONAL TERMS CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER CUSTOMER'S LOCAL LAWS, MICROSOFT EXCLUDES ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

Hardware Updates; Support

Hardware Updates

Microsoft is not required to provide Customer with any new Appliance releases, enhancements, or updates for the Appliance. If Microsoft opts to do so, such new releases, enhancements, or updates ("Hardware Updates") will be subject to the terms of these Additional Terms. Customer agrees to provide limited access to the Customer Specified Location for the purpose of applying new hardware components or the Appliance itself.

Support

As part of the subscription to the Service, Microsoft will provide a baseline level of support for the Service and Appliance. Customer will also enroll in the Microsoft Premier Support plan.

Maintenance

Customer agrees that it will not allow anyone to access, repair, or otherwise maintain the Appliance at the Customer Specified Location other than Microsoft or its designees upon request, except for an emergency situation such as fire or imminent personal injury.

Privacy Terms

- **Privacy.** The Microsoft Privacy Statement (<http://www.microsoft.com/privacystatement/OnlineServices/Default.aspx>) applies to the Service and the Appliance under these Additional Terms.
- **Terms.** Customer agrees to comply with all data protection laws that apply to Customer's use of the Service, its handling of data with the Appliance or in Azure, or if government Customer moves the Appliance as described in the "Responsibilities if a Government Customer Moves an Appliance between Customer's Locations" section above.

- **Processing of Personal Data.** To the extent Microsoft is a processor or subprocessor of personal data in connection with the software, Microsoft makes the commitments in the European Union General Data Protection Regulation Terms of the Online Services Terms to all customers effective May 25, 2018, at <http://go.microsoft.com/?linkid=9840733>.

Applicability of Service Level Agreement

Service level agreements that apply to specified Azure services listed in the Service Level Agreement for Microsoft Online Services do not apply to the Service or the Appliance, since Customer is running the Service and Appliance locally, where customer controls and has responsibility for the physical environment.

Microsoft Online Services Criminal Justice Information Services (CJIS) Customer Agreement for CJIS Covered Services

This Microsoft Online Services Criminal Justice Information Services (CJIS) Customer Agreement for Covered Services ("Agreement") is entered into between the customer entity ("Enrolled Affiliate") and Microsoft for the provision of Covered Services (as defined below). The parties agree that the Agreement applies to only the Enrolled Affiliate's use of Covered Services and is subject to the Enrolled Affiliates adherence to its independent obligations pursuant to the CJIS Policy. Enrolled Affiliate is prohibited from using Covered Services in any way that violates the CJIS Policy. Violation of the terms in this Agreement, or failure to adhere to any of the CJIS Policy (as defined below) requirements, may result in suspension of the Covered Service. Microsoft will suspend the Covered Service only to the extent reasonably necessary. However, because of the criminal justice implications associated with failure to adhere to the CJIS Policy requirements, Microsoft may not provide notice before suspending a Covered Service.

Defined Terms.

The following definitions are used in this Agreement:

"CJI" means Criminal Justice Information as that term is used in the CJIS Policy.

"CJIS Management Agreement" means the signed agreement between Microsoft and the CSA which describes the commitments Microsoft and the CSA have made to comply with the CJIS Policy.

"CJIS Policy" means the current version of the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Policy. The CJIS Policy in effect at the signing of this Agreement is, Version 5.7, dated 8/16/2018. The most recent version of the CJIS Policy is available at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>.

"CJIS Security Addendum" means the CJIS Security Addendum included in Appendix H to the CJIS Policy.

"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, the Enrolled Affiliate through use of the Covered Services, which may include but is not limited to CJI.

"Covered Services" means Services listed as in-scope at <https://www.microsoft.com/en-us/trustcenter/Compliance/CJIS>. Covered Services does not include: (a) Microsoft Dynamics 365 for supported devices (including but not limited to Microsoft Dynamics 365 services for tablets and/or smartphones); and (b) all separately-branded services made independently available with or in addition to Dynamics 365 Government.

"CSA" means the CJIS Systems Agency for the State that has entered into a CJIS Management Agreement with Microsoft.

"End User" means an individual that accesses the Covered Services.

"Security Incident" includes any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such facilities or equipment resulting in loss, disclosure or alteration of Customer Data.

"State" means the State, Commonwealth, or Territory in the United States in which Enrolled Affiliate is located or uses the Covered Services.

Capitalized terms used but not defined in this Agreement will have the meanings provided in the CJIS Management Agreement or, if not defined in the CJIS Management Agreement, in the CJIS Policy.

1. Microsoft Responsibilities and CJIS Security Addendum

Microsoft will support Enrolled Affiliate's use of the Covered Services in compliance with the CJIS Policy only in CJIS-covered states. Please refer to the following to determine if your state is a CJIS covered State <https://www.microsoft.com/en-us/TrustCenter/Compliance/CJIS>. If a state or Covered Service is not listed on the Microsoft website, Microsoft does not have FBI CJIS coverage for that state or Covered Service. Microsoft's commitments as it relates to its Covered Services compliance with the CJIS Policy are described in the CJIS Management Agreement and subject to: (i) Enrolled Affiliates' adherence to the terms of the CJIS Management Agreement; (ii) Enrolled Affiliates' adoption of this Agreement; (iii) Enrolled Affiliates' acceptance and incorporation of applicable state specific CJIS terms and conditions in this Agreement; and (iv) Enrolled Affiliates' adherence to its independent obligations under the CJIS Policy. Microsoft does not make any commitments to the Enrolled Affiliate other than are contained in this Agreement and the CJIS Management Agreement.

In furtherance of the execution of the CJIS Management Agreement with the CSA, Microsoft provided the CSA with an executed CJIS Security Addendum Certification. Without limiting the other provisions of this Agreement, Attachment 1 describes how Microsoft and Enrolled Affiliate will fulfill certain of their respective obligations under the CJIS Policy.

2. Enrolled Affiliate Responsibilities

2.1 Enrolled Affiliate is responsible for reviewing and establishing security practices consistent with the CJIS Management Agreement, including the CJIS Security Addendum contained therein. Enrolled Affiliate will notify and obtain approval from the CSA, for use of the Covered Services to store or process CJI. Prior to introducing CJI into the Covered Services Enrolled Affiliate will: (i) execute this Agreement; (ii) confirm with Enrolled Affiliate's CSA that all state CJIS prerequisites are met; and (iii) fulfill all prerequisites established or required by either the CSA or the CJIS Management Agreement prior to introducing CJI into the Covered Services.

2.2 Enrolled Affiliate is responsible for obtaining all CJIS related documentation from the CSA including but not limited to the CJIS Management Agreement and the CJIS Security Addendum. The CJIS Management Agreement also grants the CSA certain rights to audit Microsoft's compliance with CJIS Policy, as described in Attachment 1 and the CJIS Management Agreement. For avoidance of doubt, the Enrolled Affiliate has delegated all audit and inspection rights to the CSA. Enrolled Affiliate will direct all requests for documentation, audits or requests for information to the CSA.

2.3 Enrolled Affiliate acknowledges that the Covered Services utilized by Enrolled Affiliate enable End Users optionally to access and use a variety of additional resources, applications, or services that are (a) provided by third parties, or (b) provided by Microsoft subject to their own terms of use or privacy policies (collectively, for convenience, "add-ons"), as described in services documentation and/or in the portal through which Enrolled Affiliate's administrator(s) will manage and configure the Covered Services.

2.4 Enrolled Affiliate is independently responsible to review Covered Services documentation, configure its systems, and adopt and implement such policies and practices for its End Users' use of Covered Services, together with any add-ons, as Enrolled Affiliate determines are appropriate in order for Enrolled Affiliate to comply with the CJIS Policy or other legal or regulatory requirements applicable to Enrolled Affiliate and not generally applicable to Microsoft as an IT service provider. Enrolled Affiliate represents that it has reviewed the documentation for the Covered Services and confirms that its Covered Services environment is prepared and appropriate for CJI.

2.5 Enrolled Affiliate acknowledges that only Covered Services will be delivered subject to the terms of this Agreement and the CJIS Management Agreement (inclusive of the CJIS Security Addendum) executed with the CSA. Processing and storage of CJI in other services is not supported. Without limiting the foregoing, data that Enrolled Affiliate elects to provide to the Microsoft technical support organization, if any, or data provided by or on behalf of Enrolled Affiliate to Microsoft's billing or commerce systems in connection with purchasing/ordering Covered Services, if any, is not subject to the provisions of this Agreement or the CJIS Management Agreement.

2.6 For clarity, Microsoft's commitment to FBI CJIS background checks of Key Microsoft Personnel referenced in the CJIS Management Agreement refers to Microsoft's personnel only and not Enrolled Affiliate's personnel. If Enrolled Affiliate's employees will have unencrypted access to CJI, then (1) Enrolled Affiliate shall disclose such to a government Customer in its government contract as required by law, regulations or the terms of the government solicitation and (2) Enrolled Affiliate is solely responsible for CJIS background checks of Enrolled Affiliate's employees and shall not misrepresent Microsoft's commitment to CJIS background checks as applicable to Enrolled Affiliate's employees.

Remainder of this page intentionally left blank.

Attachment 1 — CJIS Policy Approach in Covered Services

This Attachment 1 describes how Microsoft and Enrolled Affiliate will fulfill certain of their obligations under the CJIS Policy in delivery and use of the Covered Services.

A. Considerations for Compliance with CJIS Security Policy

The Covered Services are cloud services operated in a standardized manner with features and processes common across multiple customers. As part of Enrolled Affiliate's preparation to use the services for CJI, Enrolled Affiliate should review applicable services documentation, including the CJIS Implementation Guidance document. Enrolled Affiliate's compliance with the CJIS Policy will be dependent, in part, on Enrolled Affiliate's configuration of the services and adoption and implementation of policies and practices for its End Users' use of Covered Services as Enrolled Affiliate determines are appropriate in order for Enrolled Affiliate to comply with the CJIS Policy.

To facilitate scalable and effective delivery of the Covered Services to entities in the State that are qualified to purchase and use the Covered Services, such as Enrolled Affiliate, Enrolled Affiliate will rely upon the CSA to discharge certain requirements under the CJIS Policy on its behalf, and Microsoft will engage with the CSA if and as requested by the CSA, as set forth below.

Microsoft and Enrolled Affiliate have agreed certain requirements of the CJIS Policy will be fulfilled as set forth in the remainder of this section A, with provisions numbered to conform to the section numbering in the CJIS Policy.

1. 5.2 Policy Area 2: Security Awareness Training

Microsoft will supplement its existing security training program as required to meet the requirements of Section 5.2 of the CJIS Policy. Required training will be delivered to personnel identified as in scope for CJIS Personnel Screening within six (6) months of the later of (1) the date the first customer in State who is a purchaser of Covered Services subject to this Agreement (or a similar Agreement executed by the applicable Enrolled Affiliate) notifies Microsoft it is introducing CJI into the Covered Services, or (2) the date the CSA notifies Microsoft that personnel have passed required personnel screening. Microsoft will refresh training for in scope personnel on at least a biennial basis thereafter.

Microsoft will maintain training records, which will be available to the CSA upon written request.

2. 5.3 Policy Area 3: Incident Response

(a) If Microsoft becomes aware of any Security Incident, Microsoft will promptly: (i) notify Enrolled Affiliate of the Security Incident; (ii) investigate the Security Incident and provide Enrolled Affiliate with detailed information about the Security Incident; and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

(b) Enrolled Affiliate agrees that:

- (i)** An unsuccessful Security Incident will not be subject to this Section. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any Microsoft equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to

traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and

(ii) Microsoft's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

(c) Notification(s) of Security Incidents, if any, will be delivered to one or more of Enrolled Affiliate's administrators by any means Microsoft selects, including via email. It is Enrolled Affiliate's sole responsibility to ensure Enrolled Affiliate's administrators maintain accurate contact information on the Online Services portal at all times.

(d) Enrolled Affiliate acknowledges that effective investigation or mitigation of a Security Incident may be dependent upon information or services configurations within Enrolled Affiliate's control. Accordingly, compliance with CJIS Policy Incident Response requirements is a joint obligation of Microsoft and Enrolled Affiliate.

(e) Enrolled Affiliate will notify the CSA of a Security Incident if required under applicable requirements in State.

In the event Microsoft reasonably anticipates that a Security Incident may require legal action against involved individual(s) or where the Security Incident involves either civil or criminal action, Microsoft will conduct its investigative activities under guidance of legal staff and in accordance with applicable rules of evidence to the extent consistent with the primary incident response objectives of containing, resolving, and mitigating the impact of a Security Incident to customers including Enrolled Affiliate.

3. 5.11 Policy Area 11: Formal Audits

(a) Audits by FBI CJIS Division. In the event the FBI CJIS Division desires to perform an audit of the Covered Services, Microsoft will cooperate with such audit in good faith. The FBI may be permitted to access Customer Data belonging to Enrolled Affiliate in connection with such audit, but not data belonging to other customers in the multi-tenant environment from which the Covered Services are delivered. If the FBI identifies what it believes to be deficiencies in the Covered Services as a result of an audit, Microsoft is committed to working in good faith to resolve the FBI's concerns through discussion and interaction between Microsoft, the CSA, and the FBI. Enrolled Affiliate is committed to working in good faith to assist in this process if and as requested.

(b) Audits by Enrolled Affiliate. In the event that Enrolled Affiliate desires to audit the Covered Services pursuant to the CJIS Policy, Enrolled Affiliate appoints the CSA to act on Enrolled Affiliate's behalf to conduct such audit activities, and Enrolled Affiliate agrees to rely on the CSA for such purposes in full satisfaction of any Enrolled Affiliate right to audit the Covered Services. Enrolled Affiliate agrees that it is not authorized to conduct an audit of Microsoft's compliance with the CJIS Policy.

Enrolled Affiliate acknowledges the CSA will exercise this right by attempting to satisfy its requirements for information via reference to Microsoft's services documentation, including audit reports prepared by Microsoft's qualified third-party auditors. Along with other customers for the Covered Services, the CSA will be provided quarterly access to information generated by Microsoft's regular monitoring of security, privacy, and operational controls in place to afford applicable customers an ongoing view into effectiveness of such controls, and the CSA may

communicate with Microsoft subject matter experts. In the event the CSA reasonably determines this information is not sufficient for the CSA's or Enrolled Affiliate's audit objectives, then, upon the CSA's written request, Microsoft will provide the CSA or its qualified third party auditor the opportunity to communicate with Microsoft's auditor at the CSA's or Enrolled Affiliate's expense and, if required, a direct right to examine the Covered Services, including examination on premises. The CSA or its auditor may only access data belonging to Enrolled Affiliate or other entities in the State that have purchased the Covered Services and rely on the CSA for purposes of audit. The Enrolled Affiliate will be responsible for Microsoft's reasonable additional costs associated with such examination it appoints the CSA to perform, unless the CSA agrees to pay for such costs on Enrolled Affiliate's behalf.

(c) Confidentiality of Audit Materials. Information provided by Microsoft to the FBI CJIS Division or CSA in connection with audit activities will consist of highly confidential proprietary or trade secret information of Microsoft. Microsoft may request reasonable assurances, written or otherwise, that information will be maintained as confidential and/or trade secret prior to providing such information to Enrolled Affiliate, and Enrolled Affiliate will ensure Microsoft's audit materials, or report(s) created by Enrolled Affiliate based on a CSA audit of the Covered Services, are afforded the highest level of confidentiality available under applicable law.

4. 5.12 Policy Area 12: Personnel Security

(a) Enrolled Affiliate appoints the CSA to perform, and will rely upon CSA's completion of, personnel screening (i.e., background checks) for personnel in scope pursuant to Section 5.12 of the CJIS Policy. Enrolled Affiliate is responsible to confirm directly with the CSA that such personnel screening as the CSA or Enrolled Affiliate determines is required has been completed prior to initial processing of CJI Data in the Covered Services. Microsoft will support centralized screening by the CSA on behalf of all agencies or entities in the State that onboard to the Covered Services. Adjudication by Enrolled Affiliate or other counties, cities, or other subdivisions or agencies of state government will not be permitted.

(i) The CSA will define adjudication criteria for personnel screening for State.

(ii) To facilitate personnel screening by the CSA, Microsoft will deliver to the CSA relevant information regarding personnel who may in the anticipated scope of their duties have logical or physical access to CJI in the Covered Services.

(iii) It is not anticipated that the CSA will deliver to Enrolled Affiliate confidential personal information pertaining to Microsoft personnel. However, if Enrolled Affiliate receives such confidential personal information it will be afforded the highest level of confidentiality available under applicable law.

(iv) If Enrolled Affiliate elects to obtain services from Microsoft in addition to the Covered Services (e.g. consulting services in connection with Enrolled Affiliates' migration and onboarding to the Covered Services), such personnel will not be included in scope for personnel screening by the CSA unless separately agreed by Enrolled Affiliate, the CSA, and Microsoft.

(b) In the event the CSA approves a process under which a federal law enforcement agency or other suitable body conducts screening of personnel who have access to Customer Data in the Covered Services compliant with requirements of the CJIS Policy in lieu of CSA-conducted

screening, Enrolled Affiliate will abide by the CSA's approval of personnel screening being conducted in this manner.

(c) Microsoft's support of centralized screening by the CSA refers to Microsoft's personnel only and not Enrolled Affiliate's or CSA's personnel. If Enrolled Affiliate's employees will have unescorted access to unencrypted CJI (including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI), then Enrolled Affiliate is independent responsible for implementing the controls outlined in the CJIS Policy Area 12 (CJIS Policy Section 2.15).

(d) Enrolled Affiliate is solely responsible for conducting CJIS Policy background checks of Enrolled Affiliate's employees and shall not misrepresent Microsoft's commitment to CJIS background checks as applicable to Enrolled Affiliate's employees.

B. NCIC 2000 Operating Manual

Enrolled Affiliate acknowledges that the current NCIC 2000 Operating Manual consists of guidance and/or requirements for Enrolled Affiliate's use of the Covered Services. In the event Enrolled Affiliate determines the NCIC 2000 Operating Manual imposes obligations with respect to the Covered Services that can, in Enrolled Affiliate's opinion, only be satisfied via changes in the manner in which the Covered Services are operated or delivered to Enrolled Affiliate, Enrolled Affiliate may request that the CSA provide Microsoft with written notification of the specific changes it believes are required of Microsoft in order to enable Enrolled Affiliate's compliance with the NCIC 2000 Operating Manual, and Microsoft agrees to consider any such request(s) relayed to Microsoft by the CSA in good faith.

C. Notices

Any notices in connection with the Covered Services will be delivered to Enrolled Affiliate by Microsoft. Enrolled Affiliate will determine whether these or any other notices regarding the Covered Services are required to be delivered to the FBI, CJIS Division, as contemplated in Section 6.05 of the Security Addendum and, if required, deliver such notices.



Microsoft Privacy Statement

Last Updated: June 2022 [What's new?](#)

Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products for a variety of purposes described below, including to operate effectively and provide you with the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, administer your organization's licensing account, submit a search query to Bing, register for a Microsoft event, speak a voice command to Cortana, upload a document to OneDrive, sign up for Microsoft 365, or contact us for support. We get some of it by collecting data about your interactions, use, and experience with our products and communications.

We rely on a variety of legal reasons and permissions (sometimes called "legal bases") to process data, including with your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with legal obligations, for a variety of purposes described below.

We also obtain data from third parties. We protect data obtained from third parties according to the practices described in this statement, plus any additional restrictions imposed by the source of the data. These third-party sources vary over time and include:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Services that make user-generated content from their service available to others, such as local business reviews or public social media posts.
- Communication services, including email providers and social networks, when you give us permission to access your data on such third-party services or networks.
- Service providers that help us determine your device's location.
- Partners with which we offer co-branded services or engage in joint marketing activities.
- Developers who create experiences through or for Microsoft products.
- Third parties that deliver experiences through Microsoft products. Publicly-available sources, such as open public sector, academic, and commercial data sets and other data sources.

If you represent an organization, such as a business or school, that utilizes Enterprise and Developer Products from Microsoft, please see the [Enterprise and developer products](#) section of this privacy statement to learn how we process your data. If you are an end user of a Microsoft product or a Microsoft account provided by your organization, please see the [Products provided by your organization](#) and the [Microsoft account](#) sections for more information.

You have choices when it comes to the technology you use and the data you share. When you are asked to provide personal data, you can decline. Many of our products require some personal data to operate and provide you with a service. If you choose not to provide data required to operate and provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you're using, we may have to suspend or cancel it. We will notify you if this is the case at the time. Where providing the data is optional, and you choose not to share personal data, features like personalization that use the data will not work for you.

The data we collect depends on the context of your interactions with Microsoft and the choices you make (including your privacy settings), the products and features you use, your location, and applicable law.

The data we collect can include the following:

Name and contact data. Your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. Passwords, password hints, and similar security information used for authentication and account access.

Demographic data. Data about you such as your age, gender, country, and preferred language.

Payment data. Data to process payments, such as your payment instrument number (such as a credit card number) and the security code associated with your payment instrument.

Subscription and licensing data. Information about your subscriptions, licenses, and other entitlements.

Interactions. Data about your use of Microsoft products. In some cases, such as search queries, this is data you provide in order to make use of the products. In other cases, such as error reports, this is data we generate. Other examples of interactions data include:

- **Device and usage data.** Data about your device and the product and features you use, including information about your hardware and software, how our products perform, as well as your settings. For example:
 - **Payment and account history.** Data about the items you purchase and activities associated with your account.
 - **Browse history.** Data about the webpages you visit.
 - **Device, connectivity, and configuration data.** Data about your device, your device configuration, and nearby networks. For example, data about the operating systems and other software installed on your device, including product keys. In addition, IP address,

device identifiers (such as the IMEI number for phones), regional and language settings, and information about WLAN access points near your device.

- **Error reports and performance data.** Data about the performance of the products and any problems you experience, including error reports. Error reports (sometimes called “crash dumps”) can include details of the software or hardware related to an error, contents of files opened when an error occurred, and data about other software on your device.
- **Troubleshooting and help data.** Data you provide when you contact Microsoft for help, such as the products you use, and other details that help us provide support. For example, contact or authentication data, the content of your chats and other communications with Microsoft, data about the condition of your device, and the products you use related to your help inquiry. When you contact us, such as for customer support, phone conversations or chat sessions with our representatives may be monitored and recorded.
- **Bot usage data.** Interactions with third party bots and skills available through Microsoft products.
- ◆ **Interests and favorites.** Data about your interests and favorites, such as the sports teams you follow, the programming languages you prefer, the stocks you track, or cities you add to track things like weather or traffic. In addition to those you explicitly provide, your interests and favorites can also be inferred or derived from other data we collect.
- ◆ **Content consumption data.** Information about media content (e.g., TV, video, music, audio, text books, apps, and games) you access through our products.
- ◆ **Searches and commands.** Search queries and commands when you use Microsoft products with search or related productivity functionality.
- ◆ **Voice data.** Your voice data, sometimes referred to as “voice clips”, such as search queries, commands, or dictation you speak, which may include background sounds.
- ◆ **Text, inking, and typing data.** Text, inking, and typing data and related information. For example, when we collect inking data, we collect information about the placement of your inking instrument on your device.
- ◆ **Images.** Images and related information, such as picture metadata. For example, we collect the image you provide when you use a Bing image-enabled service.
- ◆ **Contacts and relationships.** Data about your contacts and relationships if you use a product to share information with others, manage contacts, communicate with others, or improve your productivity.
- ◆ **Social data.** Information about your relationships and interactions between you, other people, and organizations, such as types of engagement (e.g., likes, dislikes, events, etc.) related to people and organizations.
- ◆ **Location data.** Data about your device’s location, which can be either precise or imprecise. For example, we collect location data using Global Navigation Satellite System (GNSS) (e.g., GPS) and data about nearby cell towers and Wi-Fi hotspots. Location can also be inferred from a device’s IP address or data in your account profile that indicates where it is located with less precision, such as at a city or postal code level.
- ◆ **Other input.** Other inputs provided when you use our products. For example, data such as the buttons you press on an Xbox wireless controller using the Xbox network, skeletal tracking data when you use Kinect, and other sensor data, like the number of steps you take, when you use devices that have applicable sensors. And, if you use Spend, at your direction, we also collect financial transaction data from your credit card issuer to provide the service. If you attend an in-

store event, we collect the data you provide to us when registering for or during the event and if you enter into a prize promotion, we collect the data you input into the entry form.

Content. Content of your files and communications you input, upload, receive, create, and control. For example, if you transmit a file using Skype to another Skype user, we need to collect the content of that file to display it to you and the other user. If you receive an email using Outlook.com, we need to collect the content of that email to deliver it to your inbox, display it to you, enable you to reply to it, and store it for you until you choose to delete it. Other content we collect when providing products to you include:

- Communications, including audio, video, text (typed, inked, dictated, or otherwise), in a message, email, call, meeting request, or chat.
- Photos, images, songs, movies, software, and other media or documents you store, retrieve, or otherwise process with our cloud.

Video or recordings. Recordings of events and activities at Microsoft buildings, retail spaces, and other locations. If you enter Microsoft Store locations or other facilities, or attend a Microsoft event that is recorded, we may process your image and voice data.

Feedback and ratings. Information you provide to us and the content of messages you send to us, such as feedback, survey data, and product reviews you write.

Traffic data. Data generated through your use of Microsoft's communications services. Traffic data indicates with whom you have communicated and when your communications occurred. We will process your traffic data only as required to provide, maintain, and improve our communications services and we do so with your consent.

Product-specific sections below describe data collection practices applicable to use of those products.

How we use personal data

Microsoft uses the data we collect to provide you rich, interactive experiences. In particular, we use data to:

- Provide our products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions you request.
- Improve and develop our products.
- Personalize our products and make recommendations.
- Advertise and market to you, which includes sending promotional communications, targeting advertising, and presenting you relevant offers.

We also use the data to operate our business, which includes analyzing our performance, meeting our legal obligations, developing our workforce, and doing research.

For these purposes, we combine data we collect from different contexts (for example, from your use of two Microsoft products). For example, Cortana may use information from your calendar to suggest

action items in a heads-up email, and Microsoft Store uses information about the apps and services you use to make personalized app recommendations. However, we have built in technological and procedural safeguards designed to prevent certain data combinations where required by law. For example, where required by law, we store data we collect from you when you are unauthenticated (not signed in) separately from any account information that directly identifies you, such as your name, email address, or phone number.

Our processing of personal data for these purposes includes both automated and manual (human) methods of processing. Our automated methods often are related to and supported by our manual methods. For example, our automated methods include artificial intelligence (AI), which we think of as a set of technologies that enable computers to perceive, learn, reason, and assist in decision-making to solve problems in ways that are similar to what people do. To build, train, and improve the accuracy of our automated methods of processing (including AI), we manually review some of the predictions and inferences produced by the automated methods against the underlying data from which the predictions and inferences were made. For example, we manually review short snippets of voice data that we have taken steps to de-identify to improve our speech recognition technologies. This manual review may be conducted by Microsoft employees or vendors who are working on Microsoft's behalf.

When we process personal data about you, we do so with your consent and/or as required to provide the products you use, operate our business, meet our contractual and legal obligations, protect the security of our systems and our customers, or fulfill other legitimate interests of Microsoft as described in this section and in the [Reasons we share personal data](#) section of this privacy statement. When we transfer personal data from the European Economic Area, we do so based on a variety of legal mechanisms, as described in the [Where we store and process personal data](#) section of this privacy statement.

More on the purposes of processing:

- ♦ **Provide our products.** We use data to operate our products and provide you with rich, interactive experiences. For example, if you use OneDrive, we process the documents you upload to OneDrive to enable you to retrieve, delete, edit, forward, or otherwise process it, at your direction as part of the service. Or, for example, if you enter a search query in the Bing search engine, we use that query to display search results to you. Additionally, as communications are a feature of various products, programs, and activities, we use data to contact you. For example, we may contact you by phone or email or other means to inform you when a subscription is ending or discuss your licensing account. We also communicate with you to secure our products, for example by letting you know when product updates are available.
- ♦ **Product improvement.** We use data to continually improve our products, including adding new features or capabilities. For example, we use error reports to improve security features, search queries and clicks in Bing to improve the relevancy of the search results, usage data to determine what new features to prioritize, and voice data to develop and improve speech recognition accuracy.
- ♦ **Personalization.** Many products include personalized features, such as recommendations that enhance your productivity and enjoyment. These features use automated processes to tailor your product experiences based on the data we have about you, such as inferences we make about you and your use of the product, activities, interests, and location. For example, depending on your settings, if you stream movies in a browser on your Windows device, you may see a

recommendation for an app from the Microsoft Store that streams more efficiently. If you have a Microsoft account, with your permission, we can sync your settings on several devices. Many of our products provide controls to disable personalized features.

- ♦ **Product activation.** We use data—such as device and application type, location, and unique device, application, network, and subscription identifiers—to activate products that require activation.
- ♦ **Product development.** We use data to develop new products. For example, we use data, often de-identified, to better understand our customers' computing and productivity needs which can shape the development of new products.
- ♦ **Customer support.** We use data to troubleshoot and diagnose product problems, repair customers' devices, and provide other customer care and support services, including to help us provide, improve, and secure the quality of our products, services, and training, and to investigate security incidents. Call recording data may also be used to authenticate or identify you based on your voice to enable Microsoft to provide support services and investigate security incidents.
- ♦ **Help secure and troubleshoot.** We use data to help secure and troubleshoot our products. This includes using data to protect the security and safety of our products and customers, detecting malware and malicious activities, troubleshooting performance and compatibility issues to help customers get the most out of their experiences, and notifying customers of updates to our products. This may include using automated systems to detect security and safety issues.
- ♦ **Safety.** We use data to protect the safety of our products and our customers. Our security features and products can disrupt the operation of malicious software and notify users if malicious software is found on their devices. For example, some of our products, such as Outlook.com or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, abusive actions, or URLs that have been flagged as fraud, phishing, or malware links; and we reserve the right to block delivery of a communication or remove content if it violates our terms. **In accordance with European Union Regulation (EU) 2021/1232, we have invoked the derogation permitted by that Regulation from Articles 5(1) and 6(1) of EU Directive 2002/58/EC. We use scanning technologies to create digital signatures (known as "hashes") of certain images and video content on our systems. These technologies then compare the hashes they generate with hashes of reported child sexual exploitation and abuse imagery (known as a "hash set"), in a process called "hash matching". Microsoft obtains hash sets from organizations that act in the public interest against child sex abuse. This can result in sharing information with the National Center for Missing and Exploited Children (NCMEC) and law enforcement authorities.**
- ♦ **Updates.** We use data we collect to develop product updates and security patches. For example, we may use information about your device's capabilities, such as available memory, to provide you a software update or security patch. Updates and patches are intended to maximize your experience with our products, help you protect the privacy and security of your data, provide new features, and evaluate whether your device is ready to process such updates.
- ♦ **Promotional communications.** We use data we collect to deliver promotional communications. You can sign up for email subscriptions and choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. For information about managing your contact data, email subscriptions, and promotional communications, see the [How to access and control your personal data](#) section of this privacy statement.

- ♦ **Relevant offers.** Microsoft uses data to provide you with relevant and valuable information regarding our products. We analyze data from a variety of sources to predict the information that will be most interesting and relevant to you and deliver such information to you in a variety of ways. For example, we may predict your interest in gaming and communicate with you about new games you may like.
- ♦ **Advertising.** Microsoft does not use what you say in email, chat, video calls, or voice mail, or your documents, photos, or other personal files to target ads to you. We use data we collect through our interactions with you, through some of our products, and on third-party web properties, for advertising in our products and on third-party properties. We may use automated processes to help make advertising more relevant to you. For more information about how your data is used for advertising, see the [Advertising](#) section of this privacy statement.
- ♦ **Prize promotions and events.** We use your data to administer prize promotions and events available in our physical Microsoft Stores. For example, if you enter into a prize promotion, we may use your data to select a winner and provide the prize to you if you win. Or, if you register for a coding workshop or gaming event, we will add your name to the list of expected attendees.
- ♦ **Transacting commerce.** We use data to carry out your transactions with us. For example, we process payment information to provide customers with product subscriptions and use contact information to deliver goods purchased from the Microsoft Store.
- ♦ **Reporting and business operations.** We use data to analyze our operations and perform business intelligence. This enables us to make informed decisions and report on the performance of our business.
- ♦ **Protecting rights and property.** We use data to detect and prevent fraud, resolve disputes, enforce agreements, and protect our property. For example, we use data to confirm the validity of software licenses to reduce piracy. We may use automated processes to detect and prevent activities that violate our rights and the rights of others, such as fraud.
- ♦ **Legal compliance.** We process data to comply with law. For example, we use the age of our customers to assist us in meeting our obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.
- ♦ **Research.** With appropriate technical and organizational measures to safeguard individuals' rights and freedoms, we use data to conduct research, including for public interest and scientific purposes.

Reasons we share personal data

We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorized. For example, we share your content with third parties when you tell us to do so, such as when you send an email to a friend, share photos and documents on OneDrive, or link accounts with another service. If you use a Microsoft product provided by an organization you are affiliated with, such as an employer or school, or use an email address provided by such organization to access Microsoft products, we share certain data, such as interaction data and diagnostic data to enable your organization to manage the products. When you provide payment data to make a purchase, we will share payment data with banks and other entities that process payment transactions or provide other financial services, and for fraud prevention and credit risk reduction.

In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction such as a merger or sale of assets.

Finally, we will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following:

- Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.
- Protect our customers, for example, to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone.
- Operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks.
- Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services—however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement.

For more information about data we disclose in response to requests from law enforcement and other government agencies, please see our [Law Enforcement Requests Report](#).

Please note that some of our products include links to or otherwise enable you to access products of third parties whose privacy practices differ from those of Microsoft. If you provide personal data to any of those products, your data is governed by their privacy policies.

How to access and control your personal data

You can also make choices about the collection and use of your data by Microsoft. You can control your personal data that Microsoft has obtained, and exercise your data protection rights, by contacting Microsoft or using various tools we provide. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law. How you can access or control your personal data will also depend on which products you use. For example, you can:

- Control the use of your data for interest-based advertising from Microsoft by visiting our [opt-out page](#).
- Choose whether you wish to receive promotional emails, SMS messages, telephone calls, and postal mail from Microsoft.
- Access and clear some of your data through the [Microsoft privacy dashboard](#).

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools

above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the [How to contact us](#) section or by using our [web form](#).

We provide aggregate metrics about user requests to exercise their data protection rights via the [Microsoft Privacy Report](#).

You can access and control your personal data that Microsoft has obtained with tools Microsoft provides to you, which are described below, or by contacting Microsoft. For instance:

- If Microsoft obtained your consent to use your personal data, you can withdraw that consent at any time.
- You can request access to, erasure of, and updates to your personal data.
- If you'd like to port your data elsewhere, you can use tools Microsoft provides to do so, or if none are available, you can contact Microsoft for assistance.

You can also object to or restrict the use of your personal data by Microsoft. For example, you can object at any time to our use of your personal data:

- For direct marketing purposes.
- Where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party.

You may have these rights under applicable laws, including the EU General Data Protection Regulation (GDPR), but we offer them regardless of your location. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law.

If your organization, such as your employer, school, or service provider, provides you with access to and is administering your use of Microsoft products, contact your organization to learn more about how to access and control your personal data.

You can access and control your personal data that Microsoft has obtained, and exercise your data protection rights, using various tools we provide. The tools most useful to you will depend on our interactions with you and your use of our products. Here is a general list of tools we provide to help you control your personal data; specific products may provide additional controls.

- **Bing.** If you are signed into Bing, you can view and clear your search history on your [privacy dashboard](#). If you are not signed into Bing, you can view and clear search history associated to your device in your [Bing settings](#).
- **Cortana.** You can control some of the data Cortana accesses or stores in your [Cortana settings](#).
- **Microsoft account.** If you wish to access, edit, or remove the profile information and payment information in your Microsoft account, change your password, add security information or close your account, you can do so by visiting the [Microsoft account website](#).
- If you have a **Microsoft Developer Network** (MSDN) public profile, you can access and edit your data by signing in at [MSDN forum](#).
- **Microsoft privacy dashboard.** You can control some of the data Microsoft processes through your use of a Microsoft account on the [Microsoft privacy dashboard](#). From here, for example, you can view and clear the browsing, search, and location data associated with your Microsoft account.

- ♦ **Microsoft Store.** You can access your Microsoft Store profile and account information by visiting [Microsoft Store](#) and selecting **View account** or **Order history**.
- ♦ **Microsoft Teams for personal use.** You can find out how to export or delete Teams data relating to your personal Microsoft account by visiting this [page](#).
- ♦ **OneDrive.** You can view, download, and delete your files and photos in OneDrive by signing into your [OneDrive](#).
- ♦ **Outlook.com.** You can download your emails in [Outlook.com](#) by signing into your account and navigating to your **Privacy and data** settings.
- ♦ **Skype.** If you wish to access, edit, or remove some profile and payment information for Skype or change your password, [sign in to your account](#). If you wish to export your Skype chat history and files shared on Skype, you can [request a copy](#).
- ♦ **Volume Licensing Service Center (VLSC).** If you are a Volume Licensing customer, you can control your contact information and subscription and licensing data in one location by visiting the [Volume Licensing Service Center website](#).
- ♦ **Xbox.** If you use the Xbox network or Xbox.com, you can view or edit your personal data, including billing and account information, privacy settings, and online safety and data sharing preferences by accessing [My Xbox](#) on the Xbox console or on the Xbox.com website.

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the [How to contact us](#) section or by using our [web form](#). We will respond to requests to control your personal data as required by applicable law.

Your communications preferences

You can choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. If you receive promotional email or SMS messages from us and would like to opt out, you can do so by following the directions in that message. You can also make choices about the receipt of promotional email, telephone calls, and postal mail by signing in with your personal Microsoft account, and viewing your [communication permissions](#) where you can update contact information, manage Microsoft-wide contact preferences, opt out of email subscriptions, and choose whether to share your contact information with Microsoft partners. If you do not have a personal Microsoft account, you can manage your Microsoft email contact preferences by using this [web form](#). These choices do not apply to mandatory service communications that are part of certain Microsoft products, programs, activities, or to surveys or other informational communications that have their own unsubscribe method.

Your advertising choices

To opt out of receiving interest-based advertising from Microsoft, visit our [opt-out page](#). When you opt out, your preference is stored in a cookie that is specific to the web browser you are using. The opt-out cookie has an expiration date of five years. If you delete the cookies on your device, you need to opt out again.

You can also link your opt-out choice with your personal Microsoft account. It will then apply on any device where you use that account and will continue to apply until someone signs in with a different

personal Microsoft account on that device. If you delete the cookies on your device, you will need to sign in again for the settings to apply.

For Microsoft-controlled advertising that appears in apps on Windows, you may use the opt-out linked to your personal Microsoft account, or opt out of interest-based advertising by turning off the advertising ID in Windows settings.

Because the data used for interest-based advertising is also used for other required purposes (including providing our products, analytics, and fraud detection), opting out of interest-based advertising does not stop that data collection. You will continue to get ads, although they may be less relevant to you.

You can opt out of receiving interest-based advertising from third parties we partner with by visiting their sites (see above).

Browser-based controls

When you use a browser, you can control your personal data using certain features. For example:

- **Cookie controls.** You can control the data stored by cookies and withdraw consent to cookies by using the browser-based cookie controls described in the [Cookies](#) section of this privacy statement.
- **Tracking protections.** You can control the data third-party sites can collect about you using Tracking Protection in Internet Explorer (versions 9 and up) and Microsoft Edge. This feature will block third-party content, including cookies, from any site that is listed in a Tracking Protection List you add.
- **Browser controls for "Do Not Track."** Some browsers have incorporated "Do Not Track" (DNT) features that can send a signal to the websites you visit indicating you do not wish to be tracked. Because there is not yet a common understanding of how to interpret the DNT signal, Microsoft services do not currently respond to browser DNT signals. We continue to work with the online industry to define a common understanding of how to treat DNT signals. In the meantime, you can use the range of other tools we provide to control data collection and use, including the ability to opt out of receiving interest-based advertising from Microsoft as described above.

Cookies and similar technologies

Cookies are small text files placed on your device to store data that can be recalled by a web server in the domain that placed the cookie. This data often consists of a string of numbers and letters that uniquely identifies your computer, but it can contain other information as well. Some cookies are placed by third parties acting on our behalf. We use cookies and similar technologies to store and honor your preferences and settings, enable you to sign-in, provide interest-based advertising, combat fraud, analyze how our products perform, and fulfill other legitimate purposes described below. Microsoft apps use additional identifiers, such as the advertising ID in Windows, for similar purposes, and many of our websites and applications also contain web beacons or other similar technologies, as described below.

Our use of cookies and similar technologies

Microsoft uses cookies and similar technologies for several purposes, depending on the context or product, including:

- **Storing your preferences and settings.** We use cookies to store your preferences and settings on your device, and to enhance your experiences. For example, depending on your settings, if you enter your city or postal code to get local news or weather information on a Microsoft website, we store that data in a cookie so that you will see the relevant local information when you return to the site. Saving your preferences with cookies, such as your preferred language, prevents you from having to set your preferences repeatedly. If you opt out of interest-based advertising, we store your opt-out preference in a cookie on your device. Similarly, in scenarios where we obtain your consent to place cookies on your device, we store your choice in a cookie.
- **Sign-in and authentication.** We use cookies to authenticate you. When you sign in to a website using your personal Microsoft account, we store a unique ID number, and the time you signed in, in an encrypted cookie on your device. This cookie allows you to move from page to page within the site without having to sign in again on each page. You can also save your sign-in information so you do not have to sign in each time you return to the site.
- **Security.** We use cookies to process information that helps us secure our products, as well as detect fraud and abuse.
- **Storing information you provide to a website.** We use cookies to remember information you shared. When you provide information to Microsoft, such as when you add products to a shopping cart on Microsoft websites, we store the data in a cookie for the purpose of remembering the information.
- **Social media.** Some of our websites include social media cookies, including those that enable users who are signed in to the social media service to share content via that service.
- **Feedback.** Microsoft uses cookies to enable you to provide feedback on a website.
- **Interest-based advertising.** Microsoft uses cookies to collect data about your online activity and identify your interests so that we can provide advertising that is most relevant to you. You can opt out of receiving interest-based advertising from Microsoft as described in the [How to access and control your personal data](#) section of this privacy statement.
- **Showing advertising.** Microsoft uses cookies to record how many visitors have clicked on an advertisement and to record which advertisements you have seen, for example, so you do not see the same one repeatedly.
- **Analytics.** We use first- and third-party cookies and other identifiers to gather usage and performance data. For example, we use cookies to count the number of unique visitors to a web page or service and to develop other statistics about the operations of our products.
- **Performance.** Microsoft uses cookies to understand and improve how our products perform. For example, we use cookies to gather data that helps with load balancing; this helps us keep our websites remain up and running.

Where required, we obtain your consent prior to placing or using optional cookies that are not (i) strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication. Please see the "How to Control Cookies" section below for more information.

Some of the cookies we commonly use are listed below. This list is not exhaustive, but it is intended to illustrate the primary purposes for which we typically set cookies. If you visit one of our websites, the site will set some or all of the following cookies:

- **MSCC.** Contains user choices for most Microsoft properties.
- **MUID, MC1, and MSFPC.** Identifies unique web browsers visiting Microsoft sites. These cookies are used for advertising, site analytics, and other operational purposes.
- **ANON.** Contains the ANID, a unique identifier derived from your Microsoft account, which is used for advertising, personalization, and operational purposes. It is also used to preserve your choice to opt out of interest-based advertising from Microsoft if you have chosen to associate the opt-out with your Microsoft account.
- **CC.** Contains a country code as determined from your IP address.
- **PPAuth, MSPAuth, MSNRPSAuth, KievRPSAuth, WLSSC, MSPPProf.** Helps to authenticate you when you sign in with your Microsoft account.
- **MC0.** Detects whether cookies are enabled in the browser.
- **MS0.** Identifies a specific session.
- **NAP.** Contains an encrypted version of your country, postal code, age, gender, language and occupation, if known, based on your Microsoft account profile.
- **MH.** Appears on co-branded sites where Microsoft is partnering with an advertiser. This cookie identifies the advertiser, so the right ad is selected.
- **childinfo, kcdob, kcrelid, kcru, pcfm.** Contains information that Microsoft account uses within its pages in relation to child accounts.
- **MR.** This cookie is used by Microsoft to reset or refresh the MUID cookie.
- **x-ms-gateway-slice.** Identifies a gateway for load balancing.
- **TOptOut.** Records your decision not to receive interest-based advertising delivered by Microsoft. Where required, we place this cookie by default and remove it when you consent to interest-based advertising.

In addition to the cookies Microsoft sets when you visit our websites, third parties can also set cookies when you visit Microsoft sites. For example:

- Companies we hire to provide services on our behalf, such as site analytics, place cookies when you visit our sites.
- Companies that deliver content, such as videos or news, or ads on Microsoft sites, place cookies on their own. These companies use the data they process in accordance with their privacy policies, which may enable these companies to collect and combine information about your activities across websites, apps, or online services.

For a list of the third parties that set cookies on our websites, including service providers acting on our behalf, please visit our [third party cookie inventory](#). On some of our websites, a list of third parties is available directly on the site. The third parties on these sites may not be included in the list on our [third party cookie inventory](#).

How to control cookies

Most web browsers automatically accept cookies but provide controls that allow you to block or delete them. For example, in Microsoft Edge, you can block or delete cookies by selecting **Settings** > **Privacy and services** > **Clear Browsing data** > **Cookies and other site data**. For more information about how to delete your cookies in Microsoft browsers, see [Microsoft Edge](#), [Microsoft Edge Legacy](#) or [Internet Explorer](#). If you use a different browser, refer to that browser's instructions.

As mentioned above, where required, we obtain your consent before placing or using optional cookies that are not (i) strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication. We separate these optional cookies by purpose, such as for advertising and social media purposes. You may consent to certain categories of optional cookies and not others. You also may adjust your choices by clicking “Manage cookies” in the footer of the website or through the settings made available on the website. Certain features of Microsoft products depend on cookies. If you choose to block cookies, you cannot sign in or use some of those features, and preferences that are dependent on cookies will be lost. If you choose to delete cookies, any settings and preferences controlled by those cookies, including advertising preferences, are deleted and will need to be recreated.

Certain features of Microsoft products depend on cookies. If you choose to block cookies, you cannot sign in or use some of those features, and preferences that are dependent on cookies will be lost. If you choose to delete cookies, any settings and preferences controlled by those cookies, including advertising preferences, are deleted and will need to be recreated.

Additional privacy controls that can impact cookies, including the tracking protections feature of Microsoft browsers, are described in the [How to access and control your personal data](#) section of this privacy statement.

Our use of web beacons and analytics services

Some Microsoft webpages contain electronic tags known as web beacons that we use to help deliver cookies on our websites, count users who have visited those websites, and deliver co-branded products. We also include web beacons or similar technologies in our electronic communications to determine whether you open and act on them.

In addition to placing web beacons on our own websites, we sometimes work with other companies to place our web beacons on their websites or in their advertisements. This helps us to, for example, develop statistics on how often clicking on an advertisement on a Microsoft website results in a purchase or other action on the advertiser's website. It also allows us to understand your activity on the website of a Microsoft partner in connection with your use of a Microsoft product or service.

Finally, Microsoft products often contain web beacons or similar technologies from third-party analytics providers, which help us compile aggregated statistics about the effectiveness of our promotional campaigns or other operations. These technologies enable the analytics providers to set or read their own cookies or other identifiers on your device, through which they can collect information about your online activities across applications, websites, or other products. However, we prohibit these analytics providers from using web beacons on our sites to collect or access information that directly identifies you (such as your name or email address). You can opt out of data collection or use by some of these analytics providers by visiting any of the following sites: [Adjust](#), [AppsFlyer](#), [Clicktale](#), [Flurry Analytics](#), [Google Analytics](#) (requires you to install a browser add-on), [Kissmetrics](#), [Mixpanel](#), [Nielsen](#), [Acuity Ads](#), [WebTrends](#) or [Optimizely](#).

Other similar technologies

In addition to standard cookies and web beacons, our products can also use other similar technologies to store and read data files on your computer. This is typically done to maintain your preferences or to

improve speed and performance by storing certain files locally. But, like standard cookies, these technologies can also store a unique identifier for your computer, which can then track behavior. These technologies include Local Shared Objects (or "Flash cookies") and Silverlight Application Storage.

Local Shared Objects or "Flash cookies." Websites that use Adobe Flash technologies can use Local Shared Objects or "Flash cookies" to store data on your computer. To learn how to manage or block Flash cookies, go to the [Flash Player help page](#).

Silverlight Application Storage. Websites or applications that use Microsoft Silverlight technology also have the ability to store data by using Silverlight Application Storage. To learn how to manage or block such storage, see the [Silverlight](#) section of this privacy statement.

Products provided by your organization—notice to end users

If you use a Microsoft product with an account provided by an organization you are affiliated with, such as your work or school account, that organization can:

- Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.
- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

If you lose access to your work or school account (in event of change of employment, for example), you may lose access to products and the content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such products.

Many Microsoft products are intended for use by organizations, such as schools and businesses. Please see the [Enterprise and developer products](#) section of this privacy statement. If your organization provides you with access to Microsoft products, your use of the Microsoft products is subject to your organization's policies, if any. You should direct your privacy inquiries, including any requests to exercise your data protection rights, to your organization's administrator. When you use social features in Microsoft products, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation or help content specific to the Microsoft product. Microsoft is not responsible for the privacy or security practices of our customers, which may differ from those set forth in this privacy statement.

When you use a Microsoft product provided by your organization, Microsoft's processing of your personal data in connection with that product is governed by a contract between Microsoft and your organization. Microsoft processes your personal data to provide the product to your organization and you, and in some cases for Microsoft's business operations related to providing the product as described in the [Enterprise and developer products](#) section. As mentioned above, if you have questions about Microsoft's processing of your personal data in connection with providing products to your organization, please contact your organization. If you have questions about Microsoft's business operations in connection with providing products to your organization as provided in the

Product Terms, please contact Microsoft as described in the [How to contact us](#) section. For more information on our business operations, please see the [Enterprise and developer products](#) section.

For Microsoft products provided by your K-12 school, including Microsoft 365 Education, Microsoft will:

- not collect or use student personal data beyond that needed for authorized educational or school purposes;
- not sell or rent student personal data;
- not use or share student personal data for advertising or similar commercial purposes, such as behavioral targeting of advertisements to students;
- not build a personal profile of a student, other than for supporting authorized educational or school purposes or as authorized by the parent, guardian, or student of appropriate age; and
- require that our vendors with whom student personal data is shared to deliver the educational service, if any, are obligated to implement these same commitments for student personal data.

Microsoft account

With a Microsoft account, you can sign into Microsoft products, as well as those of select Microsoft partners. Personal data associated with your Microsoft account includes credentials, name and contact data, payment data, device and usage data, your contacts, information about your activities, and your interests and favorites. Signing into your Microsoft account enables personalization, consistent experiences across products and devices, permits you to use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account, and enables other features. There are three types of Microsoft account:

- When you create your own Microsoft account tied to your personal email address, we refer to that account as a **personal Microsoft account**.
- When you or your organization (such as an employer or your school) create your Microsoft account tied to your email address provided by that organization, we refer to that account as a **work or school account**.
- When you or your service provider (such as a cable or internet service provider) create your Microsoft account tied to your email address with your service provider's domain, we refer to that account as a **third-party account**.

Personal Microsoft accounts. The data associated with your personal Microsoft account, and how that data is used, depends on how you use the account.

- **Creating your Microsoft account.** When you create a personal Microsoft account, you will be asked to provide certain personal data and we will assign a unique ID number to identify your account and associated information. While some products, such as those involving payment, require a real name, you can sign in to and use other Microsoft products without providing your real name. Some data you provide, such as your display name, email address, and phone number, can be used to help others find and connect with you within Microsoft products. For example, people who know your display name, email address, or phone number can use it to search for you on Skype or Microsoft Teams for personal use and send you an invite to connect

with them. Note that if you use a work or school email address to create a personal Microsoft account, your employer or school may gain access to your data. In some cases, you will need to change the email address to a personal email address in order to continue accessing consumer-oriented products (such as the Xbox network).

- **Signing in to Microsoft account.** When you sign in to your Microsoft account, we create a record of your sign-in, which includes the date and time, information about the product you signed in to, your sign-in name, the unique number assigned to your account, a unique identifier assigned to your device, your IP address, and your operating system and browser version.
- **Signing in to Microsoft products.** Signing in to your account enables improved personalization, provides seamless and consistent experiences across products and devices, permits you to access and use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account, and enables other enhanced features and settings. When you sign in to your account, you will stay signed in until you sign out. If you add your Microsoft account to a Windows device (version 8 or higher), Windows will automatically sign you in to products that use Microsoft account when you access those products on that device. When you are signed in, some products will display your name or username and your profile photo (if you have added one to your profile) as part of your use of Microsoft products, including in your communications, social interactions, and public posts.
- **Signing in to third-party products.** If you sign in to a third-party product with your Microsoft account, you will share data with the third party in accordance with the third party's privacy policy. The third party will also receive the version number assigned to your account (a new version number is assigned each time you change your sign-in data); and information that describes whether your account has been deactivated. If you share your profile data, the third party can display your name or user name and your profile photo (if you have added one to your profile) when you are signed in to that third-party product. If you chose to make payments to third-party merchants using your Microsoft account, Microsoft will pass information stored in your Microsoft account to the third party or its vendors (e.g., payment processors) as necessary to process your payment and fulfill your order (such as name, credit card number, billing and shipping addresses, and relevant contact information). The third party can use or share the data it receives when you sign in or make a purchase according to its own practices and policies. **You should carefully review the privacy statement for each product you sign in to and each merchant you purchase from to determine how it will use the data it collects.**

Work or school accounts. The data associated with a work or school account, and how it will be used, is generally similar to the use and collection of data associated with a personal Microsoft account.

If your employer or school uses Azure Active Directory (AAD) to manage the account it provides you, you can use your work or school account to sign in to Microsoft products, such as Microsoft 365 and Office 365, and third-party products provided to you by your organization. If required by your organization, you will also be asked to provide a phone number or an alternative email address for additional security verification. And, if allowed by your organization, you may also use your work or school account to sign in to Microsoft or third-party products that you acquire for yourself.

If you sign in to Microsoft products with a work or school account, note:

- The owner of the domain associated with your email address may control and administer your account, and access and process your data, including the contents of your communications and

files, including data stored in products provided to you by your organization, and products you acquire by yourself.

- Your use of the products is subject to your organization's policies, if any. You should consider both your organization's policies and whether you are comfortable enabling your organization to access your data before you choose to use your work or school account to sign in to products you acquire for yourself.
- If you lose access to your work or school account (if you change employers, for example), you may lose access to products, including content associated with those products, you acquired on your own behalf if you used your work or school account to sign in to such products.
- Microsoft is not responsible for the privacy or security practices of your organization, which may differ from those of Microsoft.
- If your organization is administering your use of Microsoft products, please direct your privacy inquiries, including any requests to exercise your data subject rights, to your administrator. See also the [Notice to end users](#) section of this privacy statement.
- If you are uncertain whether your account is a work or school account, please contact your organization.

Third-party accounts. The data associated with a third-party Microsoft account, and how it will be used, is generally similar to the use and collection of data associated with a personal Microsoft account. Your service provider has control over your account, including the ability to access or delete your account. **You should carefully review the terms the third party provided you to understand what it can do with your account.**

Collection of data from children

When a Microsoft product collects age, and there is an age in your jurisdiction under which parental consent or authorization is required to use the product, the product will either block users under that age or will ask them to provide consent or authorization from a parent or guardian before they can use it. We will not knowingly ask children under that age to provide more data than is required to provide for the product.

Once parental consent or authorization is granted, the child's account is treated much like any other account. The child can access communication services, like Outlook and Skype, and can freely communicate and share data with other users of all ages. [Learn more about parental consent and Microsoft child accounts.](#)

Parents or guardians can change or revoke the consent choices previously made, and review, edit, or request the deletion of the personal data of the children for whom they provided consent or authorization. As the organizer of a Microsoft family group, the parent or guardian can manage a child's information and settings on their [Family Safety](#) page and view and delete a child's data on their [privacy dashboard](#).

Below is additional information about the collection of data from children as related to Xbox.

What is Xbox? Xbox is the gaming and entertainment division of Microsoft. Xbox hosts an online network that consists of software and enables online experiences crossing multiple platforms. This

network lets your child find and play games, view content, and connect with friends on Xbox and other gaming and social networks. Children can connect to the Xbox network using Xbox consoles, Windows devices, and mobile devices (Android and iPhone).

Xbox consoles are devices your child can use to find and play games, movies, music, and other digital entertainment. When they sign in to Xbox, in apps, games or on a console, we assign a unique identifier to their device. For instance, when their Xbox console is connected to the internet and they sign in to the console, we identify which console and which version of the console's operating system they are using.

Xbox continues to provide new experiences in client apps that are connected to and backed by services such as Xbox network and cloud gaming. When signed in to an Xbox experience, we collect required data to help keep these experiences reliable, up to date, secure, and performing as expected.

Data we collect when you create an Xbox profile. You as the parent or guardian are required to consent to the collection of personal data from a child under 13 years old. With your permission, your child can have an Xbox profile and use the online Xbox network. During the child Xbox profile creation, you will sign in with your own Microsoft account to verify that you are an adult organizer in your Microsoft family group. We collect an alternate email address or phone number to boost account security. If your child needs help accessing their account, they will be able to use one of these alternates to validate they own the Microsoft account.

We collect limited information about children, including name, birthdate, email address, and region. When you sign your child up for an Xbox profile, they get a gamertag (a public nickname) and a unique identifier. When you create your child's Xbox profile you consent to Microsoft collecting, using, and sharing information based on their privacy and communication settings on the Xbox online network. Your child's privacy and communication settings are defaulted to the most restrictive.

Data we collect. We collect information about your child's use of Xbox services, games, apps, and devices including:

- When they sign in and sign out of Xbox, purchase history, and content they obtain.
- Which games they play and apps they use, their game progress, achievements, play time per game, and other play statistics.
- Performance data about Xbox consoles, Xbox Game Pass and other Xbox apps, the Xbox network, connected accessories, and network connection, including any software or hardware errors.
- Content they add, upload, or share through the Xbox network, including text, pictures, and video they capture in games and apps.
- Social activity, including chat data and interactions with other gamers, and connections they make (friends they add and people who follow them) on the Xbox network.

If your child uses an Xbox console or Xbox app on another device capable of accessing the Xbox network, and that device includes a storage device (hard drive or memory unit), usage data will be stored on the storage device and sent to Microsoft the next time they sign in to Xbox, even if they have been playing offline.

Xbox console diagnostic data. If your child uses an Xbox console, the console will send required data to Microsoft. Required data is the minimum data necessary to help keep Xbox safe, secure, up to date, and performing as expected.

Game captures. Any player in a multiplayer game session can record video (game clips) and capture screenshots of their view of the game play. Other players' game clips and screenshots can capture your child's in-game character and gamertag during that session. If a player captures game clips and screenshots on a PC, the resulting game clips might also capture audio chat if your child's privacy and communication settings on the Xbox online network allow it.

Captioning. During Xbox real-time ("party") chat, players may activate a voice-to-text feature that lets them view that chat as text. If a player activates this feature, Microsoft uses the resulting text data to provide captioning of chat for players who need it. This data may also be used to provide a safe gaming environment and enforce the [Community Standards for Xbox](#).

Data use. Microsoft uses the data we collect to improve gaming products and experiences— making it safer and more fun over time. Data we collect also enables us to provide your child with personalized, curated experiences. This includes connecting them to games, content, services, and recommendations.

Xbox data viewable by others. When your child is using the Xbox network, their online presence (which can be set to "appear offline" or "blocked"), gamertag, game play statistics, and achievements are visible to other players on the network. Depending on how you set your child's Xbox safety settings, they might share information when playing or communicating with others on the Xbox network.

In order to help make the Xbox network a safe gaming environment and enforce the Community Standards for Xbox, we may collect and review voice, text, images, videos and in-game content (such as game clips your child uploads, conversations they have, and things they post in clubs and games).

Xbox data shared with game and apps publishers. When your child uses an Xbox online game or any network-connected app on their Xbox console, PC, or mobile device, the publisher of that game or app has access to data about their usage to help the publisher deliver, support, and improve its product. This data may include: your child's Xbox user identifier, gamertag, limited account info such as country and age range, data about your child's in-game communications, any Xbox enforcement activity, game-play sessions (for example, moves made in-game or types of vehicles used in-game), your child's presence on the Xbox network, the time they spend playing the game or app, rankings, statistics, gamer profiles, avatars, or gamerpics, friends lists, activity feeds for official clubs they belong to, official club memberships, and any content they create or submit in the game or app.

Third-party publishers and developers of games and apps have their own distinct and independent relationship with users and their collection and usage of personal data is subject to their specific privacy policies. You should carefully review their policies to determine how they use your child's data. For example, publishers may choose to disclose or display game data (such as on leaderboards) through their own services. You may find their policies linked from the game or app detail pages in our stores.

Learn more at [Data Sharing with Games and Apps](#).

To stop sharing game or app data with a publisher, remove its games or app from all devices where they have been installed. Some publisher access to your child's data may be revoked at microsoft.com/consent.

Managing child settings. As the organizer of a Microsoft family group, you can manage a child's information and settings on their [Family Safety](#) page, as well as their Xbox profile privacy settings from their [Xbox Privacy & online safety page](#).

You can also use the [Xbox Family Settings](#) app to manage your child's experience on the Xbox Network including: spending for Microsoft and Xbox stores, viewing your child's Xbox activity, and setting age ratings and the amount of screen time.

Learn more about managing Xbox profiles at [Xbox online safety and privacy settings](#).

Learn more about Microsoft family groups at [Simplify your family's life](#).

Accessing child data. As the organizer of a Microsoft family group, a parent can view and delete a child's data on their [privacy dashboard](#). The dashboard allows you to review your child's personal information, have it deleted, and refuse to permit further collection or use of your child's information.

To close your child's account, sign in with their account info at account.microsoft.com/profile and select "How to close your account."

Legacy.

- ♦ **Xbox 360.** This Xbox console collects limited required diagnostic data. This data helps keep your child's console functioning as expected.
- ♦ **Kinect.** The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control game play. For example:
 - If you choose, the camera can be used to sign in to the Xbox network automatically using facial recognition. This data stays on the console, is not shared with anyone, and can be deleted at any time.
 - For game play, Kinect will map distances between the joints on your child's body to create a stick figure representation to enable play.
 - The Kinect microphone can enable voice chat between players during play. The microphone also enables voice commands for control of the console, game, or app, or to enter search terms.
 - The Kinect sensor can also be used for audio and video communications through services such as Skype.

Learn more about Kinect at [Xbox Kinect and Privacy](#).

Other important privacy information

Below you will find additional privacy information, such as how we secure your data, where we process your data, and how long we retain your data. You can find more information on Microsoft and our commitment to protecting your privacy at [Microsoft Privacy](#).

Security of personal data

Microsoft is committed to protecting the security of your personal data. We use a variety of security technologies and procedures to help protect your personal data from unauthorized access, use, or disclosure. For example, we store the personal data you provide on computer systems that have limited access and are in controlled facilities. When we transmit highly confidential data (such as a credit card number or password) over the internet, we protect it through the use of encryption. Microsoft complies with applicable data protection laws, including applicable security breach notification laws.

Where we store and process personal data

Personal data collected by Microsoft may be stored and processed in your region, in the United States, and in any other country where Microsoft or its affiliates, subsidiaries, or service providers operate facilities. Microsoft maintains major data centers in Australia, Austria, Brazil, Canada, Finland, France, Germany, Hong Kong, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom, and the United States. Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a data center in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to process the data that we collect under this privacy statement according to this statement's provisions and the requirements of applicable law.

We transfer personal data from the European Economic Area, the United Kingdom, and Switzerland to other countries, some of which have not yet been determined by the European Commission to have an adequate level of data protection. For example, their laws may not guarantee you the same rights, or there may not be a privacy supervisory authority there that is capable of addressing your complaints. When we engage in such transfers, we use a variety of legal mechanisms, including contracts such as the standard contractual clauses published by the European Commission under Commission Implementing Decision 2021/914, to help protect your rights and enable these protections to travel with your data. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Microsoft processes personal data, see this article on [the European Commission website](#).

Microsoft Corporation complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom, and Switzerland to the United States, although Microsoft does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of personal data in light of the judgment of the Court of Justice of the EU in Case C-311/18. Microsoft Corporation has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If third-party agents process personal data on our behalf in a manner inconsistent with the

principles of either Privacy Shield framework, we remain liable unless we prove we are not responsible for the event giving rise to the damage. The controlled U.S. subsidiaries of Microsoft Corporation, as identified in our self-certification submission, also adhere to the Privacy Shield Principles—for more info, see the list of [Microsoft U.S. entities or subsidiaries adhering to the Privacy Shield Principles](#).

If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, visit the [Privacy Shield website](#).

If you have a question or complaint related to participation by Microsoft in the EU-U.S. or Swiss-U.S. Privacy Shield, we encourage you to contact us via our [web form](#). For any complaints related to the Privacy Shield frameworks that Microsoft cannot resolve directly, we have chosen to cooperate with the relevant EU Data Protection Authority, or a panel established by the European data protection authorities, for resolving disputes with EU individuals, and with the Swiss Federal Data Protection and Information Commissioner (FDPIC) for resolving disputes with Swiss individuals. Please contact us if you'd like us to direct you to your data protection authority contacts. As further explained in the Privacy Shield Principles, binding arbitration is available to address residual complaints not resolved by other means. Microsoft is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Individuals whose personal data is protected by Japan's Act on the Protection of Personal Information should refer to the article on the [Japanese Personal Information Protection Commission's website](#) (only published in Japanese) for more information on the Commission's review of certain countries' personal data protection systems.

Our retention of personal data

Microsoft retains personal data for as long as necessary to provide the products and fulfill the transactions you have requested, or for other legitimate purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements. Because these needs can vary for different data types, the context of our interactions with you or your use of products, actual retention periods can vary significantly.

Other criteria used to determine the retention periods include:

- ♦ **Do customers provide, create, or maintain the data with the expectation we will retain it until they affirmatively remove it?** Examples include a document you store in OneDrive, or an email message you keep in your Outlook.com inbox. In such cases, we would aim to maintain the data until you actively delete it, such as by moving an email from your Outlook.com inbox to the Deleted Items folder, and then emptying that folder (when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion). (Note that there may be other reasons why the data has to be deleted sooner, for example if you exceed limits on how much data can be stored in your account.)

- ♦ **Is there an automated control, such as in the Microsoft privacy dashboard, that enables the customer to access and delete the personal data at any time?** If there is not, a shortened data retention time will generally be adopted.
- ♦ **Is the personal data of a sensitive type?** If so, a shortened retention time would generally be adopted.
- ♦ **Has Microsoft adopted and announced a specific retention period for a certain data type?** For example, for Bing search queries, we de-identify stored queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers that are used to identify a particular account or device after 18 months.
- ♦ **Has the user provided consent for a longer retention period?** If so, we will retain data in accordance with your consent.
- ♦ **Is Microsoft subject to a legal, contractual, or similar obligation to retain or delete the data?** Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve data relevant to an investigation, or data retained for the purposes of litigation. Conversely, if we are required by law to remove unlawful content, we will do so.

California Consumer Privacy Act

If you are a California resident, we process your personal data in accordance with the California Consumer Privacy Act (CCPA). This CCPA section of our Privacy Statement contains information required by the CCPA and supplements our Privacy Statement.

Sale. We do not sell your personal data. So, we do not offer an opt-out to the sale of personal data.

Rights. You have the right to request that we (i) disclose what personal data we collect, use, disclose, and sell and (ii) delete your personal data. You may make these requests yourself or through an authorized agent. If you use an authorized agent, we provide your agent with [detailed guidance](#) on how to exercise your CCPA rights.

If you have a Microsoft account, you must exercise your rights through the [Microsoft privacy dashboard](#), which requires you to log in to your Microsoft account. If you have an additional request or questions after using the dashboard, you may contact Microsoft at the address in the [How to contact us](#) section, use our [web form](#), or call our US toll free number 1.844.931.2038. If you do not have an account, you may exercise your rights by contacting us as described above. We may ask for additional information, such as your country of residence, email address, and phone number, to validate your request before honoring the request.

You have a right not to receive discriminatory treatment if you exercise your CCPA rights. We will not discriminate against you if you exercise your CCPA rights.

Personal Information Processing. In the bulleted list below, we outline the categories of personal data we collect, the sources of the personal data, our purposes of processing, and the categories of third-party recipients with whom we share the personal data. For a

description of the data included in each category, please see the [Personal data we collect](#) section.

Categories of Personal Data

- ◆ Name and contact data
 - Sources of personal data: Interactions with users and partners with whom we offer co-branded services
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; respond to customer questions; help, secure, and troubleshoot; and marketing
 - Recipients: Service providers and user-directed entities
- ◆ Credentials
 - Sources of personal data: Interactions with users and organizations that represent users
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; authentication and account access; and help, secure and troubleshoot
 - Recipients: Service providers and user-directed entities
- ◆ Demographic data
 - Sources of personal data: Interactions with users and purchases from data brokers
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide and personalize our products; product development; help, secure, and troubleshoot; and marketing
 - Recipients: Service providers and user-directed entities
- ◆ Payment data
 - Sources of personal data: Interactions with users and financial institutions
 - Purposes of Processing (Collection and Sharing with Third Parties): Transact commerce; process transactions; fulfill orders; help, secure, and troubleshoot; and detect and prevent fraud
 - Recipients: Service providers and user-directed entities
- ◆ Subscription and licensing data
 - Sources of personal data: Interactions with users and organizations that represent users
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide, personalize, and activate our products; customer support; help, secure, and troubleshoot; and marketing
 - Recipients: Service providers and user-directed entities
- ◆ Interactions
 - Sources of personal data: Interactions with users including data Microsoft generates through those interactions
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide and personalize our products; product improvement; product development; marketing; and help, secure and troubleshoot
 - Recipients: Service providers and user-directed entities
- ◆ Content
 - Sources of personal data: Interactions with users and organizations that represent users

- Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; safety; and help, secure, and troubleshoot
 - Recipients: Service providers and user-directed entities
- ◆ Video or recordings
 - Sources of personal data: Interactions with users and publicly available sources
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; product improvement; product development; marketing; help, secure, and troubleshoot; and safety
 - Recipients: Service providers and user-directed entities
- ◆ Feedback and ratings
 - Sources of personal data: Interactions with users
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; product improvement; product development; customer support; and help, secure, and troubleshoot
 - Recipients: Service providers and user-directed entities

While the bulleted list above contains the primary sources and purposes of processing for each category of personal data, we also collect personal data from the sources listed in the [Personal data we collect](#) section, such as developers who create experiences through or for Microsoft products. Similarly, we process all categories of personal data for the purposes described in the [How we use personal data](#) section, such as meeting our legal obligations, developing our workforce, and doing research.

Disclosures of personal data for business or commercial purposes. As indicated in the [Reasons we share personal data](#) section, we share personal data with third parties for various business and commercial purposes. The primary business and commercial purposes for which we share personal data are the purposes of processing listed in the table above. However, we share all categories of personal data for the business and commercial purposes in the [Reasons we share personal data](#) section.

See our [CCPA Notice](#) for additional information.

Advertising

Advertising allows us to provide, support, and improve some of our products. Microsoft does not use what you say in email, chat, video calls or voice mail, or your documents, photos, or other personal files to target ads to you. We use other data, detailed below, for advertising in our products and on third-party properties. For example:

- ◆ Microsoft may use data we collect to select and deliver some of the ads you see on Microsoft web properties, such as [Microsoft.com](#), MSN, and Bing.
- ◆ When the advertising ID is enabled in Windows as part of your privacy settings, third parties can access and use the advertising ID (much the same way that websites can access and use a unique identifier stored in a cookie) to select and deliver ads in such apps.

- ♦ We may share data we collect with partners, such as Verizon Media, AppNexus, or Facebook (see below), so that the ads you see in our products and their products are more relevant and valuable to you.
- ♦ Advertisers may choose to place our web beacons on their sites, or use similar technologies, in order to allow Microsoft to collect information on their sites such as activities, purchases, and visits; we use this data on behalf of our advertising customers to provide ads.

The ads that you see may be selected based on data we process about you, such as your interests and favorites, your location, your transactions, how you use our products, your search queries, or the content you view. For example, if you view content on MSN about automobiles, we may show advertisements about cars; if you search “pizza places in Seattle” on Bing, you may see advertisements in your search results for restaurants in Seattle.

The ads that you see may also be selected based on other information learned about you over time using demographic data, location data, search queries, interests and favorites, usage data from our products and sites, and the information we collect about you from the sites and apps of our advertisers and partners. We refer to these ads as “personalized advertising” in this statement. For example, if you view gaming content on [xbox.com](https://www.xbox.com), you may see offers for games on MSN. To provide personalized advertising, we combine cookies placed on your device using information that we collect (such as IP address) when your browser interacts with our websites. If you opt out of receiving personalized advertising, data associated with these cookies will not be used.

We may use information about you to serve you with personalized advertising when you use Microsoft services. If you are logged in with your Microsoft account and have consented to allow Microsoft Edge to use your online activity for personalized advertising, you will see offers for products and services based on your online activity while using Microsoft Edge. To configure your privacy settings for Edge, go to Microsoft Edge > Settings > Privacy and Services. To configure your privacy and ad settings for your Microsoft account with respect to your online activity across browsers, including Microsoft Edge, or when visiting third-party websites or apps, go to your dashboard at privacy.microsoft.com.

Further details regarding our advertising-related uses of data include:

- ♦ **Advertising industry best practices and commitments.** Microsoft is a member of the [Network Advertising Initiative](#) (NAI) and adheres to the NAI Code of Conduct. We also adhere to the following self-regulatory programs:
 - In the US: [Digital Advertising Alliance \(DAA\)](#)
 - In Europe: [European Interactive Digital Advertising Alliance \(EDAA\)](#)
 - In Canada: [Ad Choices: Digital Advertising Alliance of Canada \(DAAC\)](#) / [Choix de Pub: l'Alliance de la publicité numérique du Canada \(DAAC\)](#)
- ♦ **Health-related ad targeting.** In the United States, we provide personalized advertising based on a limited number of standard, non-sensitive health-related interest categories, including allergies, arthritis, cholesterol, cold and flu, diabetes, gastrointestinal health, headache / migraine, healthy eating, healthy heart, men’s health, oral health,

osteoporosis, skin health, sleep, and vision / eye care. We will also personalize ads based on custom, non-sensitive health-related interest categories as requested by advertisers.

- ♦ **Children and advertising.** We do not deliver personalized advertising to children whose birthdate in their Microsoft account identifies them as under 18 years of age.
- ♦ **Data retention.** For personalized advertising, we retain data for no more than 13 months, unless we obtain your consent to retain the data longer.
- ♦ **Data sharing.** In some cases, we share with advertisers reports about the data we have collected on their sites or ads.

Data collected by other advertising companies. Advertisers sometimes include their own web beacons (or those of their other advertising partners) within their advertisements that we display, enabling them to set and read their own cookie. Additionally, Microsoft partners with third-party ad companies to help provide some of our advertising services, and we also allow other third-party ad companies to display advertisements on our sites. These third parties may place cookies on your computer and collect data about your online activities across websites or online services. These companies currently include, but are not limited to: [AppNexus](#), [Facebook](#), [Media.net](#), [Outbrain](#), [Taboola](#) and [Verizon Media](#). Select any of the preceding links to find more information on each company's practices, including the choices it offers. Many of these companies are also members of the [NAI](#) or [DAA](#), which each provide a simple way to opt out of ad targeting from participating companies.

Speech recognition technologies

Speech recognition technologies are integrated into many Microsoft products and services. Microsoft provides both device-based speech recognition features and cloud-based (online) speech recognition features. Microsoft's speech recognition technology transcribes voice data into text. With your permission, Microsoft employees and vendors working on behalf of Microsoft, will be able to review snippets of your voice data or voice clips in order to build and improve our speech recognition technologies. These improvements allow us to build better voice-enabled capabilities that benefit users across all our consumer and enterprise products and services. Prior to employee or vendor review of voice data, we protect users' privacy by taking steps to de-identify the data, requiring non-disclosure agreements with relevant vendors and their employees, and requiring that employees and vendors meet high privacy standards. [Learn more about Microsoft and your voice data.](#)

Preview or free-of-charge releases

Microsoft offers preview, insider, beta or other free-of-charge products and features ("previews") to enable you to evaluate them while providing Microsoft with data about your use of the product, including feedback and device and usage data. As a result, previews can automatically collect additional data, provide fewer controls, and otherwise employ different privacy and security measures than those typically present in our products. If you participate in previews, we may contact you about your feedback or your interest in continuing to use the product after general release.

Changes to this privacy statement

We update this privacy statement when necessary to provide greater transparency or in response to:

- ♦ Feedback from customer, regulators, industry, or other stakeholders.
- ♦ Changes in our products.
- ♦ Changes in our data processing activities or policies.

When we post changes to this statement, we will revise the "last updated" date at the top of the statement and describe the changes on the [Change history](#) page. If there are material changes to the statement, such as a change to the purposes of processing of personal data that is not consistent with the purpose for which it was originally collected, we will notify you either by prominently posting a notice of such changes before they take effect or by directly sending you a notification. We encourage you to periodically review this privacy statement to learn how Microsoft is protecting your information.

How to contact us

If you have a privacy concern, complaint, or question for the Microsoft Chief Privacy Officer or the Data Protection Officer for your region, please contact us by using our [web form](#). We will respond to questions or concerns as required by law and within a period no longer than 30 days. You can also raise a concern or lodge a complaint with a data protection authority or other official with jurisdiction.

When Microsoft is a controller, unless otherwise stated, Microsoft Corporation and, for those in the European Economic Area, the United Kingdom, and Switzerland, Microsoft Ireland Operations Limited are the data controllers for personal data we collect through the products subject to this statement. Our addresses are:

- ♦ Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA. Telephone: +1 (425) 882 8080.
- ♦ Microsoft Ireland Operations Limited, Attn: Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117.

To find the Microsoft subsidiary in your country or region, see the list of [Microsoft office locations around the world](#).

If you would like to exercise your rights under the California Consumer Privacy Act, you may contact Microsoft at the address above, use our [web form](#), or call our US toll free number 1.844.931.2038.

Where French law applies, you can also send us specific instructions regarding the use of your personal data after your death, by using our [web form](#).

If you have a technical or support question, please visit [Microsoft Support](#) to learn more about Microsoft Support offerings. If you have a personal Microsoft account password question, please visit [Microsoft account support](#).

Product-specific details:

Enterprise and developer products

Enterprise and Developer Products are Microsoft products and related software offered to and designed primarily for use by organizations and developers. They include:

- Cloud services, referred to as Online Services in the Product Terms, such as Microsoft 365 and Office 365, Microsoft Azure, Microsoft Dynamics365, and Microsoft Intune for which an organization (our customer) contracts with Microsoft for the services ("Enterprise Online Services").
- Other enterprise and developer tools and cloud-based services, such as Azure PlayFab Services (to learn more see [Azure PlayFab Terms of Service](#)).
- Server, developer, and hybrid cloud platform products, such as Windows Server, SQL Server, Visual Studio, System Center, Azure Stack and open source software like Bot Framework solutions ("Enterprise and Developer Software").
- Appliances and hardware used for storage infrastructure, such as StorSimple ("Enterprise Appliances").
- Professional services referred to in the Product Terms that are available with Enterprise Online Services, such as onboarding services, data migration services, data science services, or services to supplement existing features in the Enterprise Online Services.

In the event of a conflict between this Microsoft privacy statement and the terms of any agreement(s) between a customer and Microsoft for Enterprise and Developer Products, the terms of those agreement(s) will control.

You can also learn more about our Enterprise and Developer Products' features and settings, including choices that impact your privacy or your end users' privacy, in product documentation.

If any of the terms below are not defined in this Privacy Statement or the Product Terms, they have the definitions below.

General. When a customer tries, purchases, uses, or subscribes to Enterprise and Developer Products, or obtains support for or professional services with such products, Microsoft receives data from you and collects and generates data to provide the service (including improving, securing, and updating the service), conduct our business operations, and communicate with the customer. For example:

- When a customer engages with a Microsoft sales representative, we collect the customer's name and contact data, along with information about the customer's organization, to support that engagement.
- When a customer interacts with a Microsoft support professional, we collect device and usage data or error reports to diagnose and resolve problems.

- When a customer pays for products, we collect contact and payment data to process the payment.
- When Microsoft sends communications to a customer, we use data to personalize the content of the communication.
- When a customer engages with Microsoft for professional services, we collect the name and contact data of the customer's designated point of contact and use information provided by the customer to perform the services that the customer has requested.

The Enterprise and Developer Products enable you to purchase, subscribe to, or use other products and online services from Microsoft or third parties with different privacy practices, and those other products and online services are governed by their respective privacy statements and policies.

Enterprise online services

To provide the Enterprise Online Services, Microsoft uses data you provide (including Customer Data, Personal Data, Administrator Data, Payment Data, and Support Data) and data Microsoft collects or generates associated with your use of the Enterprise Online Services. We process data as described in the [Product Terms](#), [Microsoft Products and Services Data Protection Addendum](#) and the [Microsoft Trust Center](#).

Personal Data. Customer is the controller of Personal Data and Microsoft is the processor of such data, except when (a) Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor or (b) as stated otherwise in the standard [Products and Services DPA](#). In addition, as provided in the standard [Products and Services DPA](#), Microsoft has taken on the added responsibilities of a data controller under GDPR when processing Personal Data in connection with its business operations incident to providing its services to Microsoft's commercial customers, such as billing and preparing invoices; account management; compensation; financial reporting; business planning and product strategy; improving core functionality for accessibility, privacy, and energy efficiency; and combatting fraud, cybercrime, and cyberattacks that may affect Microsoft or Microsoft products. We use Personal Data in the least identifiable form that will support processing necessary for these business operations. We generally aggregate Personal Data before using it for our business operations, removing the ability to identify specific individuals.

Administrator Data. Administrator Data is the information provided to Microsoft during sign-up, purchase, or administration of Enterprise Online Services. We use Administrator Data to provide the Enterprise Online Services, complete transactions, service the account, detect and prevent fraud, and comply with our legal obligations. Administrator Data includes the name, address, phone number, and email address you provide, as well as aggregated usage data related to your account, such as the controls you select. Administrator Data also includes contact information of your colleagues and friends if you agree to provide it to Microsoft for the limited purpose of sending them an invitation to use the Enterprise Online Services; we contact those individuals with communications that include information about you, such as your name and profile photo.

As needed, we use Administrator Data to contact you to provide information about your account, subscriptions, billing, and updates to the Enterprise Online Services, including information about new features, security, or other technical issues. We also contact you regarding third-party inquiries we receive regarding use of the Enterprise Online Services, as described in your agreement. You cannot unsubscribe from these non-promotional communications. We may also contact you regarding information and offers about other products and services, or share your contact information with Microsoft's partners. When such a partner has specific services or solutions to meet your needs, or to optimize your use of the Enterprise Online Services, we may share limited, aggregated information about your organization's account with the partner. Microsoft will not share your confidential information or contact information with the authorized partner unless we have sufficient rights to do so. You can manage your contact preferences or update your information in your account profile.

Payment Data. We use payment data to complete transactions, as well as to detect and prevent fraud.

Support Data. Customers provide or authorize Microsoft to collect data in connection with obtaining technical support for the Enterprise Online Services. We process Support Data to provide technical support and as described in the [Products and Services DPA](#).

Local Software and Diagnostic Data. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications). The local software may collect Diagnostic Data (as defined in the [Products and Services DPA](#)) about the use and performance of that software. That data may be transmitted to Microsoft and used for the purposes described in the [Products and Services DPA](#).

Bing Search Services Data. Bing Search Services, as defined in the Product Terms, use data such as search queries as described in the [Bing](#) section of this privacy statement.

Enterprise and developer software and enterprise appliances

Enterprise and developer software and enterprise appliances collect data to operate effectively and provide you the best experiences. The data we collect depends on the features you use, as well as your configuration and settings, but it is generally limited to device and usage data. Customers have choices about the data they provide. Here are examples of the data we collect:

- ♦ During installation or when you upgrade an enterprise and developer software, we may collect device and usage data to learn whether you experience any difficulties.
- ♦ When you use enterprise software or enterprise appliances, we may collect device and usage data to learn about your operating environment to improve security features.
- ♦ When you experience a crash using enterprise software or enterprise appliances, you may choose to send Microsoft an error report to help us diagnose the problem and deliver customer support.

Microsoft uses the data we collect from enterprise and developer software and enterprise appliances to provide and improve our products, to deliver customer support, to activate the product, to communicate with you, and to operate our business.

Microsoft SQL Server is a relational database management platform and includes products that can be installed separately (such as SQL Server Management Studio). For detailed information about what data we collect, how we use it, and how to manage your privacy options, visit the [SQL Server privacy page](#). If you work in an organization, your administrator can set certain telemetry settings in SQL Server via Group Policy.

HoloLens. HoloLens headsets are self-contained Windows computers with Wi-Fi connectivity that enable a mixed reality experience for apps and solutions. Microsoft collects diagnostic data to solve problems and to keep Windows running on HoloLens up to date, secure, and operating properly. Diagnostic data also helps us improve HoloLens and related Microsoft products and services depending on the diagnostic data settings you've chosen for your device. [Learn more about Windows diagnostic data](#).

HoloLens also processes and collects data related to the HoloLens experience and device, which include cameras, microphones, and infrared sensors that enable motions and voice to navigate.

- ♦ If you choose, cameras can be used to sign you in automatically using your iris. To do this, HoloLens takes an image of your iris and measures distances between key points to create and store a numeric value that represents only you. This data stays on the HoloLens and is not shared with anyone, and you can choose to delete this data from your HoloLens at any time.
- ♦ HoloLens also detects hand gestures intended for system interactions (such as menu navigation, pan/zoom, and scroll). This data is processed on your HoloLens device and is not stored.
- ♦ HoloLens derives tracking points based on your environment which allows it to understand surfaces in space and allows you to place digital assets on them. There are no images associated with this environmental data and it is stored locally on the HoloLens device. You can choose to delete this data from your HoloLens at any time.

The headset's microphones enable voice commands for navigation, controlling apps, or to enter search terms. [Learn more about voice data collection](#).

Productivity and communications products

Productivity and communications products are applications, software, and services you can use to create, store, and share documents, as well as communicate with others.

Microsoft 365

Microsoft 365, previous versions called Office 365, is a collection of productivity services and Office applications including Word, Excel, PowerPoint, and Outlook, among others. For more details about Outlook, see the [Outlook](#) section of this privacy statement. Microsoft 365 is a service that is comprised of client software applications and connected online services that span many platforms and have numerous interdependent experiences. Various Microsoft 365 services enable you to use your file content for designs and recommendations, collaborate with others within your documents, and provide you functionality from other Microsoft products, such as Bing and Cortana, and third-party connected products. If you work in an organization, your administrator may turn off or disable these connected services. You can access the privacy controls within your Office apps by selecting **File > Account > Account Privacy**. See [Account Privacy Settings](#) for more information.

Office Roaming Service. The Office Roaming Service helps keep your Microsoft 365 settings up to date across your devices running Microsoft 365. When you sign in to Microsoft 365 with your Microsoft account or an account issued by your organization, the Office Client Policy Service is turned on and syncs some of your customized Microsoft 365 settings to Microsoft servers (such as a list of most recently used documents and the last location viewed within a document). When you sign in to Microsoft 365 on another device with the same account, the Office Roaming Service downloads your settings from Microsoft servers and applies them to the additional device. The Office Roaming Service also applies some of your customized Microsoft 365 settings when you sign in to Office.com. When you sign out of Microsoft 365, the Office Roaming Service removes your Microsoft 365 settings from your device. Any changes you make to your customized Microsoft 365 settings are sent to Microsoft servers.

Microsoft Updates. Microsoft uses services such as Click-to-Run or Microsoft AutoUpdate to provide you with security and other important updates.

Click-to-Run Update Service. The Click-to-Run Update Service allows you to install certain Microsoft 365 products over the internet. The Click-to-Run Update Service also automatically detects online updates to Click-to-Run-enabled products on your device and downloads and installs them automatically.

Translator. Translator used in Office apps is designed as a no-trace connected experience. With [no trace](#) connected experience, no portion of your translation request that gets sent to Microsoft Translator API service will be logged, your submitted text will not be used to improve the quality of the Microsoft Translator service, and there will not be any record of any portion of your data retained by Microsoft.

Diagnostic Data. Diagnostic data is used to (i) keep your Office apps secure and up to date; (ii) detect, diagnose, and remediate problems; and (iii) make product improvements. This data does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Office. Users have a choice between two different levels of diagnostic data collection, Required and Optional.

- ♦ **Required.** The minimum data necessary to help keep Office apps secure, up to date, and performing as expected on the device it's installed on.
- ♦ **Optional.** Additional data that helps us make product improvements and provides enhanced information to help us detect, diagnose, and remediate issues.

See [Diagnostic Data in Office](#) for more information.

Connected Experiences. Microsoft 365 continues to provide more experiences in client applications that are connected to and backed by cloud-based services. If you choose to use connected experiences, required service data will be collected to help keep these connected experiences reliable, up to date, secure, and performing as expected.

Microsoft 365 consists of client software applications and connected experiences designed to enable you to create, communicate, and collaborate more effectively. Working with others on a document stored on OneDrive for Business or translating the contents of a Word document into a different language are examples of connected experiences. There are two types of connected experiences.

- ♦ **Experiences that analyze your content.** Experiences that use your Office content to provide you with design recommendations, editing suggestions, data insights, and similar features. For example, PowerPoint Designer or Editor in Word.
- ♦ **Experiences that download online content.** Experiences that allow you to search and download online content including templates, images, 3D models, videos, and reference materials to enhance your documents. For example, templates or PowerPoint QuickStarter.

You can access the privacy controls within your Office apps by selecting **File > Account > Account Privacy**. These privacy settings allow you to configure your connected experiences. For example, you can choose to enable connected experiences that download online content, but not connected experiences that analyze content. Turning off connected experiences will also turn off additional experiences, such as document co-authoring and online file storage. But even if you use this privacy setting to turn off connected experiences, certain functionality will remain available, such as syncing your mailbox in Outlook, as well as essential services described below.

If you choose to disable certain types of connected experiences, either the ribbon or menu command for those connected experiences will be grayed out or you will get an error message when you try to use those connected experiences.

There are a set of services that are essential to how Microsoft 365 functions and cannot be disabled. For example, the licensing service that confirms that you are properly licensed to use Microsoft 365 is essential. Required service data about these services is collected and sent to Microsoft, regardless of any other settings that you have configured. See [Essential Services](#) for more information.

Required service data for connected experiences. As you use a connected experience, data is sent to and processed by Microsoft to provide you that connected experience. This data is necessary because this information enables us to deliver these cloud-based connected experiences. We refer to this data as required service data.

Required service data can include information related to the operation of the connected experience that is needed to keep the underlying service secure, up to date, and performing as expected. If you choose to use a connected experience that analyzes your content, for

example Translate in Word, the text you typed and selected to translate is also sent and processed to provide you the connected experience. Your text and the translation are not stored by our service. Required service data can also include information needed by a connected experience to perform its task, such as configuration information about the Office app.

See [Required service data for Office](#) for more information.

Microsoft Teams

This section applies to the consumer offering of Teams; if you are using Teams with a school or work account, see the [Enterprise and developer products](#) of this privacy statement.

Teams is an all-in-one collaboration and communication hub. Teams lets you stay organised and connected across your entire life. Teams allows you to call people with voice or video calling. Teams allows you to easily find people, files, photos, conversations, tasks, and calendars in one convenient and secure place. Teams allows you to store confidential information like passwords, rewards numbers, or login information and share it with others within Teams. With your consent, you can share your location with friends and family.

As part of providing these features, Microsoft collects data about the usage of the features as well as information about your communications, including the time and date of the communication and users that are part of the communication.

Teams profile. Your Teams profile includes information you provided when you set up a Microsoft account. To enable other people to find you on Teams (or products that interact with Teams for personal use, including Teams for enterprise) your display name and picture are visible to other users on Teams that have your contact information.

Teams contacts. With your permission, Teams will sync your device, Outlook, and Skype contacts periodically and check for other Teams users that match contacts in your device, Outlook, or Skype address books. You are always in control of your contacts and can stop syncing at any time. If you choose to stop syncing your device, Outlook, or Skype contacts, or you are inactive on your device, any contacts that have not been matched during the synchronization process will be deleted from Teams. If you wish to invite any of your device, Outlook, or Skype contacts to join a conversation, you can invite users to a 1:1 directly, or Microsoft can send an invitation on your behalf via SMS or email for invitations to group conversations. You can block users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Notice to non-user contacts. If your information appears in the device, Outlook, or Skype address books of a Teams user who chooses to sync their device, Outlook, or Skype contacts with their Teams contacts, Microsoft may process your data in order to determine whether you are a current Teams user and to allow Teams users to invite you to the service, including via SMS and email. As long as the Teams user continues to be active on Teams on their device and continues to enable contact syncing with the applicable device or service, your information

will be stored on our servers and we will periodically process your information as a part of the Teams user's contact syncing experience to check whether you have subsequently joined Teams.

[Learn more about how we process your information in connection with the contact syncing feature offered to Teams users.](#)

If you do choose to join Teams, you will appear as a suggested new Teams contact for any Teams users with your information in their device, Outlook, or Skype address books. As a Teams user, you will be able to block other Teams users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Third-party contacts. You can also choose to sync contacts from third-party providers. If you choose to unsync your third-party contacts on Teams, all third-party contacts are deleted from Teams. If you gave your consent to use those third-party contacts on other Microsoft apps and services, these contacts will still be available to those other Microsoft apps and services.

You can remove third-party contacts from all Microsoft apps and services by removing third-party accounts from Teams. Please note that removing a third-party account from Teams may impact your experiences on other Microsoft apps and services that also use that third-party account.

Teams calendar. You can also choose to sync your Teams calendar with calendars from third-party providers. You can stop syncing your Teams calendar anytime by removing a third-party account from Teams. If you have consented to use third-party data on other Microsoft apps and services, please note that removing this third-party account data in Teams may impact your experiences on other Microsoft apps and services.

Location sharing. You can share your static or live location with individuals or groups within Teams. You are in control and can stop sharing at any time. Sharing location for children is permitted with parental consent and in groups where an adult from the Microsoft family group is present.

Push notifications. To let you know of incoming calls, chats, and other messages, Teams uses the notification service on your device. For many devices, these services are provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Teams has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by the company providing the notification service.

If you do not want to use the notification services for incoming Teams calls and messages, turn it off in the settings found on your device.

OneDrive

OneDrive lets you store and access your files on virtually any device. You can also share and collaborate on your files with others. Some versions of the OneDrive application enable you to access both your personal OneDrive by signing in with your personal Microsoft account and your OneDrive for Business by signing in with your work or school Microsoft account as part of your organization's use of Microsoft 365 or Office 365.

When you use OneDrive, we collect data about your usage of the service, as well as the content you store, to provide, improve, and protect the services. Examples include indexing the contents of your OneDrive documents so that you can search for them later and using location information to enable you to search for photos based on where the photo was taken. We also collect device information so we can deliver personalized experiences, such as enabling you to sync content across devices and roam customized settings.

When you store content in OneDrive, that content will inherit the sharing permissions of the folder in which you store it. For example, if you decide to store content in the public folder, the content will be public and available to anyone on the internet who can find the folder. If you store content in a private folder, the content will be private.

When you share content to a social network like Facebook from a device that you have synced with your OneDrive account, your content is either uploaded to that social network, or a link to that content is posted to that social network. Doing this makes the content accessible to anyone on that social network. To delete the content, you need to delete it from the social network (if it was uploaded there, rather than a link to it) and from OneDrive.

When you share your OneDrive content with your friends via a link, an email with the link is sent to those friends. The link contains an authorization code that allows anyone with the link to access your content. If one of your friends sends the link to other people, they will also be able to access your content, even if you did not choose to share the content with them. To revoke permissions for your content on OneDrive, sign in to your account and then select the specific content to manage the permission levels. Revoking permissions for a link effectively deactivates the link. No one will be able to use the link to access the content unless you decide to share the link again.

Files managed with OneDrive for Business are stored separately from files stored with your personal OneDrive. OneDrive for Business collects and transmits personal data for authentication, such as your email address and password, which will be transmitted to Microsoft and/or to the provider of your Microsoft 365 or Office 365 service.

Outlook

Outlook products are designed to improve your productivity through improved communications and include Outlook.com, Outlook applications, and related services.

Outlook.com. Outlook.com is the primary consumer email service from Microsoft and includes email accounts with addresses that end in outlook.com, live.com, hotmail.com, and

msn.com. Outlook.com provides features that let you connect with your friends on social networks. You will need to create a Microsoft account to use Outlook.com.

When you delete an email or item from a mailbox in Outlook.com, the item generally goes into your Deleted Items folder where it remains for approximately 7 days unless you move it back to your inbox, you empty the folder, or the service empties the folder automatically, whichever comes first. When the Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion, unless we are legally required to retain the data for longer.

Outlook applications. Outlook client applications are software you install on your device that permits you to manage email, calendar items, files, contacts, and other data from email, file storage, and other services, like Exchange Online or Outlook.com, or servers, like Microsoft Exchange. You can use multiple accounts from different providers, including third-party providers, with Outlook applications.

To add an account, you must provide permission for Outlook to access data from the email or file storage services.

When you add an account to Outlook, your mail, calendar items, files, contacts, settings and other data from that account will automatically sync to your device. If you are using the mobile Outlook application, that data will also sync to Microsoft servers to enable additional features such as faster search, personalized filtering of less important mail, and an ability to add email attachments from linked file storage providers without leaving the Outlook application. If you are using the desktop Outlook application, you can choose whether to allow the data to sync to our servers. At any time, you can remove an account or make changes to the data that is synced from your account.

If you add an account provided by an organization (such as your employer or school), the owner of the organizational domain can implement policies and controls (for example, requiring multi-factor authentication or the ability to remotely wipe data from your device) that can affect your use of Outlook.

To learn more about the data the Outlook applications collect and process, please see the [Microsoft 365](#) section of this privacy statement.

Skype

Skype lets you send and receive voice, video, SMS, and instant message communications. This section applies to the consumer version of Skype; if you are using Skype for Business, see the [Enterprise and developer products](#) section of this privacy statement.

As part of providing these features, Microsoft collects usage data about your communications that includes the time and date of the communication and the numbers or user names that are part of the communication.

Skype profile. Your Skype profile includes information you provided when you set up a Microsoft account. To enable other people to find you on Skype (or products that interact with Skype, such as Skype for Business), depending on your profile settings, your Skype profile is included in the Skype public search. Your profile includes your user name, avatar, and any other data you choose to add to your profile or display to others.

Emergency calling in the United States. If you enable location sharing for emergency calling, your location will be periodically collected to enable Microsoft to share your location with emergency calling service providers if you dial 911. Your location information is only shared if you enable location sharing for emergency calling and you initiate a 911 call.

Skype contacts. If you use Outlook.com to manage contacts, Skype will automatically add the people you know to your Skype contact list until you tell the application to stop. With your permission, Skype will sync your device contacts periodically and check for other Skype users that match contacts in your device or Outlook address books. You are always in control of your contacts and can stop syncing at any time. You can block users if you do not want to receive their communications. If you choose to stop syncing your device contacts, or you are inactive on your device, any contacts that have not been matched during the synchronization process will be deleted from Skype. If you wish to invite any of your device or Outlook contacts to join a conversation, you can invite users to a 1:1 directly, or Microsoft can send an invitation on your behalf via SMS or email for invitations to group conversations. You can block users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Notice to non-user contacts. If your information appears in the device or Outlook address book of a Skype user who chooses to sync their device or Outlook contacts with their Skype contacts, Microsoft may process your data in order to determine whether you are a current Skype user and to allow Skype users to invite you to the service, including via SMS and email. As long as the Skype user continues to be active on Skype on their device and continues to enable contact syncing, your information will be stored on our servers and we will periodically process your information as a part of the Skype user's contact syncing experience to check whether you have subsequently joined Skype.

[Learn more about how we process your information in connection with the contact syncing feature offered to Skype users.](#)

If you do choose to join Skype, you will appear as a suggested new Skype contact for any Skype users with your information in their device or Outlook address books. As a Skype user, you will be able to block other Skype users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Partner companies. To make Skype available to more people, we partner with other companies to allow Skype to be offered via those companies' services. If you use Skype through a company other than Microsoft, that company's privacy policy governs how it handles your data. To comply with applicable law or respond to valid legal process, or to help our partner company or local operator comply or respond, we may access, transfer, disclose, and preserve your data. That data could include, for example, your private content, such as the content of your instant messages, stored video messages, voicemails, or file transfers.

Skype Manager. Skype Manager lets you manage a group's (such as your family's) Skype usage from one central place. When you set up a group, you will be the Skype Manager Administrator and can see the patterns of usage, including detailed information, like traffic data and details of purchases, of other members of the group who have consented to such access. If you add information like your name, other people in the group will be able to see it. Members of the group can withdraw consent for Skype Manager by visiting their [Skype account page](#).

Push notifications. To let you know of incoming calls, chats, and other messages, Skype apps use the notification service on your device. For many devices, these services are provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Skype has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by the company providing the notification service. If you do not want to use the notification services for incoming Skype calls and messages, turn it off in the settings found in the Skype application or your device.

Translation features. When you use Skype's translation features, Skype collects and uses your conversation to provide the translation service. With your permission, your data may be used to help improve Microsoft products and services. To help the translation and speech recognition technology learn and grow, sentences and automatic transcripts are analyzed and any corrections are entered into our system, to build better performing services. This data may include manual transcription of your voice clips. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#).

Recording features. Some versions of Skype have a recording feature that allows you to capture and share all or part of your audio / video call. The recording will be stored and shared as part of your conversation history with the person or group with whom the call occurred. **You should understand your legal responsibilities before recording any communication. This may include obtaining the prior consent of everyone participating in the conversation or any other authorizations as required.** Microsoft is not responsible for how you use your recordings or the recording features.

Skype bots. Bots are programs offered by Microsoft or third parties that can do many useful things like search for news, play games, and more. Depending on their capabilities, bots may have access to your display name, Skype ID, country, region, language, and any messages, audio, video, or content that you share with the bot. Please review the bot profile and its privacy statement before engaging in a one-to-one or group conversation with a bot. You can delete a bot that you no longer wish to engage with. Prior to adding a bot to a group, please ensure that your group participants have consented to their information being shared with the bot.

Captioning. Certain Skype features include accessibility functionality such as captioning. During Skype calls, a call participant can activate a voice-to-text feature, which allows the user to view the audio chat as text. If a user activates this feature, other call participants will not

receive a notification. Microsoft uses this voice and text data to provide captioning of audio for users.

Surface Duo

The Surface Duo is a device featuring two screens that fits in your pocket for productivity on the go. Powered by the Google Android operating system, Surface Duo supports cellular and Wi-Fi connectivity and can be used for email, internet browsing, games, and business connectivity.

Microsoft provides a core Surface Duo experience that runs on the Android operating system. The core Surface Duo experience includes apps such as the Microsoft Launcher, Setup Wizard, and Your Phone Companion. You can sign in with a Google ID and enable various Google services; you can then also sign in with your Microsoft account (MSA) and enable Microsoft's services. Microsoft apps and services may rely on information provided by Google. Some features, such as location, require that you enable this functionality for Google and separately allow Microsoft to leverage this information.

Diagnostic data. Surface Duo collects diagnostic data to solve problems and to keep the core Surface Duo experience up to date, secure, and operating properly. This data also helps us improve Surface Duo and related Microsoft products and services. The data does not include your user name, email address, or the content of your files. There are two levels of diagnostic data: Required diagnostic data and Optional diagnostic data.

- ♦ **Required.** The minimum data necessary to help keep the core Surface Duo experience secure, up to date, and performing as expected.
- ♦ **Optional.** Additional data that helps us make product improvements and provides enhanced information to help Microsoft detect, diagnose, and remediate issues.

[Learn more in Surface Duo Privacy Settings.](#)

Surface Duo location settings. Surface Duo relies on Google location services to determine the device's precise geographic location to display the local weather. The location of your Surface Duo can be determined with varying degrees of accuracy and may in some cases be determined precisely. If you want Microsoft apps to be able to reference or display weather or other location related information, you need to enable Google location services and Microsoft location access. Some apps may require these settings be enabled independently for the app and can be set or changed in the Surface Duo's Settings. The [Google Privacy Policy](#) provides details about Google's location service and related data privacy practices. See [Surface Duo Location Settings](#) for more information.

Microsoft apps included with the Surface Duo. The diagnostic data options for the core Surface Duo experience are configured when you initially set up your Surface Duo and can be changed in the Surface Duo's Settings under the Diagnostic Data section.

The other Microsoft apps on your Surface Duo may prompt you to enable functionality to enable the full experience of the app or you may be asked to allow optional diagnostic data

collection. You can change the settings for these apps in the Surface Duo Settings under the app name. More information about these apps is available in the [Productivity and communications products](#) and [Search, Microsoft Edge, and artificial intelligence](#) sections of this Privacy Statement.

LinkedIn

To learn about the data LinkedIn collects and how it is used and shared, please see LinkedIn's [Privacy Policy](#).

Search, Microsoft Edge, and artificial intelligence

Search and artificial intelligence products connect you with information and intelligently sense, process, and act on information—learning and adapting over time.

Bing

Bing services include search and mapping services, as well as the Bing Toolbar and Bing Desktop apps. Bing services collect and process data in many forms, including text that has been inked or typed, voice data, and images. Bing services are also included within other Microsoft services, such as Microsoft 365, Cortana, and certain features in Windows (which we refer to as Bing-powered experiences).

When you conduct a search, or use a feature of a Bing-powered experience that involves conducting a search or entering a command on your behalf, Microsoft will collect the searches or commands you provide (which may be in the form of text, voice data, or an image), along with your IP address, location, the unique identifiers contained in our cookies or similar technologies, the time and date of your search, and your browser configuration. For example, if you use Bing voice-enabled services, your voice input and performance data associated with the speech functionality will be sent to Microsoft. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#). And, if you use Bing image-enabled services, the image you provide will be sent to Microsoft. When you use Bing-powered experiences, such as Bing Lookup to search a particular word or phrase within a webpage or document, that word or phrase is sent to Bing along with some surrounding content in order to provide contextually relevant search results.

Search suggestions. For the search suggestions feature, the characters that you type into a Bing-powered experience (such as search and site suggestions in the Microsoft Edge browser) to conduct a search and what you click on will be sent to Microsoft. This allows us to provide you with relevant suggestions as you type your searches. To turn this feature on or off, while using Bing Search, go to [Bing Settings](#). There are other methods to control this feature in other Bing-powered experiences, such as the Microsoft Edge browser. Search Suggestions

cannot be turned off in the search box in Windows 10 and Windows 11. If you choose, you can always hide the search box or icon on the taskbar.

Bing experience improvement program for Bing Desktop and Bing Toolbar. If you are using Bing Desktop or Bing Toolbar and choose to participate in the Bing Experience Improvement Program, we also collect additional data about how you use these specific Bing apps, such as the addresses of the websites you visit, to help improve search ranking and relevance. To help protect your privacy, we do not use the data collected through the Bing Experience Improvement Program to identify or contact you or target advertising to you. You can turn off the Bing Experience Improvement Program at any time in the Bing Desktop or Bing Toolbar settings. Finally, we delete the information collected through the Bing Experience Improvement Program after 18 months.

Retention and de-identification. We de-identify stored search queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers that are used to identify a particular account or device after 18 months.

Personalization through Microsoft account. Some Bing services provide you with an enhanced experience when you sign in with your personal Microsoft account, for example, syncing your search history across devices. You can use these personalization features to customize your interests, favorites, and settings, and to connect your account with third-party services. Visit [Bing Settings](#) to manage your personalization settings, or the [Microsoft privacy dashboard](#) to manage your data.

Managing search history. When you're signed-in to a personal Microsoft account, you can erase your search history on the [Microsoft privacy dashboard](#). The Search History service from Bing, located in Bing Settings, provides another method of revisiting the search terms you've entered and results you've clicked when using Bing search through your browser. You may clear your search history on a device through this service. Clearing your history prevents that history from being displayed on the Search History site, but does not delete information from our search logs, which are retained and de-identified as described above or as you have instructed through the privacy dashboard. If you are signed-in to a work or school Microsoft account using Microsoft Search in Bing, you can export your Microsoft Search in Bing search history, but you cannot delete it. Your Microsoft Search in Bing service administrator can see aggregated search history across all enterprise users but cannot see specific searches by user.

Third-party services that use Bing. You may access Bing-powered experiences when using third-party services, such as those from Yahoo!. In order to provide these services, Bing receives data from these and other partners, including your search query and related data (such as date, time, IP address, and a unique identifier). This data will be sent to Microsoft to provide the search service. Microsoft will use this data as described in this statement or as further limited by our contractual obligations with our partners. You should refer to the privacy policies of the third-party services for any questions about how they collect and use data.

Data passed to destination website. When you select a search result or advertisement from a Bing search results page and go to the destination website, the destination website will receive the standard data your browser sends to every web site you visit—such as your IP

address, browser type and language, and the host name of the site you came from (in this case, <https://www.bing.com/>).

Sharing data from Bing and Bing-powered experiences with third parties. We share some de-identified data (data where the identity of a specific person is not known) from Bing and Bing-powered experiences with selected third parties. Before we do so, we run the data through a process designed to remove certain sensitive data that users may have included in the search terms themselves (such as social security numbers or credit card numbers). Additionally, we require these third parties to keep the data secure and to not use the data for purposes other than for which it is provided.

Cortana

Cortana is your personal productivity assistant in Microsoft 365. As a digital assistant, Cortana is designed to help you achieve more with less effort so you can focus on what matters and can answer a wide range of questions about things such as weather, sports, stocks, and general information. When you ask questions, the data Cortana collects depends on whether you are using the consumer or enterprise version.

This section applies to the consumer version of Cortana experiences in Windows 10 and Windows 11. If you are using Cortana with an account provided by an organization, such as a work or school account, see the [Notice to end users](#) section of this privacy statement. [Learn more about the enterprise version of Cortana in Microsoft 365.](#)

When you ask Cortana a question, whether you are speaking or typing, Cortana collects that question as a text string. To answer your questions Cortana uses the Bing service. For information about the data Bing collects, see the [Bing](#) section of this privacy statement.

By default, if you speak your question, Cortana also collects speech transcription data and does not collect voice clips. You have the option to provide your consent and allow Microsoft to collect voice clips. If you choose to opt in and allow Microsoft to collect voice clips, the voice clip files are stored and anonymized and will not be associated with your Microsoft account or any other Microsoft IDs. This anonymous data is used to improve the product. For more information about Microsoft and your voice data, see the [Speech Recognition Technologies](#) section of this privacy statement.

Cortana legacy. Cortana in Windows 10 version 1909 and earlier collects user query data (a text transcription of the question the user asked), which is anonymized and used for product maintenance. Cortana in Windows 10 version 1909 also uses the Bing service to answer your questions. For information about the data Bing collects, see the [Bing](#) section of the Privacy Statement.

[Learn more about Cortana and privacy.](#)

Microsoft Edge

Whenever you use a web browser to access the internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address, browser type and language, access times, and referring website addresses. This data might be logged on those websites' or online services' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use. Certain features in Microsoft Edge, such as when you open a new tab in the browser, connect you to MSN Content and your experiences with such content is covered by the MSN section of this privacy statement. Additionally, Microsoft Edge sends a unique browser ID to certain websites to enable us to develop aggregate data used to improve browser features and services.

Microsoft Edge for Windows, Linux, and macOS. Microsoft Edge is the default web browser for Windows 10 and later and is also available on other supported versions of Windows and macOS.

Data about how you use your browser, such as your browsing history, web form data, temporary internet files, and cookies, is stored on your device. You can delete this data from your device using Clear Browsing History.

Microsoft Edge allows you to capture and save content on your device, such as:

- ♦ **Settings and More.** Allows you to manage your favorites, downloads, history, extensions, and collections.
- ♦ **Collections.** Allows you to collect text, images, videos, and other content in a note page in your browser. When you drag content into your collection, it is cached on your device and can be deleted through your collection.
- ♦ **Website Pin to Taskbar.** Allows you to pin your favorite websites to the Windows taskbar. Websites will be able to see which of their webpages you have pinned, so they can provide you a notification badge letting you know there is something new for you to check out on their websites.

Microsoft collects data necessary to provide features you request in Microsoft Edge. For example, you may choose to sync browser information saved on your device across other devices when you are signed in with your Microsoft account. You may choose which browser data to sync, including your favorites, browsing history, extensions and associated data, settings, open tabs, autofill form entries (such as your name, address, and phone number), passwords, payment information, and other data types as they become available. If you choose to sync extensions that you acquired from third-party web stores, a copy of those extensions will be downloaded directly from those web stores on your synced device(s). If you have turned on Password Monitor, your saved credentials are hashed, encrypted and sent to Microsoft's Password Monitor service to warn you if your credentials were detected as part of a malicious attack or a breach. Microsoft does not retain this data after the check is complete. You can disable or configure syncing in the Microsoft Edge settings.

Microsoft Edge's **Search and site suggestions** uses your search queries and browsing history to provide you with faster browsing and more relevant search recommendations. Microsoft Edge sends the information you type into the browser address bar to the default search provider configured in the address bar to offer search recommendations as you type each

character. You can turn off these features at any time in the browser settings. In order to provide search results, Microsoft Edge sends your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the Bing section of this privacy statement.

Microsoft Edge collects and uses data from your search activity across the web, including websites Microsoft does not own or operate, to improve Microsoft services, such as Microsoft Edge, Microsoft Bing and Microsoft News. This data may include the search query, the search results that are displayed to you, demographic information that is part of the search results, and the interaction you have with those search results, such as the links you click. Microsoft Edge takes steps to de-identify the data it collects by removing data that identifies the person or device from which it was collected and retains this data for one year from when it is collected. Microsoft does not use this collected data to personalize or provide ads to you. You can turn off the collection of this data at any time in the browser settings.

Microsoft Edge downloads content from Microsoft services to enhance your browsing experiences; for example, when data is downloaded to prerender site content for faster browsing or to provide content required to power features you choose to use, such as providing templates for Collections.

You may also choose to share your Microsoft Edge browsing activity to allow us to personalize Microsoft Edge and Microsoft services like ads, search, shopping, and news. Microsoft Edge browsing activity includes your history, favorites, usage data, and other browsing data. For more information about our **advertising privacy policies** see the Advertising section of the privacy statement. In the Microsoft privacy dashboard you can control the use of your browsing activity for personalized ads in the **See ads that interest you** setting. If you disable this setting in the Microsoft privacy dashboard you will continue to receive personalized web experiences like search and news based on your browsing activity if you have **Allow Microsoft to use your browsing activity including history, favorites, usage and other browsing data to personalize Microsoft Edge and Microsoft services like ads, search, shopping and news** turned on in Microsoft Edge settings. You may disable this browser setting in Microsoft Edge at any time to stop receiving personalized web experiences based on your browsing activity.

Microsoft Edge collects required diagnostic data to solve problems and to keep Microsoft Edge up to date, secure, and operating properly. Required diagnostic data also helps us improve Microsoft Edge and Windows.

Separate from your search activity data mentioned above, you can choose to send optional diagnostic data about how you use Microsoft Edge and information about your browser activity, including browsing history and search terms to Microsoft to help us improve Microsoft Edge and other Microsoft products and services. For Microsoft Edge on Windows 10 and later, this information is provided when you have enabled optional diagnostic data. For details, see the Windows Diagnostics section of the privacy statement. For Microsoft Edge on other operating systems, optional diagnostic information is provided when you enable **Improve Microsoft products by sending data about how you use the browser** or **Make**

searches and Microsoft products better by sending info about websites you visit in Microsoft Edge in the browser settings.

The diagnostic data collected by Microsoft Edge is transmitted to Microsoft and is stored with one or more unique identifiers that help us recognize an individual browser installation on a device and understand the browser's service issues and use patterns.

[Learn more about Microsoft Edge, browsing data, and privacy.](#)

Microsoft Edge on iOS and Android. Microsoft Edge on iOS and Android devices collects data necessary to provide features you request in Microsoft Edge. Microsoft also collects required diagnostic data to solve problems and to keep Microsoft Edge up to date, secure, and operating properly. Required diagnostic data also helps us improve Microsoft Edge.

Additionally, you may share optional diagnostic data about how you use Microsoft Edge and information about websites you visit (browsing history) for personalized experiences on your browser, Windows, and other Microsoft products and services. This information also helps us improve Microsoft Edge and other Microsoft products and services. This optional diagnostic data is sent to us when you enable **Share usage data for personalization** or **Share info about websites you visit** in the browser settings.

The diagnostic data collected by Microsoft Edge is transmitted to Microsoft and is stored with one or more unique identifiers that help us recognize an individual user on a device and understand the browser's service issues and use patterns.

For information about the privacy practices of legacy versions Microsoft Edge (versions 44 and below), see the Web browsers—Microsoft Edge Legacy and Internet Explorer section of the privacy statement.

Microsoft Translator

Microsoft Translator is a machine translation system and service designed to automatically translate text and voice input between numerous supported languages. Microsoft Translator is made available as a stand-alone consumer app for Android, iOS, and Windows and its service capabilities are also integrated in a variety of Microsoft products and services, such as Translator Hub, Translator for Bing, and Translator for Microsoft Edge. Microsoft Translator processes the text, image, and voice data you submit, as well as device and usage data. We use this data to provide Microsoft Translator, personalize your experiences, and improve our products and services. Microsoft has implemented business and technical measures designed to help de-identify the data you submit to Microsoft Translator. For example, when we randomly sample text and audio to improve Microsoft Translator and Microsoft's speech recognition technologies, we delete identifiers and certain text, such as email addresses and some number sequences, detected in the sample that could contain personal data. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#).

Separate from Microsoft Translator, Microsoft translation services are available as features in other Microsoft products and services that have different privacy practices than Microsoft

Translator. For more information on the Microsoft Azure Cognitive Services Translator Text API, Custom Translator, and Translator Speech API, see the [Enterprise and developer products](#) section of this privacy statement. For the Translate feature in Office apps and Skype, see the [Productivity and communications products](#) section of this privacy statement.

SwiftKey

The Microsoft Swiftkey keyboard and related cloud-based services (collectively, the “SwiftKey Services”) process data about words you use and how you type and use this data to learn your writing style and provide personalized autocorrection and predictive text that adapts to you. We also use this data to offer a range of other features, such as hashtag and emoji predictions.

SwiftKey prediction technology learns from the way you use language to build a personalized language model. This model is an optimized view of the words and phrases that you use most often in context and reflects your unique writing style. The model itself contains the words you commonly type arranged in a way that enables SwiftKey’s algorithms to make predictions, based on text you have already entered. The model draws from all scenarios in which you use your keyboard, including when you type while using apps or visiting websites. The SwiftKey keyboard and model attempt to avoid collecting sensitive data, by not collecting data from certain fields such as those recognized as containing password or payment data. SwiftKey Services do not log, store, or learn from data you type, or the data contained in your model, unless you choose to share your data with us (as described further below). When you use SwiftKey Services, we also collect device and usage data. We use de-identified device and usage data to analyze service performance and help improve our products.

The SwiftKey Services also include an optional cloud component called a SwiftKey Account. If you choose to create a SwiftKey Account, your language model will be synced with the SwiftKey Account cloud service, so you can benefit from that model on the different devices you use and access additional services such as prediction synchronization and backup. When you create a SwiftKey Account, Microsoft will also collect your email address and basic demographic data. All data collected is transferred to our servers over encrypted channels.

You may also opt in to share your language, typing data, and/or voice clips for the purposes of improving Microsoft products and services. Depending on the opt-ins you choose, SwiftKey may send short snippets of data about what and how you type and/or your voice clips, and related correction data to our servers for processing. These text snippets and/or voice clips are used in various automated processes to validate that our prediction services are working correctly and to make product improvements. To preserve your privacy, SwiftKey Services de-identify these text snippets, and even if you have a SwiftKey Account, these text snippets and/or voice clips will not be linked to it. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#).

If you sign into your SwiftKey Account and opt to share your language and typing data or voice clips, Microsoft will process your shared data in order to look for new patterns of language usage across our user base. This allows us to improve our basic models for

individual languages. Language and typing data used in this process is aggregated and any words or combinations of words that might be personal to individuals or small groups of users are filtered out.

You can withdraw your consent to share your language and typing data or voice clips for product improvement at any time in SwiftKey Settings. You can also withdraw your consent for SwiftKey Services to retain your personal data in SwiftKey Settings. When you withdraw consent for SwiftKey to retain your personal data, all personal data collected through your use of the SwiftKey Services will be deleted.

You may receive occasional notifications on your device alerting you to product updates and features that may be of interest to you. You can disable these notifications at any time in the SwiftKey Settings.

Windows

Windows is a personalized computing environment that enables you to seamlessly roam and access services, preferences, and content across your computing devices from phones to tablets to the Surface Hub. Rather than residing as a static software program on your device, key components of Windows are cloud-based, and both cloud and local elements of Windows are updated regularly, providing you with the latest improvements and features. In order to provide this computing experience, we collect data about you, your device, and the way you use Windows. And because Windows is personal to you, we give you choices about the personal data we collect and how we use it. Note that if your Windows device is managed by your organization (such as your employer or school), your organization may use centralized management tools provided by Microsoft or others to access and process your data and to control device settings (including privacy settings), device policies, software updates, data collection by us or the organization, or other aspects of your device. Additionally, your organization may use management tools provided by Microsoft or others to access and process your data from that device, including your interaction data, diagnostic data, and the contents of your communications and files. For more information about data collection in Windows, see [Data collection summary for Windows](#). This statement discusses Windows 10 and Windows 11 and references to Windows in this section relate to those product versions. Earlier versions of Windows (including Windows Vista, Windows 7, Windows 8, and Windows 8.1) are subject to their own privacy statements.

Activation

When you activate Windows, a specific product key is associated with the device on which your software is installed. The product key and data about the software and your device is sent to Microsoft to help validate your license to the software. This data may be sent again if there is a need to re-activate or validate your license. On phones running Windows, device and network identifiers, as well as device location at the time of the first power-up of the device, are also sent to Microsoft for the purpose of warranty registration, stock replenishment, and fraud prevention.

Activity history

Activity history helps keep track of the things you do on your device, such as the apps and services you use, the files you open, and the websites you browse. Your activity history is created when using different apps and features such as Microsoft Edge Legacy, some Microsoft Store apps, and Microsoft 365 apps and is stored locally on your device. If you've signed in to your device with a work or school account and give your permission, Windows sends your activity history to Microsoft. Once your activity history is in the cloud, Microsoft uses that data to enable cross-device experiences, to provide you with the ability to continue those activities on other devices, to provide personalized experiences (such as ordering your activities based on duration of use) and relevant suggestions (such as anticipating what your needs might be based on your activity history), and to help improve Microsoft products.

You can turn settings off or on for sending your activity history to Microsoft and storing activity history locally on your device, and you can also clear your device's activity history at any time by going to **Privacy > Activity history** in the Windows settings app. [Learn more about activity history in Windows.](#)

Advertising ID

Windows generates a unique advertising ID for each person using a device, which app developers and advertising networks can then use for their own purposes, including providing relevant advertising in apps. When the advertising ID is enabled, both Microsoft apps and third-party apps can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. Thus, your advertising ID can be used by app developers and advertising networks to provide more relevant advertising and other personalized experiences across their apps and on the web. Microsoft collects the advertising ID for the uses described here only when you choose to enable the advertising ID as part of your privacy setting.

The advertising ID setting applies to Windows apps using the Windows advertising identifier. You can turn off access to this identifier at any time by turning off the advertising ID in the Windows settings app. If you choose to turn it on again, the advertising ID will be reset and a new identifier will be generated. When a third-party app accesses the advertising ID, its use of the advertising ID will be subject to its own privacy policy. [Learn more about advertising ID in Windows.](#)

The advertising ID setting does not apply to other methods of interest-based advertising delivered by Microsoft or third parties, such as cookies used to provide interest-based display ads on websites. Third-party products accessed through or installed on Windows may also deliver other forms of interest-based advertising subject to their own privacy policies. Microsoft delivers other forms of interest-based ads in certain Microsoft products, both directly and by partnering with third-party ad providers. For more information on how

Microsoft uses data for advertising, see the [How we use personal data](#) section of this statement.

Diagnostics

Microsoft collects Windows diagnostic data to solve problems and to keep Windows up to date, secure, and operating properly. It also helps us improve Windows and related Microsoft products and services and, for customers who have turned on the “Tailored experiences” setting, to provide more relevant tips and recommendations to tailor Microsoft and third-party products and services for Windows to the customer’s needs. This data is transmitted to Microsoft and stored with one or more unique identifiers that can help us recognize an individual user on an individual device and understand the device’s service issues and use patterns.

There are two levels of diagnostic and activity data: Required diagnostic data and Optional diagnostic data. Certain product documentation and other materials refer to Required diagnostic data as Basic diagnostic data and to Optional diagnostic data as Full diagnostic data.

If an organization (such as your employer or school) uses Azure Active Directory (AAD) to manage the account it provides to you and enrolls your device in the Windows diagnostic data processor configuration, Microsoft’s processing of diagnostic data in connection with Windows is governed by a contract between Microsoft and the organization. If an organization uses Microsoft management tools or engages Microsoft to manage your device, Microsoft and the organization will use and process diagnostic and error data from your device to allow the management, monitoring, and troubleshooting of your devices managed by the organization, and for other purposes of the organization.

Required diagnostic data includes information about your device, its settings and capabilities, and whether it is performing properly. We collect the following Required diagnostic data:

- ◆ Device, connectivity, and configuration data:
 - Data about the device such as the processor type, OEM manufacturer, type of battery and capacity, number and type of cameras, firmware, and memory attributes.
 - Network capabilities and connection data such as the device’s IP address, mobile network (including IMEI and mobile operator), and whether the device is connected to a free or paid network.
 - Data about the operating system and its configuration such as the OS version and build number, region and language settings, diagnostics data settings, and whether the device is part of the Windows Insider program.
 - Data about connected peripherals such as model, manufacturer, drivers, and compatibility data.
 - Data about the applications installed on the device such as application name, version, and publisher.

- ◆ Whether a device is ready for an update and whether there are factors that may impede the ability to receive updates, such as low battery, limited disk space, or connectivity through a paid network.
- ◆ Whether updates complete successfully or fail.
- ◆ Data about the reliability of the diagnostics collection system itself.
- ◆ Basic error reporting, which is health data about the operating system and applications running on your device. For example, basic error reporting tells us if an application, such as Microsoft Paint or a third-party game, hangs or crashes.

Optional diagnostic data includes more detailed information about your device and its settings, capabilities, and device health. Optional diagnostic data also includes data about the websites you browse, device activity (also sometimes referred to as usage), and enhanced error reporting that helps Microsoft to fix and improve products and services for all users. When you choose to send Optional diagnostic data, Required diagnostic data will always be included, and we collect the following additional information:

- ◆ Additional data about the device, connectivity, and configuration, beyond that collected under Required diagnostic data.
- ◆ Status and logging information about the health of operating system and other system components beyond that collected about the update and diagnostics systems under Required diagnostic data.
- ◆ App activity, such as which programs are launched on a device, how long they run, and how quickly they respond to input.
- ◆ Browser activity, including browsing history and search terms, in Microsoft browsers (Microsoft Edge or Internet Explorer).
- ◆ Enhanced error reporting, including the memory state of the device when a system or app crash occurs (which may unintentionally contain user content, such as parts of a file you were using when the problem occurred). Crash data is never used for Tailored experiences as described below.

Some of the data described above may not be collected from your device even if you choose to send Optional diagnostic data. Microsoft minimizes the volume of Optional diagnostic data it collects from all devices by collecting some of the data from only a subset of devices (sample). By running the Diagnostic Data Viewer tool, you can see an icon which indicates whether your device is part of a sample and also which specific data is collected from your device. Instructions for how to download the Diagnostic Data Viewer tool can be found in the Windows settings app under Diagnostics & feedback.

Specific data items collected in Windows diagnostics are subject to change to give Microsoft flexibility to collect the data needed for the purposes described. For example, to enable Microsoft to troubleshoot the latest performance issue impacting users' computing experience or update a Windows device that is new to the market, Microsoft may need to collect data items that were not collected previously. For a current list of data types collected at **Required diagnostic data** and **Optional diagnostic data**, see [Windows Required \(Basic level\) diagnostic events and fields](#) or [Windows Optional \(Full level\) diagnostic data](#). We provide limited portions of error report information to partners (such as the device manufacturer) to help them troubleshoot products and services which work with Windows and other Microsoft

product and services. They are only permitted to use this information to repair or improve those products and services. We may also share some aggregated, de-identified diagnostic data, such as general usage trends for Windows apps and features, with selected third parties. [Learn more about diagnostic data in Windows.](#)

Inking and typing Recognition. You also can choose to help Microsoft improve inking and typing recognition by sending inking and typing diagnostic data. If you choose to do so, Microsoft will collect samples of the content you type or write to improve features such as handwriting recognition, autocompletion, next word prediction, and spelling correction in the many languages used by Microsoft customers. When Microsoft collects inking and typing diagnostic data, it is divided into small samples and processed to remove unique identifiers, sequencing information, and other data (such as email addresses and numeric values) which could be used to reconstruct the original content or associate the input to you. It also includes associated performance data, such as changes you manually make to text, as well as words you've added to the dictionary. [Learn more about improving inking and typing in Windows.](#)

If you choose to turn on **Tailored experiences**, we will use your Windows diagnostic data (Required or Optional as you have selected) to offer you personalized tips, ads, and recommendations to enhance Microsoft experiences. If you have selected Required as your diagnostic data setting, personalization is based on information about your device, its settings and capabilities, and whether it is performing properly. If you have selected Optional, personalization is also based on information about how you use apps and features, plus additional information about the health of your device. However, we do not use information about the websites you browse, the content of crash dumps, speech, typing, or inking input data for personalization when we receive such data from customers who have selected Optional.

Tailored experiences include suggestions on how to customize and optimize Windows, as well as ads and recommendations for Microsoft and third-party products and services, features, apps, and hardware for your Windows experiences. For example, to help you get the most out of your device, we may tell you about features you may not know about or that are new. If you are having a problem with your Windows device, you may be offered a solution. You may be offered a chance to customize your lock screen with pictures, or to be shown more pictures of the kind you like, or fewer of the ones you do not. If you stream movies in your browser, you may be recommended an app from the Microsoft Store that streams more efficiently. Or, if you are running out of space on your hard drive, Windows may recommend you try OneDrive or purchase hardware to gain more space. [Learn more about tailored experiences in Windows.](#)

Feedback Hub

Feedback Hub is a preinstalled app that provides a way to gather feedback on Microsoft products and installed first party and third-party apps. You can sign into Feedback Hub using either your personal Microsoft account or an account provided by your organization (such as your employer or school) that you use to sign into Microsoft products. Signing in with your work or school account allows you to submit feedback to Microsoft in association with your organization.

Any feedback you provide whether using your work or school account or personal Microsoft account may be publicly viewable depending on the settings configured by your organization's administrators. Additionally, if feedback is provided using your work or school account, your feedback can be viewed through the Feedback Hub by your organization's administrators.

When you submit feedback to Microsoft about a problem or add more details to a problem, diagnostic data will be sent to Microsoft to improve Microsoft products and services. Depending on your Diagnostic data settings in the **Diagnostics & feedback** section of the Windows settings app, Feedback Hub will either send diagnostic data automatically or you will have the option to send it to Microsoft at the time you provide feedback. Based on the category chosen when submitting feedback, there may be additional personal data collected that helps to further troubleshoot issues; for example, location related information when submitting feedback about location services or gaze related information when submitting feedback on Mixed Reality. Microsoft may also share your feedback along with the data collected when you submit your feedback with Microsoft partners (such as a device manufacturer, or firmware developer) to help them troubleshoot products and services that work with Windows and other Microsoft products and services. [Learn more about diagnostic data in Windows.](#)

Location services and recording

Windows location service. Microsoft operates a location service that helps determine the precise geographic location of a specific Windows device. Depending on the capabilities of the device, the device's location can be determined with varying degrees of accuracy and may in some cases be determined precisely. When you have enabled location on a Windows device, or you have given permission for Microsoft apps to access location information on non-Windows devices, data about cell towers and Wi-Fi access points and their locations is collected by Microsoft and added to the location database after removing any data identifying the person or device from which it was collected. This de-identified location information is used to improve Microsoft's location services and, in some instances, shared with our location service provider partners, currently HERE (see <https://www.here.com/>) and Skyhook (see <https://www.skyhook.com>) to improve the location services of the provider.

Windows services and features, apps running on Windows, and websites opened in Windows browsers can access the device's location through Windows if your settings allow them to do so. Some features and apps request location permission when you first install Windows, some ask the first time you use the app, and others ask every time you access the device's location. For information about certain Windows apps that use the device's location, see the [Windows apps](#) section of this privacy statement.

When an app or feature accesses the device's location and you are signed in with a Microsoft account, your Windows device will also upload its location to the cloud where it is available across your devices to other apps or services that use your Microsoft account and for which you've granted permission. We will retain only the last known location (each new location replaces the previous one). Data about a Windows device's recent location history is also

stored on the device even if not using a Microsoft account, and certain apps and Windows features can access this location history. You can clear your device's location history at any time in the Windows settings app.

In the Windows settings app, you can also view which apps have access to the device's precise location or your device's location history, turn off or on access to the device's location for particular apps, or turn off access to the device's location. You can also set a default location, which will be used when the location service can't detect a more exact location for your device.

Even when you've turned off access to the device's location, some third-party desktop apps and services could use other technologies (such as Bluetooth, Wi-Fi, cellular modem, etc.) to determine the device's precise location. [Learn more about third-party desktop apps and how they may still be able to determine your device's location when the device's location setting is off.](#)

In addition, to facilitate getting help in an emergency, whenever you make an emergency call, Windows will attempt to determine and share your precise location, regardless of your location settings. If your device has a SIM card or is otherwise using cellular service, your mobile operator will have access to your device's location. [Learn more about location in Windows.](#)

General Location. If you turn on Location services, apps that cannot use your precise location may still have access to your general location, such as your city, postal code, or region.

Find my device. The Find my device feature allows an administrator of a Windows device to find the location of that device from account.microsoft.com/devices. To enable Find my device, an administrator needs to be signed in with a Microsoft account and have the location setting enabled. This feature will work even if other users have denied access to location for all their apps. When the administrator attempts to locate the device, users will see a notification in the notification area. [Learn more about Find my device in Windows.](#)

Recording. Some Windows devices have a recording feature that allows you to capture audio and video clips of your activity on the device, including your communications with others. If you choose to record a session, the recording will be saved locally on your device. In some cases, you may have the option to transmit the recording to a Microsoft product or service that broadcasts the recording publicly. **Important: You should understand your legal responsibilities before recording and/or transmitting any communication. This may include obtaining the prior consent of everyone participating in the conversation or any other authorizations as required.** Microsoft is not responsible for how you use recording features or your recordings.

Phone Link

The Phone Link app lets you link your Android phone with your Windows device, enabling a variety of cross-device experiences. You can use Phone Link to see recent photos from your

Android phone on your Windows device; make and receive calls from your Android phone on your Windows device; view and send text messages from your Windows device; view, dismiss, or perform other actions to your Android phone notifications from your Windows device; and share your phone screen on your Windows device through Phone Link's mirroring function.

To use Phone Link, the Phone Link app must be installed on your Windows device and the Link to Windows app must be installed on your Android phone. Upon launching the Phone Link app on your Windows device, you will be prompted to provide your mobile phone number. We use this mobile phone number solely to send you a link with information about downloading the Link to Windows app.

To use Phone Link, you must log into your Microsoft account on the Phone Link app on your Windows device and on the Link to Windows app on your Android phone. Your Android phone must be connected to Wi-Fi and your Windows device must be connected to the internet and permit Phone Link to run in the background. To use Phone Link's mirroring function, your Android phone must also have Bluetooth enabled. Phone Link also requires your Windows device to be set up with Windows Hello, as an additional security measure.

As part of providing Phone Link's features to you, Microsoft collects performance, usage, and device data that includes, for example, the hardware capabilities of your mobile phone and Windows device, the number and duration of your sessions on Phone Link, and the amount of time you spent during setup.

You can unlink your Android phone from your Windows device at any time by logging in with your Microsoft account at accounts.microsoft.com/devices and updating the Settings on your Android phone. For detailed information, see [our support page](#).

Text Messages. Phone Link allows you to view text messages delivered to your Android phone on your Windows device and send text messages from your Windows device. Only text messages received and sent within the last 30 days are visible on your Windows device. These text messages are temporarily stored on your Windows device. We never store your text messages on our servers or change or delete any text messages on your Android phone. You can see messages sent via SMS (Short Message Service) and MMS (Multimedia Messaging Service) but not messages sent via RCS (Rich Communication Services). To provide this functionality, Phone Link accesses the content of your text messages and the contact information of the individuals or businesses from whom you are receiving or sending text messages.

Calls. Phone Link allows you to make and receive calls from your Android phone on your Windows device. Through Phone Link, you can also view your recent calls on your Windows device. To activate this feature, you must enable certain permissions on both your Windows device and Android phone, such as call logs access and permission to make phone calls from your PC. These permissions can be revoked at any time under the Phone Link Settings page on your Windows device and your Android phone's settings. Only calls received and dialed within the last 30 days are visible under call logs on your Windows device. These call details are temporarily stored on your Windows device. We do not change or delete your call history on your Android phone.

Photos. Phone Link allows you to copy, share or edit photos from your Android phone on your Windows device. Only a limited number of your most recent photos from the Camera Roll and Screenshots folders on your Android phone will be visible on your Windows device at any given time. These photos are temporarily stored on your Windows device and as you take more photos on your Android phone, we remove the temporary copies of the older photos from your Windows device. We never store your photos on our servers or change or delete any photos on your Android phone.

Notifications. Phone Link allows you to view your Android phone's notifications on your Windows device. Through Phone Link, you can read and dismiss your Android phone's notifications from your Windows device or perform other actions related to the notifications. To activate this Phone Link feature, you must enable certain permissions, such as sync notifications, on both your Windows device and Android phone. These permissions can be revoked at any time under the Phone Link Settings page on your Windows device and your Android phone's settings. For detailed information, see [our support page](#).

Mirroring. Phone Link allows you to view your Android phone's screen on your Windows device. Your Android phone screen will be visible on your Windows device as a pixel stream and any audio that you enable on your Android phone screen while it is linked to your Windows device through Phone Link will play through your Android phone.

Text-to-voice. Phone Link features include accessibility functionality such as text-to-voice. You can activate a text-to-voice feature, which allows you to hear the contents of a text message or notification as audio. If you activate this feature, your text messages and notifications will be read out loud as they are received.

Security and safety features

Device encryption. Device encryption helps protect the data stored on your device by encrypting it using BitLocker Drive Encryption technology. When device encryption is on, Windows automatically encrypts the drive Windows is installed on and generates a recovery key. The BitLocker recovery key for your personal device is automatically backed up online in your personal Microsoft OneDrive account. Microsoft doesn't use your individual recovery keys for any purpose.

Malicious Software Removal Tool. The Malicious Software Removal Tool (MSRT) runs on your device at least once per month as part of Windows Update. MSRT checks devices for infections by specific, prevalent malicious software ("malware") and helps remove any infections found. When the MSRT runs, it will remove the malware listed on the Microsoft Support website if the malware is on your device. During a malware check, a report will be sent to Microsoft with specific data about malware detected, errors, and other data about your device. If you do not want MSRT to send this data to Microsoft, you can disable MSRT's reporting component.

Microsoft Family. Parents can use Microsoft Family to understand and set boundaries on how their child is using their device. There are many features available to Family members, so

please carefully review the information provided when you create or join a Family. If you live in a region that requires permission to create an account to access Microsoft services, you may be prompted to request or give parental consent. If a user is under the statutory age in your region, during the registration process they will be prompted to request consent from a parent or guardian by entering an adult's email. When Family activity reporting is turned on for a child, Microsoft will collect details about how the child uses their device and provide parents with reports of that child's activities. Activity reports are routinely deleted from Microsoft servers after a short period of time.

Microsoft Defender SmartScreen. Microsoft Defender SmartScreen helps protect you when using our services by checking downloaded files and web content for malicious software, potentially unsafe web content, and other threats to you or your device. When checking a file, data about that file is sent to Microsoft, including the file name, a hash of the file's contents, the download location, and the file's digital certificates. If Microsoft Defender SmartScreen identifies the file as unknown or potentially unsafe, you will see a warning prior to opening the file. When checking web content, data about the content and your device is sent to Microsoft, including the full web address of the content. If Microsoft Defender SmartScreen detects that content is potentially unsafe, you will see a warning in place of the content. Microsoft Defender SmartScreen can be turned on or off in Settings.

Microsoft Defender Antivirus. Microsoft Defender Antivirus looks for malware and other unwanted software, potentially unwanted apps, and other malicious content on your device. Microsoft Defender Antivirus is automatically turned on to help protect your device if no other antimalware software is actively protecting your device. If Microsoft Defender Antivirus is turned on, it will monitor the security status of your device. When Microsoft Defender Antivirus is turned on, or is running because Limited Periodic Scanning is enabled, it will automatically send reports to Microsoft that contain data about suspected malware and other unwanted software, potentially unwanted apps, and other malicious content, and it may also send files that could contain malicious content, such as malware or unknown files for further inspection. If a report is likely to contain personal data, the report is not sent automatically, and you'll be prompted before it is sent. You can configure Microsoft Defender Antivirus not to send reports and suspected malware to Microsoft.

Speech, Voice Activation, Inking, and Typing

Speech. Microsoft provides both a device-based speech recognition feature and cloud-based (online) speech recognition technologies.

Turning on the Online speech recognition setting lets apps use Microsoft cloud-based speech recognition. Additionally, in Windows 10, the Online speech recognition setting enables your ability to use dictation within Windows.

Turning on speech while setting up a HoloLens device or installing Windows Mixed Reality allows you to use your voice for commands, dictation, and app interactions. Both device-based speech recognition and online speech recognition settings will be enabled. With both settings enabled, while your headset is turned on the device will always be listening to your

voice input and will send your voice data to Microsoft's cloud-based speech recognition technologies.

When you use cloud-based speech recognition technologies from Microsoft, whether enabled by the Online speech recognition setting or when you interact with HoloLens or voice typing, Microsoft collects and uses your voice recordings to provide the speech recognition service by creating a text transcription of the spoken words in the voice data. Microsoft will not listen to your voice recording without your permission. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#).

You can use device-based speech recognition without sending your voice data to Microsoft. However, Microsoft cloud-based speech recognition technologies provide more accurate recognition than the device-based speech recognition. When the online speech recognition setting is turned off, speech services that do not rely on the cloud and only use device-based recognition—like the Narrator app or the Windows Speech Recognition app—will still work and Microsoft won't collect any voice data.

You can turn off online speech recognition at any time. This will stop any apps that rely on the Online speech recognition setting from sending your voice data to Microsoft. If you are using a HoloLens or Windows Mixed Reality headset, you can also turn off device-based speech recognition at any time. This will stop the device from listening for your voice input. [Learn more about speech recognition in Windows](#).

Voice Activation. Windows provides supported apps with the ability to respond and take action based on voice keywords that are specific to that app—for example allowing Cortana to listen and respond when you say "Cortana."

If you've given permission for an app to listen for voice keywords, Windows will be actively listening to the microphone for these keywords. Once a keyword is recognized, the app will have access to your voice recording, can process the recording, take action, and respond, such as with a spoken answer. The app may send the voice recording to its own services in the cloud to process the commands. Each app should ask you for permission before accessing voice recordings.

Additionally, voice activation can be enabled when the device is locked. If enabled, the relevant app will continue listening to the microphone for voice keywords when you have locked your device and can activate for anyone who speaks near the device. When the device is locked, the app will have access to the same set of capabilities and information as when the device is unlocked.

You can turn off voice activation at any time. [Learn more about voice activation in Windows](#).

Even when you've turned off voice activation, some third-party desktop apps and services could still be listening to the microphone and collect your voice input. [Learn more about third-party desktop apps and how they may still be able to access your microphone even with these settings turned off](#).

Voice typing. In Windows 11, dictation has been updated and renamed as voice typing. Like dictation, voice typing uses online speech recognition technologies to power its speech-to-text transcription service. You can also choose to contribute voice clips to help improve voice typing. If you choose not to contribute voice clips, you can still use voice typing. You can change your choice anytime in the voice typing settings. Microsoft will not listen to your voice recordings without your permission. [Learn more about voice typing in Windows.](#)

Inking & Typing Personalization. Your typed and handwritten words are collected to provide you with: a personal dictionary, better character recognition to help you type and write on your device, and text suggestions that appear as you type or write.

You can turn off Inking & typing personalization at any time. This will delete data stored on your device, such as your personal dictionary. [Learn more about inking & typing personalization in Windows.](#)

Sync and backup settings

When you sign into Windows with your Microsoft account or work or school account, Windows can store your settings, files, and device configuration data in Microsoft's servers. Windows will only use the stored settings, files, and device configuration data to make it easier for you to migrate your experience on a different device.

You can turn off this feature and stop Windows from storing your settings, files, and configuration data from the Windows settings app. You can also delete the sync and backup data Windows has stored in the settings app.

[Learn more about Windows backup and sync settings.](#)

Update Services

Update Services for Windows includes Windows Update and Microsoft Update. Windows Update is a service that provides you with software updates for Windows software and other supporting software, such as drivers and firmware supplied by device manufacturers. Microsoft Update is a service that provides you with software updates for other Microsoft software such as Microsoft 365.

Windows Update automatically downloads Windows software updates to your device. You can configure Windows Update to automatically install these updates as they become available (recommended) or have Windows notify you when a restart is required to finish installing updates. Apps available through the Microsoft Store are automatically updated through the Microsoft Store, as described in the [Microsoft Store](#) section of this privacy statement.

Web browsers—Microsoft Edge Legacy and Internet Explorer

This section applies to legacy versions of Microsoft Edge (versions 44 and below). See the [Microsoft Edge](#) section of the Privacy Statement for information about non-legacy versions of Microsoft Edge.

Microsoft Edge is the default web browser for Windows. Internet Explorer, the legacy browser from Microsoft, is also available in Windows. Whenever you use a web browser to access the internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address, browser type and language, access times, and referring website addresses. This data might be logged on those websites' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use. Additionally, Microsoft Edge sends a unique browser ID to certain websites to enable us to develop aggregate data used to improve browser features and services.

Additionally, data about how you use your browser, such as your browsing history, web form data, temporary internet files, and cookies, is stored on your device. You can delete this data from your device using Delete Browsing History.

Microsoft Edge allows you to capture and save content on your device, such as:

- ♦ **Web note.** Allows you to create ink and text annotations on the webpages you visit, and clip, save, or share them.
- ♦ **Active reading.** Allows you to create and manage reading lists, including websites or documents.
- ♦ **Hub.** Allows you to easily manage your reading lists, favorites, downloads, and history all in one area.
- ♦ **Website Pin to Taskbar.** Allows you to pin your favorite websites to the Windows taskbar. Websites will be able to see which of their webpages you have pinned, so they can provide you a notification badge letting you know there is something new for you to check out on their websites.

Some Microsoft browser information saved on your device will be synced across other devices when you sign in with your Microsoft account. For instance, in Internet Explorer, this information includes your browsing history and favorites; and in Microsoft Edge, it includes your favorites, reading lists, autofill form entries (such as your name, address, and phone number), and may include data for extensions that you have installed. As an example, if you sync your Microsoft Edge reading list across devices, copies of the content you choose to save to your reading list will be sent to each synced device for later viewing. You can disable syncing in Internet Explorer by going to **Start > Settings > Accounts > Sync your settings**. (For more information, see the [Sync settings](#) section of this privacy statement.) You can also disable syncing of Microsoft Edge browser information by turning off the sync option in Microsoft Edge Settings.

Microsoft Edge and Internet Explorer use your search queries and browsing history to provide you with faster browsing and more relevant search results. These features include:

- ♦ **Search suggestions** in Internet Explorer automatically sends the information you type into the browser address bar to your default search provider (such as Bing) to offer search recommendations as you type each character.
- ♦ **Search and site suggestions** in Microsoft Edge automatically sends the information you type into the browser address bar to Bing (even if you have selected another default search provider) to offer search recommendations as you type each character.

You can turn off these features at any time. In order to provide search results, Microsoft Edge and Internet Explorer send your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the [Bing](#) section of this privacy statement.

Cortana can assist you with your web browsing in Microsoft Edge with features such as Ask Cortana. You can disable Cortana assistance in Microsoft Edge at any time in Microsoft Edge Settings. To learn more about how Cortana uses data and how you can control that, go to the [Cortana](#) section of this privacy statement.

Windows apps

A number of Microsoft apps are included with Windows and others are available in Microsoft Store. Some of those apps include:

Maps app. The Maps app provides location-based services and uses Bing services to process your searches within the Maps app. When the Maps app has access to your location, and you have enabled location-based services in Windows, when you use the "@" key to initiate a search in supported text boxes in Windows apps, Bing services collect the text you type after the "@" key to provide location-based suggestions. To learn more about these Bing-powered experiences, see the [Bing](#) section of this privacy statement. When the Maps app has access to your location, even when the app is not in use, Microsoft may collect de-identified location data from your device to improve Microsoft services. You can disable the Maps app's access to your location by turning off the location service or turning off the Maps app's access to the location service.

You can keep track of your favorite places and recent map searches in the Maps app. Your favorite places and search history will be included as search suggestions. If you're signed in with your Microsoft account, your favorite places, search history, and certain app settings will be synced across other devices and services (for example, Cortana). For more information, see the [Sync and backup settings](#) section of this privacy statement.

Camera app. If you allow the Camera app to use your location, location data is embedded in the photos and videos you take with your device. Other descriptive data, such as camera model and the date that the picture or video was taken, is also embedded in photos and videos. If you choose to share a photo or video, any embedded data will be accessible to the people and services you share with. Once enabled, you can always disable the Camera app's access to your location by turning off all access to the location service in your device's Settings menu or turning off the Camera app's access to the location service.

When the Camera app is open, it shows rectangles detected by the selected camera for areas in the image that are potentially used for image enhancement. The Camera app does not retain any image enhancing data. You can always change your camera access settings in the Camera app's Settings menu or the Windows Settings menu.

Photos app. The Photos app helps you organize and share your photos. For example, the Photos app presents different ways to group photos and videos by date, location, tags, and faces. The Collection tab displays photos and videos according to the date they are taken. The Album tab helps users organize their photos and videos by location and common tags. The People tab helps you organize your photos and videos by grouping photos and videos with similar faces, which you can then associate with contacts.

If you enable the People setting on the Photos app's settings page, the app will use face grouping technologies to organize your photos and videos into groups. The grouping feature can detect faces in a photo or video and determine whether they are visually similar to faces in other photos and videos in your local photo collection. You can choose to associate a facial grouping with a contact from your People app.

If you choose to share a photo or video using the Photos app, any embedded data (such as location, camera model, and date) will be accessible to the people and services you share the photo or video. If enabled, facial groupings are only accessible to you, on that device, within the Photos app and the groups and grouping data are not embedded in any shared photos or videos. You, and not Microsoft, are responsible for ensuring you have appropriate permissions from the people in your photos and videos to use facial grouping technology to group your photos and videos in your personal albums.

Your groupings will be stored on your device for as long as you choose to keep the groupings or the photos or videos. If the People setting is turned on, you will be prompted to allow the Photos app to continue to permit facial groupings after three years of non-interaction with the Photos app. At any time, you can go to the Settings page in the Photos app to turn the People setting on or off. This will remove facial grouping data from the Photos app, but will not remove your photos or videos. [Learn more about the Photos app and facial grouping.](#)

People app. The People app lets you see and interact with all your contacts in one place. When you add an account to the People app, your contacts from your account will be automatically added to the People app. You can add other accounts to the People app, including your social networks (such as Facebook and Twitter) and email accounts. When you add an account, we tell you what data the People app can import or sync with the particular service and let you choose what you want to add. Other apps you install may also sync data to the People app, including providing additional details to existing contacts. When you view a contact in the People app, information about your recent interactions with the contact (such as emails and calendar events, including from apps that the People app syncs data from) will be retrieved and displayed to you. You can remove an account from the People app at any time.

Mail and Calendar app. The Mail and Calendar app allows you to connect all your email, calendars, and files in one place, including those from third-party email and file storage providers. The app provides location-based services, such as weather information in your

calendar, but you can disable the app's use of your location. When you add an account to the Mail and Calendar app, your email, calendar items, files, contacts, and other settings from your account will automatically sync to your device and to Microsoft servers. At any time, you can remove an account or make changes to the data that's synced from your account. To configure an account, you must provide the app with the account credentials (such as user name and password), which will be sent over the internet to the third-party provider's server. The app will first attempt to use a secure (SSL) connection to configure your account but will send this information unencrypted if your email provider does not support SSL. If you add an account provided by an organization (such as a company email address), the owner of the organizational domain can implement certain policies and controls (for example, multi-factor authentication or the ability to remotely wipe data from your device) that may affect your use of the app.

Messaging app. When you sign in with a Microsoft account on your device, you can choose to back up your information, which will sync your SMS and MMS messages and store them in your Microsoft account. This allows you to retrieve the messages if you lose or change phones. After your initial device set-up, you can manage your messaging settings at any time. Turning off your SMS/MMS backup will not delete messages that have been previously backed up to your Microsoft account. To delete such messages, you must first delete them from your device prior to turning off backup. If you allow the Messaging app to use your location, you can attach a link to your current location to an outgoing message. Location information will be collected by Microsoft as described in the Windows [Location services](#) section of this privacy statement.

Narrator. Narrator is a screen-reading app that helps you use Windows without a screen. Narrator offers intelligent image and page title description and web page summaries when you encounter undescribed images and ambiguous links.

When you choose to get an image description by pressing Narrator + Ctrl + D, the image will be sent to Microsoft to perform analysis of the image and generate a description. Images are used only to generate the description and are not stored by Microsoft.

When you choose to get page title descriptions by pressing Narrator + Ctrl + D, the URL of the site you are visiting will be sent to Microsoft to generate the page title description and to provide and improve Microsoft services, such as Bing services as described in the Bing section above.

When you choose to get a list of popular links for a web page by pressing Narrator + double press of S, the URL of the site you are visiting will be sent to Microsoft to generate the summary of popular links and to provide and improve Microsoft services, such as Bing.

You can disable these features at any time by going to **Narrator > Get image descriptions, page titles and popular links** in the Windows setting app.

You can also send feedback about Narrator to help Microsoft diagnose and resolve problems with Narrator and improve Microsoft products and services, such as Windows. Verbal feedback can be submitted at any time in Narrator by using Narrator Key + Alt + F. When you use this command, the Feedback Hub app will launch, giving you the opportunity to submit verbal

feedback. If you enable the setting “Help Make Narrator Better” in the Windows settings app and submit verbal feedback through Feedback Hub, recent device and usage data, including event trace log (ETL) data, will be submitted along with your verbal feedback to improve Microsoft products and services, such as Windows.

Windows Media Player

Windows Media Player allows you to play CDs, DVDs, and other digital content (such as WMA and MP3 files), rip CDs, and manage your media library. To enrich your experience when you play content in your library, Windows Media player displays related media information, such as album title, song titles, album art, artist, and composer. To augment your media information, Windows Media player will send a request to Microsoft which contains standard computer information, an identifier for the media content, and the media information already contained in your Windows Media Player library (including information you may have edited or entered yourself) so that Microsoft can recognize the track and then return additional information that is available.

Windows Media Player also allows you to play back content that is streamed to you over a network. To provide this service, it is necessary for Windows Media Player to communicate with a streaming media server. These servers are typically operated by non-Microsoft content providers. During playback of streaming media, Windows Media Player will send a log to the streaming media server or other web server(s) if the streaming media server requests it. The log includes such details as: connection time, IP address, operating system version, Windows Media Player version, Player identification number (Player ID), date, and protocol. To protect your privacy, Windows Media Player defaults to sending a Player ID that is different for each session.

Windows Hello

Windows Hello provides instant access to your devices through biometric authentication. If you turn it on, Windows Hello uses your face, fingerprint, or iris to identify you based on a set of unique points or features that are extracted from the image and stored on your device as a template—but it does not store the actual image of your face, fingerprint, or iris. Biometric verification data that's used when you sign in doesn't leave your device. Your biometric verification data will remain on your device until you remove it. However, after a significant period of Windows Hello inactivity, you will be prompted to confirm that you want to continue to store your biometric verification data. You can delete your biometric verification data from within Settings. Learn more about [Windows Hello](#).

Windows Search

Windows Search lets you search your stuff and the web from one place. If you choose to use Windows Search to search "your stuff," it will provide results for items on your personal

OneDrive, your OneDrive for Business if so enabled, other cloud storage providers to the extent supported by those third-party providers, and on your device. If you choose to use Windows Search to search the web, or get search suggestions with Windows Search, your search results will be powered by Bing and we will use your search query as described in the [Bing](#) section of this privacy statement. [Learn more about search in Windows.](#)

Entertainment and related services

Entertainment and Related Services power rich experiences and enable you to access a variety of content, applications and games.

Xbox

The Xbox network is the online gaming and entertainment service from Microsoft that consists of software and enables online experiences across different platforms. This service lets you find and play games, view content, and connect with friends on Xbox and other gaming and social networks. You can connect to the Xbox network using Xbox consoles, Windows devices, and mobile devices (Android and iPhone).

When you sign up for an Xbox profile, we assign you a gamertag (a public nickname) and a unique identifier. When you sign in on Xbox devices, apps, and services, the data we collect about your use is stored using these unique identifier(s).

Xbox consoles are devices you can use to find and play games, movies, music, and other digital entertainment. When you sign in to Xbox experiences—in apps or on a console—we also assign a unique identifier to your device. When your Xbox console is connected to the internet, for instance, and you sign in to the console, we identify which console and which version of the console's operating system you're using.

Xbox continues to provide new experiences in client apps that are connected to and backed by services such as the Xbox network and cloud gaming. When signed in to an Xbox experience, we collect required data to help keep these experiences reliable, up to date, secure, and performing as expected.

Data we collect about your use of Xbox services, games, apps, and consoles includes:

- ◆ When you sign in and sign out of Xbox, any purchases you make, and content you obtain.
- ◆ Which games you play and apps you use, your game progress, achievements, play time per game, and other play statistics.
- ◆ Performance data about Xbox consoles, Xbox Game Pass and other Xbox apps, the Xbox network, connected accessories, and your network connection, including any software or hardware errors.
- ◆ Content you add, upload, or share through the Xbox network, including text, pictures, and video you capture in games and apps.

- ♦ Social activity, including chat data and interactions with other gamers, and connections you make (friends you add and people who follow you) on the Xbox network.

If you use an Xbox console or Xbox app on another device capable of accessing the Xbox network, and that device includes a storage device (hard drive or memory unit), usage data will be stored on the storage device and sent to Microsoft the next time you sign in to Xbox, even if you've been playing offline.

Xbox console diagnostic data. Diagnostic data has two categories: required and optional. If you use an Xbox console, the console will send required data to Microsoft. Optional data is additional data that you choose to share with Microsoft.

- ♦ **Required.** The minimum data necessary to help keep Xbox safe, secure, up to date, and performing as expected.
- ♦ **Optional.** Optional data includes additional details about your console, its settings, its health, its use, and enhanced error reporting to help us detect, diagnose, and fix problems.

Learn more at [Manage settings for optional data sharing](#).

Game captures. Any player in a multiplayer game session can record video (game clips) and capture screenshots of their view of the game play. Other players' game clips and screenshots can capture your in-game character and gamertag during that session. If a player captures game clips and screenshots on a PC, the resulting game clips might also capture audio chat.

Captioning. During Xbox real-time ("party") chat, players may activate a voice-to-text feature that lets them view that chat as text. If a player activates this feature, all voice communication in the party is captioned for the player. Microsoft uses the resulting text data to provide captioning of chat for players who need it, as well as the other purposes described in this statement.

Data use. Microsoft uses the data we collect to improve gaming products and experiences—making them safer and more fun over time.

Data we collect also enables us to provide you with personalized, curated experiences. This includes connecting you to games, content, and services, as well as presenting you with offers, discounts, and recommendations.

Xbox data viewable by others. Your gamertag, game and play statistics, achievements, presence (whether you are currently signed in to Xbox), content you share, and other data about your activity on Xbox can be seen by:

- ♦ Other players signed in to Xbox.
- ♦ Customers of third-party services you've linked your profile to, or
- ♦ Other services associated with Xbox (including those of partner companies).

For example, your gamertag and scores that show on game leaderboards are considered public and cannot be hidden. For other data, you can adjust your privacy settings on consoles and at [Xbox.com](https://xbox.com) to limit or block what is shared with the public or with friends.

Learn more at [Xbox online safety and privacy settings](#).

Xbox data shared with third parties including game and apps publishers. When you use an Xbox online game or any network-connected app on your Xbox console, PC, or mobile device, the publisher of that game or app has access to data about your usage to help the publisher deliver, support, and improve its product. This data may include: your Xbox user identifier, gamertag, limited account info such as country and age range, data about your in-game communications, any Xbox enforcement activity, game-play sessions (for example, moves made in-game, types of vehicles used in-game), your presence on the Xbox network, the time you spend playing the game or app, rankings, statistics, gamer profiles, avatars, or gamerpics, friends lists, activity feeds for official clubs you belong to, official club memberships, and any content you create or submit in the game or app.

Third-party publishers and developers of games and apps have their own distinct and independent relationship with users and their collection and usage of personal data is subject to their specific privacy policies. You should carefully review their policies to determine how they use the data. For example, publishers may choose to disclose or display game data (such as on leaderboards) through their own services. You may find their policies linked from game or app detail pages in the Microsoft Store.

Learn more at [Data Sharing with Games and Apps](#).

To stop sharing game or app data with a publisher, remove its games or app from all devices where you have installed them. Some publisher access to your data may be revoked at <https://microsoft.com/consent>.

Children and family. If you have kids who want to use the Xbox network, you can set up child and teen profiles for them once they have Microsoft accounts. Adult organizers in your Microsoft family group can change consent choices and online safety settings for child and teen profiles on [Xbox.com](#).

Learn more about Microsoft family groups at [Simplify your family's life](#).

Learn more about managing Xbox profiles, at [Xbox online safety and privacy settings](#).

For more information about Microsoft's collection of data from children, including Xbox, please see the [Collection of data from children](#) section of this privacy statement.

Safety. In order to help make the Xbox network a safe gaming environment and enforce the Community Standards for Xbox, we may collect and review voice, text, images, videos and in-game content (such as game clips you upload, conversations you have, and things you post in clubs and games).

Legacy.

- ♦ **Xbox 360.** This Xbox console collects limited required diagnostic data to keep your console functioning as expected while using a console connected to the Xbox network.
- ♦ **Kinect.** The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control gameplay. For example:

- If you choose, the camera can be used to sign you in to the Xbox network automatically using facial recognition. This data stays on the console and is not shared with anyone, and you can choose to delete this data from your console at any time.
- For game play, Kinect will map distances between your body's joints to create a stick figure representation of you that helps Kinect enable play.
- The Kinect microphone can enable voice chat between players during play. The microphone also enables voice commands for control of the console, game, or app, or to enter search terms.
- The Kinect sensor can also be used for audio and video communications through services such as Skype.

Learn more about Kinect at [Xbox Kinect and Privacy](#).

Microsoft Store

Microsoft Store is an online service, accessible via PC, the Xbox Console and the Xbox App, that allows you to browse, download, purchase, rate, and review applications and other digital content. It includes:

- ◆ Apps and content for Windows devices such as phones, PCs, and tablets.
- ◆ Games, subscriptions and other apps for Xbox consoles and other devices.
- ◆ Products and apps for Microsoft 365, SharePoint, Exchange, Access, and Project (2013 versions or later).

We collect data about how you access and use Microsoft Store; the products you've viewed, purchased, or installed; the preferences you set for viewing apps in Microsoft Store; and any ratings, reviews, or problem reports you submit. Your Microsoft account is associated with your ratings and reviews; and if you write a review, the name and picture from your Microsoft account will be published with your review.

Permission for Microsoft Store apps. Many apps you install from the Microsoft Store are designed to take advantage of specific hardware and software features of your device. An app's use of certain hardware and software features may give the app or its related service access to your data. For example, a photo editing app might access your device's camera to let you take a new photo or access photos or videos stored on your device for editing, and a restaurant guide might use your location to provide nearby recommendations. Information about the features that an app uses is provided on the app's product description page in Microsoft Store. Many of the features that Microsoft Store apps use can be turned on or off through your device's privacy settings. In Windows, in many cases, you can choose which apps can use a particular feature. Go to **Start > Settings > Privacy or Privacy & Security**, select the feature (for example, Calendar), and then select which app permissions are on or off. The lists of apps in Windows privacy settings that can use hardware and software features will not include "Classic Windows" applications, and these applications are not affected by these settings.

App updates. Unless you have turned off automatic app updates in the relevant Microsoft Store settings or have acquired an app provided and updated by the app developer, Microsoft Store will automatically check for, download, and install app updates to verify that you have the latest versions. Updated apps might use different Windows hardware and software features from the previous versions, which could give them access to different data on your device. You will be prompted for consent if an updated app accesses certain features, such as location. You can also review the hardware and software features an app uses by viewing its product description page in Microsoft Store.

Each app's use of your data collected through any of these features is subject to the app developer's privacy policies. If an app available through Microsoft Store collects and uses any of your personal data, the app developer is required to provide a privacy policy, and a link to the privacy policy is available on the app's product description page in Microsoft Store.

Sideloaded apps and developer mode. Developer features such as the "developer mode" setting are intended for development use only. If you enable developer features, your device may become unreliable or unusable, and expose you to security risks. Downloading or otherwise acquiring apps from sources other than Microsoft Store, also known as "sideloading" apps, may make your device and personal data more vulnerable to attack or unexpected use by apps. Windows policies, notifications, permissions, and other features intended to help protect your privacy when apps access your data may not function as described in this statement for sideloaded apps or when developer features are enabled.

MSN

MSN services include websites and a suite of apps, including MSN News, Weather, Sports, and Money, and previous versions of the apps branded as Bing (together, "MSN Apps"). The MSN Apps are available on various platforms, including Windows, iOS, and Android. MSN services are also included within other Microsoft services, including the Microsoft Edge browser.

When you install MSN Apps, we collect data that tells us if the app was installed properly, the installation date, the app version, and other data about your device such as the operating system and browser. This data is collected on a regular basis to help us determine the number of MSN App users and identify performance issues associated with different app versions, operating systems, and browsers.

We also collect data about how you interact with MSN services, such as usage frequency and articles viewed, to provide you with relevant content. Some MSN services provide an enhanced experience when you sign in with your Microsoft account, including allowing you to customize your interests and favorites. You can manage personalization through MSN and Bing settings, as well as through settings in other Microsoft services that include MSN services. We also use the data we collect to provide you with advertisements that may be of interest to you. You can opt out of interest-based advertising through the advertising links within MSN services, or by visiting the Microsoft [opt-out page](#).

Previous versions of MSN Money allow you to access personal finance information from third-party financial institutions. MSN Money only displays this information and does not store it on our servers. Your sign-in credentials used to access your financial information from third parties are encrypted on your device and are not sent to Microsoft. These financial institutions, as well as any other third-party services you access through MSN services, are subject to their own terms and privacy policies.

Groove Music and Movies & TV

Groove Music lets you easily play your music collection and make playlists. Microsoft Movies & TV allows you to play your video collection and rent or buy movies and TV episodes. These services were formerly offered as Xbox Music and Video.

To help you discover content that may interest you, Microsoft will collect data about what content you play, the length of play, and the rating you give it.

To enrich your experience when playing content, Groove Music and Movies & TV will display related information about the content you play and the content in your music and video libraries, such as the album title, cover art, song or video title, and other information, where available. To provide this information, Groove Music and Movies & TV send an information request to Microsoft containing standard device data, such as your device IP address, device software version, your regional and language settings, and an identifier for the content.

If you use Movies & TV to access content that has been protected with Microsoft Digital Rights Management (DRM), it may automatically request media usage rights from an online rights server and download and install DRM updates in order to let you play the content. See the DRM information in the [Silverlight](#) section of this privacy statement for more information.

Silverlight

Microsoft Silverlight helps you to access and enjoy rich content on the Web. Silverlight enables websites and services to store data on your device. Other Silverlight features involve connecting to Microsoft to obtain updates, or to Microsoft or third-party servers to play protected digital content.

Silverlight Configuration tool. You can make choices about these features in the Silverlight Configuration tool. To access the Silverlight Configuration tool, right click on content that is currently being displayed by Silverlight and select **Silverlight**. You can also run the Silverlight Configuration tool directly. In Windows, for example, you can access the tool by searching for "Microsoft Silverlight."

Silverlight application storage. Silverlight-based applications can store data files locally on your computer for a variety of purposes, including saving your custom settings, storing large files for graphically intensive features (such as games, maps, and images), and storing content

that you create within certain applications. You can turn off or configure application storage in the Silverlight Configuration tool.

Silverlight updates. Silverlight will periodically check a Microsoft server for updates to provide you with the latest features and improvements. A small file containing information about the latest Silverlight version will be downloaded to your computer and compared to your currently installed version. If a newer version is available, it will be downloaded and installed on your computer. You can turn off or configure updates in the Silverlight Configuration tool.

Digital Rights Management. Silverlight uses Microsoft Digital Rights Management (DRM) technology to help protect the rights of content owners. If you access DRM-protected content (such as music or video) with Silverlight, it will request media usage rights from a rights server on the Internet. In order to provide a seamless playback experience, you will not be prompted before Silverlight sends the request to the rights server. When requesting media usage rights, Silverlight will provide the rights server with an ID for the DRM-protected content file and basic data about your device, including data about the DRM components on your device such as their revision and security levels, and a unique identifier for your device.

DRM updates. In some cases, accessing DRM-protected content will require an update to Silverlight or to the DRM components on your device. When you attempt to play content that requires a DRM update, Silverlight will send a request to a Microsoft server containing basic data about your device, including information about the DRM components on your computer such as their revision and security levels, troubleshooting data, and a unique identifier for your device. The Microsoft server uses this identifier to return a unique DRM update for your device, which will then be installed by Silverlight. You can turn off or configure DRM component updates on the **Playback** tab in the Silverlight Configuration tool.

Windows Mixed Reality

Windows Mixed Reality allows you to enable a virtual reality experience that immerses you in apps and games. Mixed Reality uses a compatible headset's camera, microphone, and infrared sensors to enable motions and voice to be used to control gameplay and to navigate apps and games.

Microsoft collects diagnostic data to solve problems and to keep Mixed Reality running on Windows up to date, secure, and operating properly. Diagnostic data also helps us improve Mixed Reality and related Microsoft products and services depending on the diagnostic data settings you've chosen for your device. [Learn more about Windows diagnostic data.](#)

Mixed Reality also processes and collects data specifically related to the Mixed Reality experiences, such as:

- ♦ Mixed Reality maps distances between your body's joints to create a stick figure representation of you. If you are connected to the Internet, we collect those numeric values to enable and improve your experience.

- ♦ Mixed Reality detects specific hand gestures intended to perform simple system interactions (such as menu navigation, pan/zoom, and scroll). This data is processed on your PC and is not stored.
- ♦ The headset's microphones enable voice commands to control games, apps, or to enter search terms. [Learn more about voice data collection.](#)
- ♦ Windows Mixed Reality can also be used for audio and video communications through services such as Skype.

Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products for a variety of purposes described below, including to operate effectively and provide you with the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, administer your organization's licensing account, submit a search query to Bing, register for a Microsoft event, speak a voice command to Cortana, upload a document to OneDrive, sign up for Microsoft 365, or contact us for support. We get some of it by collecting data about your interactions, use, and experience with our products and communications.

We rely on a variety of legal reasons and permissions (sometimes called "legal bases") to process data, including with your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with legal obligations, for a variety of purposes described below.

We also obtain data from third parties. We protect data obtained from third parties according to the practices described in this statement, plus any additional restrictions imposed by the source of the data. These third-party sources vary over time and include:

- ♦ Data brokers from which we purchase demographic data to supplement the data we collect.
- ♦ Services that make user-generated content from their service available to others, such as local business reviews or public social media posts.
- ♦ Communication services, including email providers and social networks, when you give us permission to access your data on such third-party services or networks.
- ♦ Service providers that help us determine your device's location.
- ♦ Partners with which we offer co-branded services or engage in joint marketing activities.
- ♦ Developers who create experiences through or for Microsoft products.
- ♦ Third parties that deliver experiences through Microsoft products. Publicly-available sources, such as open public sector, academic, and commercial data sets and other data sources.

If you represent an organization, such as a business or school, that utilizes Enterprise and Developer Products from Microsoft, please see the [Enterprise and developer products](#) section of this privacy statement to learn how we process your data. If you are an end user of a Microsoft product or a Microsoft account provided by your organization, please see the [Products provided by your organization](#) and the [Microsoft account](#) sections for more information.

You have choices when it comes to the technology you use and the data you share. When you are asked to provide personal data, you can decline. Many of our products require some personal data to operate and provide you with a service. If you choose not to provide data required to operate and

provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you're using, we may have to suspend or cancel it. We will notify you if this is the case at the time. Where providing the data is optional, and you choose not to share personal data, features like personalization that use the data will not work for you.

The data we collect depends on the context of your interactions with Microsoft and the choices you make (including your privacy settings), the products and features you use, your location, and applicable law.

The data we collect can include the following:

Name and contact data. Your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. Passwords, password hints, and similar security information used for authentication and account access.

Demographic data. Data about you such as your age, gender, country, and preferred language.

Payment data. Data to process payments, such as your payment instrument number (such as a credit card number) and the security code associated with your payment instrument.

Subscription and licensing data. Information about your subscriptions, licenses, and other entitlements.

Interactions. Data about your use of Microsoft products. In some cases, such as search queries, this is data you provide in order to make use of the products. In other cases, such as error reports, this is data we generate. Other examples of interactions data include:

- ◆ **Device and usage data.** Data about your device and the product and features you use, including information about your hardware and software, how our products perform, as well as your settings. For example:
 - **Payment and account history.** Data about the items you purchase and activities associated with your account.
 - **Browse history.** Data about the webpages you visit.
 - **Device, connectivity, and configuration data.** Data about your device, your device configuration, and nearby networks. For example, data about the operating systems and other software installed on your device, including product keys. In addition, IP address, device identifiers (such as the IMEI number for phones), regional and language settings, and information about WLAN access points near your device.
 - **Error reports and performance data.** Data about the performance of the products and any problems you experience, including error reports. Error reports (sometimes called "crash dumps") can include details of the software or hardware related to an error, contents of files opened when an error occurred, and data about other software on your device.
 - **Troubleshooting and help data.** Data you provide when you contact Microsoft for help, such as the products you use, and other details that help us provide support. For example,

contact or authentication data, the content of your chats and other communications with Microsoft, data about the condition of your device, and the products you use related to your help inquiry. When you contact us, such as for customer support, phone conversations or chat sessions with our representatives may be monitored and recorded.

- **Bot usage data.** Interactions with third party bots and skills available through Microsoft products.
- ◆ **Interests and favorites.** Data about your interests and favorites, such as the sports teams you follow, the programming languages you prefer, the stocks you track, or cities you add to track things like weather or traffic. In addition to those you explicitly provide, your interests and favorites can also be inferred or derived from other data we collect.
- ◆ **Content consumption data.** Information about media content (e.g., TV, video, music, audio, text books, apps, and games) you access through our products.
- ◆ **Searches and commands.** Search queries and commands when you use Microsoft products with search or related productivity functionality.
- ◆ **Voice data.** Your voice data, sometimes referred to as “voice clips”, such as search queries, commands, or dictation you speak, which may include background sounds.
- ◆ **Text, inking, and typing data.** Text, inking, and typing data and related information. For example, when we collect inking data, we collect information about the placement of your inking instrument on your device.
- ◆ **Images.** Images and related information, such as picture metadata. For example, we collect the image you provide when you use a Bing image-enabled service.
- ◆ **Contacts and relationships.** Data about your contacts and relationships if you use a product to share information with others, manage contacts, communicate with others, or improve your productivity.
- ◆ **Social data.** Information about your relationships and interactions between you, other people, and organizations, such as types of engagement (e.g., likes, dislikes, events, etc.) related to people and organizations.
- ◆ **Location data.** Data about your device’s location, which can be either precise or imprecise. For example, we collect location data using Global Navigation Satellite System (GNSS) (e.g., GPS) and data about nearby cell towers and Wi-Fi hotspots. Location can also be inferred from a device’s IP address or data in your account profile that indicates where it is located with less precision, such as at a city or postal code level.
- ◆ **Other input.** Other inputs provided when you use our products. For example, data such as the buttons you press on an Xbox wireless controller using the Xbox network, skeletal tracking data when you use Kinect, and other sensor data, like the number of steps you take, when you use devices that have applicable sensors. And, if you use Spend, at your direction, we also collect financial transaction data from your credit card issuer to provide the service. If you attend an in-store event, we collect the data you provide to us when registering for or during the event and if you enter into a prize promotion, we collect the data you input into the entry form.

Content. Content of your files and communications you input, upload, receive, create, and control. For example, if you transmit a file using Skype to another Skype user, we need to collect the content of that file to display it to you and the other user. If you receive an email using Outlook.com, we need to collect the content of that email to deliver it to your inbox, display it to you, enable you to reply to it, and store it for you until you choose to delete it. Other content we collect when providing products to you include:

- Communications, including audio, video, text (typed, inked, dictated, or otherwise), in a message, email, call, meeting request, or chat.
- Photos, images, songs, movies, software, and other media or documents you store, retrieve, or otherwise process with our cloud.

Video or recordings. Recordings of events and activities at Microsoft buildings, retail spaces, and other locations. If you enter Microsoft Store locations or other facilities, or attend a Microsoft event that is recorded, we may process your image and voice data.

Feedback and ratings. Information you provide to us and the content of messages you send to us, such as feedback, survey data, and product reviews you write.

Traffic data. Data generated through your use of Microsoft's communications services. Traffic data indicates with whom you have communicated and when your communications occurred. We will process your traffic data only as required to provide, maintain, and improve our communications services and we do so with your consent.

Product-specific sections below describe data collection practices applicable to use of those products.

How we use personal data

Microsoft uses the data we collect to provide you rich, interactive experiences. In particular, we use data to:

- Provide our products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions you request.
- Improve and develop our products.
- Personalize our products and make recommendations.
- Advertise and market to you, which includes sending promotional communications, targeting advertising, and presenting you relevant offers.

We also use the data to operate our business, which includes analyzing our performance, meeting our legal obligations, developing our workforce, and doing research.

For these purposes, we combine data we collect from different contexts (for example, from your use of two Microsoft products). For example, Cortana may use information from your calendar to suggest action items in a heads-up email, and Microsoft Store uses information about the apps and services you use to make personalized app recommendations. However, we have built in technological and procedural safeguards designed to prevent certain data combinations where required by law. For example, where required by law, we store data we collect from you when you are unauthenticated (not signed in) separately from any account information that directly identifies you, such as your name, email address, or phone number.

Our processing of personal data for these purposes includes both automated and manual (human) methods of processing. Our automated methods often are related to and supported by our manual methods. For example, our automated methods include artificial intelligence (AI), which we think of as

a set of technologies that enable computers to perceive, learn, reason, and assist in decision-making to solve problems in ways that are similar to what people do. To build, train, and improve the accuracy of our automated methods of processing (including AI), we manually review some of the predictions and inferences produced by the automated methods against the underlying data from which the predictions and inferences were made. For example, we manually review short snippets of voice data that we have taken steps to de-identify to improve our speech recognition technologies. This manual review may be conducted by Microsoft employees or vendors who are working on Microsoft's behalf.

When we process personal data about you, we do so with your consent and/or as required to provide the products you use, operate our business, meet our contractual and legal obligations, protect the security of our systems and our customers, or fulfill other legitimate interests of Microsoft as described in this section and in the [Reasons we share personal data](#) section of this privacy statement. When we transfer personal data from the European Economic Area, we do so based on a variety of legal mechanisms, as described in the [Where we store and process personal data](#) section of this privacy statement.

More on the purposes of processing:

- ♦ **Provide our products.** We use data to operate our products and provide you with rich, interactive experiences. For example, if you use OneDrive, we process the documents you upload to OneDrive to enable you to retrieve, delete, edit, forward, or otherwise process it, at your direction as part of the service. Or, for example, if you enter a search query in the Bing search engine, we use that query to display search results to you. Additionally, as communications are a feature of various products, programs, and activities, we use data to contact you. For example, we may contact you by phone or email or other means to inform you when a subscription is ending or discuss your licensing account. We also communicate with you to secure our products, for example by letting you know when product updates are available.
- ♦ **Product improvement.** We use data to continually improve our products, including adding new features or capabilities. For example, we use error reports to improve security features, search queries and clicks in Bing to improve the relevancy of the search results, usage data to determine what new features to prioritize, and voice data to develop and improve speech recognition accuracy.
- ♦ **Personalization.** Many products include personalized features, such as recommendations that enhance your productivity and enjoyment. These features use automated processes to tailor your product experiences based on the data we have about you, such as inferences we make about you and your use of the product, activities, interests, and location. For example, depending on your settings, if you stream movies in a browser on your Windows device, you may see a recommendation for an app from the Microsoft Store that streams more efficiently. If you have a Microsoft account, with your permission, we can sync your settings on several devices. Many of our products provide controls to disable personalized features.
- ♦ **Product activation.** We use data—such as device and application type, location, and unique device, application, network, and subscription identifiers—to activate products that require activation.
- ♦ **Product development.** We use data to develop new products. For example, we use data, often de-identified, to better understand our customers' computing and productivity needs which can shape the development of new products.

- ♦ **Customer support.** We use data to troubleshoot and diagnose product problems, repair customers' devices, and provide other customer care and support services, including to help us provide, improve, and secure the quality of our products, services, and training, and to investigate security incidents. Call recording data may also be used to authenticate or identify you based on your voice to enable Microsoft to provide support services and investigate security incidents.
- ♦ **Help secure and troubleshoot.** We use data to help secure and troubleshoot our products. This includes using data to protect the security and safety of our products and customers, detecting malware and malicious activities, troubleshooting performance and compatibility issues to help customers get the most out of their experiences, and notifying customers of updates to our products. This may include using automated systems to detect security and safety issues.
- ♦ **Safety.** We use data to protect the safety of our products and our customers. Our security features and products can disrupt the operation of malicious software and notify users if malicious software is found on their devices. For example, some of our products, such as Outlook.com or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, abusive actions, or URLs that have been flagged as fraud, phishing, or malware links; and we reserve the right to block delivery of a communication or remove content if it violates our terms. **In accordance with European Union Regulation (EU) 2021/1232, we have invoked the derogation permitted by that Regulation from Articles 5(1) and 6(1) of EU Directive 2002/58/EC. We use scanning technologies to create digital signatures (known as "hashes") of certain images and video content on our systems. These technologies then compare the hashes they generate with hashes of reported child sexual exploitation and abuse imagery (known as a "hash set"), in a process called "hash matching". Microsoft obtains hash sets from organizations that act in the public interest against child sex abuse. This can result in sharing information with the National Center for Missing and Exploited Children (NCMEC) and law enforcement authorities.**
- ♦ **Updates.** We use data we collect to develop product updates and security patches. For example, we may use information about your device's capabilities, such as available memory, to provide you a software update or security patch. Updates and patches are intended to maximize your experience with our products, help you protect the privacy and security of your data, provide new features, and evaluate whether your device is ready to process such updates.
- ♦ **Promotional communications.** We use data we collect to deliver promotional communications. You can sign up for email subscriptions and choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. For information about managing your contact data, email subscriptions, and promotional communications, see the [How to access and control your personal data](#) section of this privacy statement.
- ♦ **Relevant offers.** Microsoft uses data to provide you with relevant and valuable information regarding our products. We analyze data from a variety of sources to predict the information that will be most interesting and relevant to you and deliver such information to you in a variety of ways. For example, we may predict your interest in gaming and communicate with you about new games you may like.
- ♦ **Advertising.** Microsoft does not use what you say in email, chat, video calls, or voice mail, or your documents, photos, or other personal files to target ads to you. We use data we collect through our interactions with you, through some of our products, and on third-party web properties, for advertising in our products and on third-party properties. We may use automated

processes to help make advertising more relevant to you. For more information about how your data is used for advertising, see the [Advertising](#) section of this privacy statement.

- ♦ **Prize promotions and events.** We use your data to administer prize promotions and events available in our physical Microsoft Stores. For example, if you enter into a prize promotion, we may use your data to select a winner and provide the prize to you if you win. Or, if you register for a coding workshop or gaming event, we will add your name to the list of expected attendees.
- ♦ **Transacting commerce.** We use data to carry out your transactions with us. For example, we process payment information to provide customers with product subscriptions and use contact information to deliver goods purchased from the Microsoft Store.
- ♦ **Reporting and business operations.** We use data to analyze our operations and perform business intelligence. This enables us to make informed decisions and report on the performance of our business.
- ♦ **Protecting rights and property.** We use data to detect and prevent fraud, resolve disputes, enforce agreements, and protect our property. For example, we use data to confirm the validity of software licenses to reduce piracy. We may use automated processes to detect and prevent activities that violate our rights and the rights of others, such as fraud.
- ♦ **Legal compliance.** We process data to comply with law. For example, we use the age of our customers to assist us in meeting our obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.
- ♦ **Research.** With appropriate technical and organizational measures to safeguard individuals' rights and freedoms, we use data to conduct research, including for public interest and scientific purposes.

Reasons we share personal data

We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorized. For example, we share your content with third parties when you tell us to do so, such as when you send an email to a friend, share photos and documents on OneDrive, or link accounts with another service. If you use a Microsoft product provided by an organization you are affiliated with, such as an employer or school, or use an email address provided by such organization to access Microsoft products, we share certain data, such as interaction data and diagnostic data to enable your organization to manage the products. When you provide payment data to make a purchase, we will share payment data with banks and other entities that process payment transactions or provide other financial services, and for fraud prevention and credit risk reduction.

In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction such as a merger or sale of assets.

Finally, we will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following:

- Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.
- Protect our customers, for example, to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone.
- Operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks.
- Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services—however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement.

For more information about data we disclose in response to requests from law enforcement and other government agencies, please see our [Law Enforcement Requests Report](#).

Please note that some of our products include links to or otherwise enable you to access products of third parties whose privacy practices differ from those of Microsoft. If you provide personal data to any of those products, your data is governed by their privacy policies.

How to access and control your personal data

You can also make choices about the collection and use of your data by Microsoft. You can control your personal data that Microsoft has obtained, and exercise your data protection rights, by contacting Microsoft or using various tools we provide. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law. How you can access or control your personal data will also depend on which products you use. For example, you can:

- Control the use of your data for interest-based advertising from Microsoft by visiting our [opt-out page](#).
- Choose whether you wish to receive promotional emails, SMS messages, telephone calls, and postal mail from Microsoft.
- Access and clear some of your data through the [Microsoft privacy dashboard](#).

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the [How to contact us](#) section or by using our [web form](#).

We provide aggregate metrics about user requests to exercise their data protection rights via the [Microsoft Privacy Report](#).

You can access and control your personal data that Microsoft has obtained with tools Microsoft provides to you, which are described below, or by contacting Microsoft. For instance:

- If Microsoft obtained your consent to use your personal data, you can withdraw that consent at any time.
- You can request access to, erasure of, and updates to your personal data.

- ♦ If you'd like to port your data elsewhere, you can use tools Microsoft provides to do so, or if none are available, you can contact Microsoft for assistance.

You can also object to or restrict the use of your personal data by Microsoft. For example, you can object at any time to our use of your personal data:

- ♦ For direct marketing purposes.
- ♦ Where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party.

You may have these rights under applicable laws, including the EU General Data Protection Regulation (GDPR), but we offer them regardless of your location. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law.

If your organization, such as your employer, school, or service provider, provides you with access to and is administering your use of Microsoft products, contact your organization to learn more about how to access and control your personal data.

You can access and control your personal data that Microsoft has obtained, and exercise your data protection rights, using various tools we provide. The tools most useful to you will depend on our interactions with you and your use of our products. Here is a general list of tools we provide to help you control your personal data; specific products may provide additional controls.

- ♦ **Bing.** If you are signed into Bing, you can view and clear your search history on your [privacy dashboard](#). If you are not signed into Bing, you can view and clear search history associated to your device in your [Bing settings](#).
- ♦ **Cortana.** You can control some of the data Cortana accesses or stores in your [Cortana settings](#).
- ♦ **Microsoft account.** If you wish to access, edit, or remove the profile information and payment information in your Microsoft account, change your password, add security information or close your account, you can do so by visiting the [Microsoft account website](#).
- ♦ If you have a **Microsoft Developer Network** (MSDN) public profile, you can access and edit your data by signing in at [MSDN forum](#).
- ♦ **Microsoft privacy dashboard.** You can control some of the data Microsoft processes through your use of a Microsoft account on the [Microsoft privacy dashboard](#). From here, for example, you can view and clear the browsing, search, and location data associated with your Microsoft account.
- ♦ **Microsoft Store.** You can access your Microsoft Store profile and account information by visiting [Microsoft Store](#) and selecting **View account** or **Order history**.
- ♦ **Microsoft Teams for personal use.** You can find out how to export or delete Teams data relating to your personal Microsoft account by visiting this [page](#).
- ♦ **OneDrive.** You can view, download, and delete your files and photos in OneDrive by signing into your [OneDrive](#).
- ♦ **Outlook.com.** You can download your emails in [Outlook.com](#) by signing into your account and navigating to your **Privacy and data** settings.
- ♦ **Skype.** If you wish to access, edit, or remove some profile and payment information for Skype or change your password, [sign in to your account](#). If you wish to export your Skype chat history and files shared on Skype, you can [request a copy](#).

- ♦ **Volume Licensing Service Center (VLSC).** If you are a Volume Licensing customer, you can control your contact information and subscription and licensing data in one location by visiting the [Volume Licensing Service Center website](#).
- ♦ **Xbox.** If you use the Xbox network or Xbox.com, you can view or edit your personal data, including billing and account information, privacy settings, and online safety and data sharing preferences by accessing [My Xbox](#) on the Xbox console or on the Xbox.com website.

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the [How to contact us](#) section or by using our [web form](#). We will respond to requests to control your personal data as required by applicable law.

Your communications preferences

You can choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. If you receive promotional email or SMS messages from us and would like to opt out, you can do so by following the directions in that message. You can also make choices about the receipt of promotional email, telephone calls, and postal mail by signing in with your personal Microsoft account, and viewing your [communication permissions](#) where you can update contact information, manage Microsoft-wide contact preferences, opt out of email subscriptions, and choose whether to share your contact information with Microsoft partners. If you do not have a personal Microsoft account, you can manage your Microsoft email contact preferences by using this [web form](#). These choices do not apply to mandatory service communications that are part of certain Microsoft products, programs, activities, or to surveys or other informational communications that have their own unsubscribe method.

Your advertising choices

To opt out of receiving interest-based advertising from Microsoft, visit our [opt-out page](#). When you opt out, your preference is stored in a cookie that is specific to the web browser you are using. The opt-out cookie has an expiration date of five years. If you delete the cookies on your device, you need to opt out again.

You can also link your opt-out choice with your personal Microsoft account. It will then apply on any device where you use that account and will continue to apply until someone signs in with a different personal Microsoft account on that device. If you delete the cookies on your device, you will need to sign in again for the settings to apply.

For Microsoft-controlled advertising that appears in apps on Windows, you may use the opt-out linked to your personal Microsoft account, or opt out of interest-based advertising by turning off the advertising ID in Windows settings.

Because the data used for interest-based advertising is also used for other required purposes (including providing our products, analytics, and fraud detection), opting out of interest-based advertising does not stop that data collection. You will continue to get ads, although they may be less relevant to you.

You can opt out of receiving interest-based advertising from third parties we partner with by visiting their sites (see above).

Browser-based controls

When you use a browser, you can control your personal data using certain features. For example:

- ♦ **Cookie controls.** You can control the data stored by cookies and withdraw consent to cookies by using the browser-based cookie controls described in the [Cookies](#) section of this privacy statement.
- ♦ **Tracking protections.** You can control the data third-party sites can collect about you using Tracking Protection in Internet Explorer (versions 9 and up) and Microsoft Edge. This feature will block third-party content, including cookies, from any site that is listed in a Tracking Protection List you add.
- ♦ **Browser controls for "Do Not Track."** Some browsers have incorporated "Do Not Track" (DNT) features that can send a signal to the websites you visit indicating you do not wish to be tracked. Because there is not yet a common understanding of how to interpret the DNT signal, Microsoft services do not currently respond to browser DNT signals. We continue to work with the online industry to define a common understanding of how to treat DNT signals. In the meantime, you can use the range of other tools we provide to control data collection and use, including the ability to opt out of receiving interest-based advertising from Microsoft as described above.

Cookies and similar technologies

Cookies are small text files placed on your device to store data that can be recalled by a web server in the domain that placed the cookie. This data often consists of a string of numbers and letters that uniquely identifies your computer, but it can contain other information as well. Some cookies are placed by third parties acting on our behalf. We use cookies and similar technologies to store and honor your preferences and settings, enable you to sign-in, provide interest-based advertising, combat fraud, analyze how our products perform, and fulfill other legitimate purposes described below. Microsoft apps use additional identifiers, such as the advertising ID in Windows, for similar purposes, and many of our websites and applications also contain web beacons or other similar technologies, as described below.

Our use of cookies and similar technologies

Microsoft uses cookies and similar technologies for several purposes, depending on the context or product, including:

- ♦ **Storing your preferences and settings.** We use cookies to store your preferences and settings on your device, and to enhance your experiences. For example, depending on your settings, if you enter your city or postal code to get local news or weather information on a Microsoft website, we store that data in a cookie so that you will see the relevant local information when you return to the site. Saving your preferences with cookies, such as your preferred language, prevents you from having to set your preferences repeatedly. If you opt out of interest-based

advertising, we store your opt-out preference in a cookie on your device. Similarly, in scenarios where we obtain your consent to place cookies on your device, we store your choice in a cookie.

- ♦ **Sign-in and authentication.** We use cookies to authenticate you. When you sign in to a website using your personal Microsoft account, we store a unique ID number, and the time you signed in, in an encrypted cookie on your device. This cookie allows you to move from page to page within the site without having to sign in again on each page. You can also save your sign-in information so you do not have to sign in each time you return to the site.
- ♦ **Security.** We use cookies to process information that helps us secure our products, as well as detect fraud and abuse.
- ♦ **Storing information you provide to a website.** We use cookies to remember information you shared. When you provide information to Microsoft, such as when you add products to a shopping cart on Microsoft websites, we store the data in a cookie for the purpose of remembering the information.
- ♦ **Social media.** Some of our websites include social media cookies, including those that enable users who are signed in to the social media service to share content via that service.
- ♦ **Feedback.** Microsoft uses cookies to enable you to provide feedback on a website.
- ♦ **Interest-based advertising.** Microsoft uses cookies to collect data about your online activity and identify your interests so that we can provide advertising that is most relevant to you. You can opt out of receiving interest-based advertising from Microsoft as described in the [How to access and control your personal data](#) section of this privacy statement.
- ♦ **Showing advertising.** Microsoft uses cookies to record how many visitors have clicked on an advertisement and to record which advertisements you have seen, for example, so you do not see the same one repeatedly.
- ♦ **Analytics.** We use first- and third-party cookies and other identifiers to gather usage and performance data. For example, we use cookies to count the number of unique visitors to a web page or service and to develop other statistics about the operations of our products.
- ♦ **Performance.** Microsoft uses cookies to understand and improve how our products perform. For example, we use cookies to gather data that helps with load balancing; this helps us keep our websites remain up and running.

Where required, we obtain your consent prior to placing or using optional cookies that are not (i) strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication. Please see the "How to Control Cookies" section below for more information.

Some of the cookies we commonly use are listed below. This list is not exhaustive, but it is intended to illustrate the primary purposes for which we typically set cookies. If you visit one of our websites, the site will set some or all of the following cookies:

- ♦ **MSCC.** Contains user choices for most Microsoft properties.
- ♦ **MUID, MC1, and MSFPC.** Identifies unique web browsers visiting Microsoft sites. These cookies are used for advertising, site analytics, and other operational purposes.
- ♦ **ANON.** Contains the ANID, a unique identifier derived from your Microsoft account, which is used for advertising, personalization, and operational purposes. It is also used to preserve your choice to opt out of interest-based advertising from Microsoft if you have chosen to associate the opt-out with your Microsoft account.
- ♦ **CC.** Contains a country code as determined from your IP address.

- **PPAuth, MSPAuth, MSNRPSAuth, KievRPSAuth, WLSSC, MSPPProf.** Helps to authenticate you when you sign in with your Microsoft account.
- **MC0.** Detects whether cookies are enabled in the browser.
- **MS0.** Identifies a specific session.
- **NAP.** Contains an encrypted version of your country, postal code, age, gender, language and occupation, if known, based on your Microsoft account profile.
- **MH.** Appears on co-branded sites where Microsoft is partnering with an advertiser. This cookie identifies the advertiser, so the right ad is selected.
- **childinfo, kcdob, kcrelid, kcru, pcfm.** Contains information that Microsoft account uses within its pages in relation to child accounts.
- **MR.** This cookie is used by Microsoft to reset or refresh the MUID cookie.
- **x-ms-gateway-slice.** Identifies a gateway for load balancing.
- **TOptOut.** Records your decision not to receive interest-based advertising delivered by Microsoft. Where required, we place this cookie by default and remove it when you consent to interest-based advertising.

In addition to the cookies Microsoft sets when you visit our websites, third parties can also set cookies when you visit Microsoft sites. For example:

- Companies we hire to provide services on our behalf, such as site analytics, place cookies when you visit our sites.
- Companies that deliver content, such as videos or news, or ads on Microsoft sites, place cookies on their own. These companies use the data they process in accordance with their privacy policies, which may enable these companies to collect and combine information about your activities across websites, apps, or online services.

For a list of the third parties that set cookies on our websites, including service providers acting on our behalf, please visit our [third party cookie inventory](#). On some of our websites, a list of third parties is available directly on the site. The third parties on these sites may not be included in the list on our [third party cookie inventory](#).

How to control cookies

Most web browsers automatically accept cookies but provide controls that allow you to block or delete them. For example, in Microsoft Edge, you can block or delete cookies by selecting **Settings** > **Privacy and services** > **Clear Browsing data** > **Cookies and other site data**. For more information about how to delete your cookies in Microsoft browsers, see [Microsoft Edge](#), [Microsoft Edge Legacy](#) or [Internet Explorer](#). If you use a different browser, refer to that browser's instructions.

As mentioned above, where required, we obtain your consent before placing or using optional cookies that are not (i) strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication. We separate these optional cookies by purpose, such as for advertising and social media purposes. You may consent to certain categories of optional cookies and not others. You also may adjust your choices by clicking "Manage cookies" in the footer of the website or through the settings made available on the website. Certain features of Microsoft products depend on cookies. If you choose to block cookies, you cannot sign in or use some of those features, and preferences that are dependent on cookies will be lost. If you choose to delete cookies, any settings and preferences

controlled by those cookies, including advertising preferences, are deleted and will need to be recreated.

Certain features of Microsoft products depend on cookies. If you choose to block cookies, you cannot sign in or use some of those features, and preferences that are dependent on cookies will be lost. If you choose to delete cookies, any settings and preferences controlled by those cookies, including advertising preferences, are deleted and will need to be recreated.

Additional privacy controls that can impact cookies, including the tracking protections feature of Microsoft browsers, are described in the [How to access and control your personal data](#) section of this privacy statement.

Our use of web beacons and analytics services

Some Microsoft webpages contain electronic tags known as web beacons that we use to help deliver cookies on our websites, count users who have visited those websites, and deliver co-branded products. We also include web beacons or similar technologies in our electronic communications to determine whether you open and act on them.

In addition to placing web beacons on our own websites, we sometimes work with other companies to place our web beacons on their websites or in their advertisements. This helps us to, for example, develop statistics on how often clicking on an advertisement on a Microsoft website results in a purchase or other action on the advertiser's website. It also allows us to understand your activity on the website of a Microsoft partner in connection with your use of a Microsoft product or service.

Finally, Microsoft products often contain web beacons or similar technologies from third-party analytics providers, which help us compile aggregated statistics about the effectiveness of our promotional campaigns or other operations. These technologies enable the analytics providers to set or read their own cookies or other identifiers on your device, through which they can collect information about your online activities across applications, websites, or other products. However, we prohibit these analytics providers from using web beacons on our sites to collect or access information that directly identifies you (such as your name or email address). You can opt out of data collection or use by some of these analytics providers by visiting any of the following sites: [Adjust](#), [AppsFlyer](#), [Clicktale](#), [Flurry Analytics](#), [Google Analytics](#) (requires you to install a browser add-on), [Kissmetrics](#), [Mixpanel](#), [Nielsen](#), [Acuity Ads](#), [WebTrends](#) or [Optimizely](#).

Other similar technologies

In addition to standard cookies and web beacons, our products can also use other similar technologies to store and read data files on your computer. This is typically done to maintain your preferences or to improve speed and performance by storing certain files locally. But, like standard cookies, these technologies can also store a unique identifier for your computer, which can then track behavior. These technologies include Local Shared Objects (or "Flash cookies") and Silverlight Application Storage.

Local Shared Objects or "Flash cookies." Websites that use Adobe Flash technologies can use Local Shared Objects or "Flash cookies" to store data on your computer. To learn how to manage or block Flash cookies, go to the [Flash Player help page](#).

Silverlight Application Storage. Websites or applications that use Microsoft Silverlight technology also have the ability to store data by using Silverlight Application Storage. To learn how to manage or block such storage, see the [Silverlight](#) section of this privacy statement.

Products provided by your organization—notice to end users

If you use a Microsoft product with an account provided by an organization you are affiliated with, such as your work or school account, that organization can:

- ♦ Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.
- ♦ Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

If you lose access to your work or school account (in event of change of employment, for example), you may lose access to products and the content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such products.

Many Microsoft products are intended for use by organizations, such as schools and businesses. Please see the [Enterprise and developer products](#) section of this privacy statement. If your organization provides you with access to Microsoft products, your use of the Microsoft products is subject to your organization's policies, if any. You should direct your privacy inquiries, including any requests to exercise your data protection rights, to your organization's administrator. When you use social features in Microsoft products, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation or help content specific to the Microsoft product. Microsoft is not responsible for the privacy or security practices of our customers, which may differ from those set forth in this privacy statement.

When you use a Microsoft product provided by your organization, Microsoft's processing of your personal data in connection with that product is governed by a contract between Microsoft and your organization. Microsoft processes your personal data to provide the product to your organization and you, and in some cases for Microsoft's business operations related to providing the product as described in the [Enterprise and developer products](#) section. As mentioned above, if you have questions about Microsoft's processing of your personal data in connection with providing products to your organization, please contact your organization. If you have questions about Microsoft's business operations in connection with providing products to your organization as provided in the Product Terms, please contact Microsoft as described in the [How to contact us](#) section. For more information on our business operations, please see the [Enterprise and developer products](#) section.

For Microsoft products provided by your K-12 school, including Microsoft 365 Education, Microsoft will:

- ♦ not collect or use student personal data beyond that needed for authorized educational or school purposes;
- ♦ not sell or rent student personal data;

- not use or share student personal data for advertising or similar commercial purposes, such as behavioral targeting of advertisements to students;
- not build a personal profile of a student, other than for supporting authorized educational or school purposes or as authorized by the parent, guardian, or student of appropriate age; and
- require that our vendors with whom student personal data is shared to deliver the educational service, if any, are obligated to implement these same commitments for student personal data.

Microsoft account

With a Microsoft account, you can sign into Microsoft products, as well as those of select Microsoft partners. Personal data associated with your Microsoft account includes credentials, name and contact data, payment data, device and usage data, your contacts, information about your activities, and your interests and favorites. Signing into your Microsoft account enables personalization, consistent experiences across products and devices, permits you to use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account, and enables other features. There are three types of Microsoft account:

- When you create your own Microsoft account tied to your personal email address, we refer to that account as a **personal Microsoft account**.
- When you or your organization (such as an employer or your school) create your Microsoft account tied to your email address provided by that organization, we refer to that account as a **work or school account**.
- When you or your service provider (such as a cable or internet service provider) create your Microsoft account tied to your email address with your service provider's domain, we refer to that account as a **third-party account**.

Personal Microsoft accounts. The data associated with your personal Microsoft account, and how that data is used, depends on how you use the account.

- **Creating your Microsoft account.** When you create a personal Microsoft account, you will be asked to provide certain personal data and we will assign a unique ID number to identify your account and associated information. While some products, such as those involving payment, require a real name, you can sign in to and use other Microsoft products without providing your real name. Some data you provide, such as your display name, email address, and phone number, can be used to help others find and connect with you within Microsoft products. For example, people who know your display name, email address, or phone number can use it to search for you on Skype or Microsoft Teams for personal use and send you an invite to connect with them. Note that if you use a work or school email address to create a personal Microsoft account, your employer or school may gain access to your data. In some cases, you will need to change the email address to a personal email address in order to continue accessing consumer-oriented products (such as the Xbox network).
- **Signing in to Microsoft account.** When you sign in to your Microsoft account, we create a record of your sign-in, which includes the date and time, information about the product you signed in to, your sign-in name, the unique number assigned to your account, a unique identifier assigned to your device, your IP address, and your operating system and browser version.

- ♦ **Signing in to Microsoft products.** Signing in to your account enables improved personalization, provides seamless and consistent experiences across products and devices, permits you to access and use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account, and enables other enhanced features and settings. When you sign in to your account, you will stay signed in until you sign out. If you add your Microsoft account to a Windows device (version 8 or higher), Windows will automatically sign you in to products that use Microsoft account when you access those products on that device. When you are signed in, some products will display your name or username and your profile photo (if you have added one to your profile) as part of your use of Microsoft products, including in your communications, social interactions, and public posts.
- ♦ **Signing in to third-party products.** If you sign in to a third-party product with your Microsoft account, you will share data with the third party in accordance with the third party's privacy policy. The third party will also receive the version number assigned to your account (a new version number is assigned each time you change your sign-in data); and information that describes whether your account has been deactivated. If you share your profile data, the third party can display your name or user name and your profile photo (if you have added one to your profile) when you are signed in to that third-party product. If you chose to make payments to third-party merchants using your Microsoft account, Microsoft will pass information stored in your Microsoft account to the third party or its vendors (e.g., payment processors) as necessary to process your payment and fulfill your order (such as name, credit card number, billing and shipping addresses, and relevant contact information). The third party can use or share the data it receives when you sign in or make a purchase according to its own practices and policies. **You should carefully review the privacy statement for each product you sign in to and each merchant you purchase from to determine how it will use the data it collects.**

Work or school accounts. The data associated with a work or school account, and how it will be used, is generally similar to the use and collection of data associated with a personal Microsoft account.

If your employer or school uses Azure Active Directory (AAD) to manage the account it provides you, you can use your work or school account to sign in to Microsoft products, such as Microsoft 365 and Office 365, and third-party products provided to you by your organization. If required by your organization, you will also be asked to provide a phone number or an alternative email address for additional security verification. And, if allowed by your organization, you may also use your work or school account to sign in to Microsoft or third-party products that you acquire for yourself.

If you sign in to Microsoft products with a work or school account, note:

- ♦ The owner of the domain associated with your email address may control and administer your account, and access and process your data, including the contents of your communications and files, including data stored in products provided to you by your organization, and products you acquire by yourself.
- ♦ Your use of the products is subject to your organization's policies, if any. You should consider both your organization's policies and whether you are comfortable enabling your organization to access your data before you choose to use your work or school account to sign in to products you acquire for yourself.
- ♦ If you lose access to your work or school account (if you change employers, for example), you may lose access to products, including content associated with those products, you acquired on

your own behalf if you used your work or school account to sign in to such products.

- ♦ Microsoft is not responsible for the privacy or security practices of your organization, which may differ from those of Microsoft.
- ♦ If your organization is administering your use of Microsoft products, please direct your privacy inquiries, including any requests to exercise your data subject rights, to your administrator. See also the [Notice to end users](#) section of this privacy statement.
- ♦ If you are uncertain whether your account is a work or school account, please contact your organization.

Third-party accounts. The data associated with a third-party Microsoft account, and how it will be used, is generally similar to the use and collection of data associated with a personal Microsoft account. Your service provider has control over your account, including the ability to access or delete your account. **You should carefully review the terms the third party provided you to understand what it can do with your account.**

Collection of data from children

When a Microsoft product collects age, and there is an age in your jurisdiction under which parental consent or authorization is required to use the product, the product will either block users under that age or will ask them to provide consent or authorization from a parent or guardian before they can use it. We will not knowingly ask children under that age to provide more data than is required to provide for the product.

Once parental consent or authorization is granted, the child's account is treated much like any other account. The child can access communication services, like Outlook and Skype, and can freely communicate and share data with other users of all ages. [Learn more about parental consent and Microsoft child accounts.](#)

Parents or guardians can change or revoke the consent choices previously made, and review, edit, or request the deletion of the personal data of the children for whom they provided consent or authorization. As the organizer of a Microsoft family group, the parent or guardian can manage a child's information and settings on their [Family Safety](#) page and view and delete a child's data on their [privacy dashboard](#).

Below is additional information about the collection of data from children as related to Xbox.

What is Xbox? Xbox is the gaming and entertainment division of Microsoft. Xbox hosts an online network that consists of software and enables online experiences crossing multiple platforms. This network lets your child find and play games, view content, and connect with friends on Xbox and other gaming and social networks. Children can connect to the Xbox network using Xbox consoles, Windows devices, and mobile devices (Android and iPhone).

Xbox consoles are devices your child can use to find and play games, movies, music, and other digital entertainment. When they sign in to Xbox, in apps, games or on a console, we assign a unique identifier to their device. For instance, when their Xbox console is connected to the internet and they

sign in to the console, we identify which console and which version of the console's operating system they are using.

Xbox continues to provide new experiences in client apps that are connected to and backed by services such as Xbox network and cloud gaming. When signed in to an Xbox experience, we collect required data to help keep these experiences reliable, up to date, secure, and performing as expected.

Data we collect when you create an Xbox profile. You as the parent or guardian are required to consent to the collection of personal data from a child under 13 years old. With your permission, your child can have an Xbox profile and use the online Xbox network. During the child Xbox profile creation, you will sign in with your own Microsoft account to verify that you are an adult organizer in your Microsoft family group. We collect an alternate email address or phone number to boost account security. If your child needs help accessing their account, they will be able to use one of these alternates to validate they own the Microsoft account.

We collect limited information about children, including name, birthdate, email address, and region. When you sign your child up for an Xbox profile, they get a gamertag (a public nickname) and a unique identifier. When you create your child's Xbox profile you consent to Microsoft collecting, using, and sharing information based on their privacy and communication settings on the Xbox online network. Your child's privacy and communication settings are defaulted to the most restrictive.

Data we collect. We collect information about your child's use of Xbox services, games, apps, and devices including:

- ♦ When they sign in and sign out of Xbox, purchase history, and content they obtain.
- ♦ Which games they play and apps they use, their game progress, achievements, play time per game, and other play statistics.
- ♦ Performance data about Xbox consoles, Xbox Game Pass and other Xbox apps, the Xbox network, connected accessories, and network connection, including any software or hardware errors.
- ♦ Content they add, upload, or share through the Xbox network, including text, pictures, and video they capture in games and apps.
- ♦ Social activity, including chat data and interactions with other gamers, and connections they make (friends they add and people who follow them) on the Xbox network.

If your child uses an Xbox console or Xbox app on another device capable of accessing the Xbox network, and that device includes a storage device (hard drive or memory unit), usage data will be stored on the storage device and sent to Microsoft the next time they sign in to Xbox, even if they have been playing offline.

Xbox console diagnostic data. If your child uses an Xbox console, the console will send required data to Microsoft. Required data is the minimum data necessary to help keep Xbox safe, secure, up to date, and performing as expected.

Game captures. Any player in a multiplayer game session can record video (game clips) and capture screenshots of their view of the game play. Other players' game clips and screenshots can capture your child's in-game character and gamertag during that session. If a player captures game clips and

screenshots on a PC, the resulting game clips might also capture audio chat if your child's privacy and communication settings on the Xbox online network allow it.

Captioning. During Xbox real-time ("party") chat, players may activate a voice-to-text feature that lets them view that chat as text. If a player activates this feature, Microsoft uses the resulting text data to provide captioning of chat for players who need it. This data may also be used to provide a safe gaming environment and enforce the [Community Standards for Xbox](#).

Data use. Microsoft uses the data we collect to improve gaming products and experiences— making it safer and more fun over time. Data we collect also enables us to provide your child with personalized, curated experiences. This includes connecting them to games, content, services, and recommendations.

Xbox data viewable by others. When your child is using the Xbox network, their online presence (which can be set to "appear offline" or "blocked"), gamertag, game play statistics, and achievements are visible to other players on the network. Depending on how you set your child's Xbox safety settings, they might share information when playing or communicating with others on the Xbox network.

In order to help make the Xbox network a safe gaming environment and enforce the Community Standards for Xbox, we may collect and review voice, text, images, videos and in-game content (such as game clips your child uploads, conversations they have, and things they post in clubs and games).

Xbox data shared with game and apps publishers. When your child uses an Xbox online game or any network-connected app on their Xbox console, PC, or mobile device, the publisher of that game or app has access to data about their usage to help the publisher deliver, support, and improve its product. This data may include: your child's Xbox user identifier, gamertag, limited account info such as country and age range, data about your child's in-game communications, any Xbox enforcement activity, game-play sessions (for example, moves made in-game or types of vehicles used in-game), your child's presence on the Xbox network, the time they spend playing the game or app, rankings, statistics, gamer profiles, avatars, or gamerpics, friends lists, activity feeds for official clubs they belong to, official club memberships, and any content they create or submit in the game or app.

Third-party publishers and developers of games and apps have their own distinct and independent relationship with users and their collection and usage of personal data is subject to their specific privacy policies. You should carefully review their policies to determine how they use your child's data. For example, publishers may choose to disclose or display game data (such as on leaderboards) through their own services. You may find their policies linked from the game or app detail pages in our stores.

Learn more at [Data Sharing with Games and Apps](#).

To stop sharing game or app data with a publisher, remove its games or app from all devices where they have been installed. Some publisher access to your child's data may be revoked at microsoft.com/consent.

Managing child settings. As the organizer of a Microsoft family group, you can manage a child's information and settings on their [Family Safety](#) page, as well as their Xbox profile privacy settings from

their [Xbox Privacy & online safety page](#).

You can also use the [Xbox Family Settings](#) app to manage your child's experience on the Xbox Network including: spending for Microsoft and Xbox stores, viewing your child's Xbox activity, and setting age ratings and the amount of screen time.

Learn more about managing Xbox profiles at [Xbox online safety and privacy settings](#).

Learn more about Microsoft family groups at [Simplify your family's life](#).

Accessing child data. As the organizer of a Microsoft family group, a parent can view and delete a child's data on their [privacy dashboard](#). The dashboard allows you to review your child's personal information, have it deleted, and refuse to permit further collection or use of your child's information.

To close your child's account, sign in with their account info at account.microsoft.com/profile and select "How to close your account."

Legacy.

- ♦ **Xbox 360.** This Xbox console collects limited required diagnostic data. This data helps keep your child's console functioning as expected.
- ♦ **Kinect.** The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control game play. For example:
 - If you choose, the camera can be used to sign in to the Xbox network automatically using facial recognition. This data stays on the console, is not shared with anyone, and can be deleted at any time.
 - For game play, Kinect will map distances between the joints on your child's body to create a stick figure representation to enable play.
 - The Kinect microphone can enable voice chat between players during play. The microphone also enables voice commands for control of the console, game, or app, or to enter search terms.
 - The Kinect sensor can also be used for audio and video communications through services such as Skype.

Learn more about Kinect at [Xbox Kinect and Privacy](#).

Other important privacy information

Below you will find additional privacy information, such as how we secure your data, where we process your data, and how long we retain your data. You can find more information on Microsoft and our commitment to protecting your privacy at [Microsoft Privacy](#).

Security of personal data

Microsoft is committed to protecting the security of your personal data. We use a variety of security technologies and procedures to help protect your personal data from unauthorized

access, use, or disclosure. For example, we store the personal data you provide on computer systems that have limited access and are in controlled facilities. When we transmit highly confidential data (such as a credit card number or password) over the internet, we protect it through the use of encryption. Microsoft complies with applicable data protection laws, including applicable security breach notification laws.

Where we store and process personal data

Personal data collected by Microsoft may be stored and processed in your region, in the United States, and in any other country where Microsoft or its affiliates, subsidiaries, or service providers operate facilities. Microsoft maintains major data centers in Australia, Austria, Brazil, Canada, Finland, France, Germany, Hong Kong, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom, and the United States. Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a data center in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to process the data that we collect under this privacy statement according to this statement's provisions and the requirements of applicable law.

We transfer personal data from the European Economic Area, the United Kingdom, and Switzerland to other countries, some of which have not yet been determined by the European Commission to have an adequate level of data protection. For example, their laws may not guarantee you the same rights, or there may not be a privacy supervisory authority there that is capable of addressing your complaints. When we engage in such transfers, we use a variety of legal mechanisms, including contracts such as the standard contractual clauses published by the European Commission under Commission Implementing Decision 2021/914, to help protect your rights and enable these protections to travel with your data. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Microsoft processes personal data, see this article on [the European Commission website](#).

Microsoft Corporation complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom, and Switzerland to the United States, although Microsoft does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of personal data in light of the judgment of the Court of Justice of the EU in Case C-311/18. Microsoft Corporation has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If third-party agents process personal data on our behalf in a manner inconsistent with the principles of either Privacy Shield framework, we remain liable unless we prove we are not responsible for the event giving rise to the damage. The controlled U.S. subsidiaries of Microsoft Corporation, as identified in our self-certification submission, also adhere to the Privacy Shield Principles—for more info, see the list of [Microsoft U.S. entities or subsidiaries adhering to the Privacy Shield Principles](#).

If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, visit the [Privacy Shield website](#).

If you have a question or complaint related to participation by Microsoft in the EU-U.S. or Swiss-U.S. Privacy Shield, we encourage you to contact us via our [web form](#). For any complaints related to the Privacy Shield frameworks that Microsoft cannot resolve directly, we have chosen to cooperate with the relevant EU Data Protection Authority, or a panel established by the European data protection authorities, for resolving disputes with EU individuals, and with the Swiss Federal Data Protection and Information Commissioner (FDPIC) for resolving disputes with Swiss individuals. Please contact us if you'd like us to direct you to your data protection authority contacts. As further explained in the Privacy Shield Principles, binding arbitration is available to address residual complaints not resolved by other means. Microsoft is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Individuals whose personal data is protected by Japan's Act on the Protection of Personal Information should refer to the article on the [Japanese Personal Information Protection Commission's website](#) (only published in Japanese) for more information on the Commission's review of certain countries' personal data protection systems.

Our retention of personal data

Microsoft retains personal data for as long as necessary to provide the products and fulfill the transactions you have requested, or for other legitimate purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements. Because these needs can vary for different data types, the context of our interactions with you or your use of products, actual retention periods can vary significantly.

Other criteria used to determine the retention periods include:

- ♦ **Do customers provide, create, or maintain the data with the expectation we will retain it until they affirmatively remove it?** Examples include a document you store in OneDrive, or an email message you keep in your Outlook.com inbox. In such cases, we would aim to maintain the data until you actively delete it, such as by moving an email from your Outlook.com inbox to the Deleted Items folder, and then emptying that folder (when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion). (Note that there may be other reasons why the data has to be deleted sooner, for example if you exceed limits on how much data can be stored in your account.)
- ♦ **Is there an automated control, such as in the Microsoft privacy dashboard, that enables the customer to access and delete the personal data at any time?** If there is not, a shortened data retention time will generally be adopted.
- ♦ **Is the personal data of a sensitive type?** If so, a shortened retention time would generally be adopted.

- ♦ **Has Microsoft adopted and announced a specific retention period for a certain data type?** For example, for Bing search queries, we de-identify stored queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers that are used to identify a particular account or device after 18 months.
- ♦ **Has the user provided consent for a longer retention period?** If so, we will retain data in accordance with your consent.
- ♦ **Is Microsoft subject to a legal, contractual, or similar obligation to retain or delete the data?** Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve data relevant to an investigation, or data retained for the purposes of litigation. Conversely, if we are required by law to remove unlawful content, we will do so.

California Consumer Privacy Act

If you are a California resident, we process your personal data in accordance with the California Consumer Privacy Act (CCPA). This CCPA section of our Privacy Statement contains information required by the CCPA and supplements our Privacy Statement.

Sale. We do not sell your personal data. So, we do not offer an opt-out to the sale of personal data.

Rights. You have the right to request that we (i) disclose what personal data we collect, use, disclose, and sell and (ii) delete your personal data. You may make these requests yourself or through an authorized agent. If you use an authorized agent, we provide your agent with [detailed guidance](#) on how to exercise your CCPA rights.

If you have a Microsoft account, you must exercise your rights through the [Microsoft privacy dashboard](#), which requires you to log in to your Microsoft account. If you have an additional request or questions after using the dashboard, you may contact Microsoft at the address in the [How to contact us](#) section, use our [web form](#), or call our US toll free number 1.844.931.2038. If you do not have an account, you may exercise your rights by contacting us as described above. We may ask for additional information, such as your country of residence, email address, and phone number, to validate your request before honoring the request.

You have a right not to receive discriminatory treatment if you exercise your CCPA rights. We will not discriminate against you if you exercise your CCPA rights.

Personal Information Processing. In the bulleted list below, we outline the categories of personal data we collect, the sources of the personal data, our purposes of processing, and the categories of third-party recipients with whom we share the personal data. For a description of the data included in each category, please see the [Personal data we collect](#) section.

Categories of Personal Data

- ♦ Name and contact data

- Sources of personal data: Interactions with users and partners with whom we offer co-branded services
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; respond to customer questions; help, secure, and troubleshoot; and marketing
 - Recipients: Service providers and user-directed entities
- ◆ Credentials
 - Sources of personal data: Interactions with users and organizations that represent users
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; authentication and account access; and help, secure and troubleshoot
 - Recipients: Service providers and user-directed entities
- ◆ Demographic data
 - Sources of personal data: Interactions with users and purchases from data brokers
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide and personalize our products; product development; help, secure, and troubleshoot; and marketing
 - Recipients: Service providers and user-directed entities
- ◆ Payment data
 - Sources of personal data: Interactions with users and financial institutions
 - Purposes of Processing (Collection and Sharing with Third Parties): Transact commerce; process transactions; fulfill orders; help, secure, and troubleshoot; and detect and prevent fraud
 - Recipients: Service providers and user-directed entities
- ◆ Subscription and licensing data
 - Sources of personal data: Interactions with users and organizations that represent users
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide, personalize, and activate our products; customer support; help, secure, and troubleshoot; and marketing
 - Recipients: Service providers and user-directed entities
- ◆ Interactions
 - Sources of personal data: Interactions with users including data Microsoft generates through those interactions
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide and personalize our products; product improvement; product development; marketing; and help, secure and troubleshoot
 - Recipients: Service providers and user-directed entities
- ◆ Content
 - Sources of personal data: Interactions with users and organizations that represent users
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; safety; and help, secure, and troubleshoot
 - Recipients: Service providers and user-directed entities
- ◆ Video or recordings
 - Sources of personal data: Interactions with users and publicly available sources

- Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; product improvement; product development; marketing; help, secure, and troubleshoot; and safety
 - Recipients: Service providers and user-directed entities
- ◆ Feedback and ratings
 - Sources of personal data: Interactions with users
 - Purposes of Processing (Collection and Sharing with Third Parties): Provide our products; product improvement; product development; customer support; and help, secure, and troubleshoot
 - Recipients: Service providers and user-directed entities

While the bulleted list above contains the primary sources and purposes of processing for each category of personal data, we also collect personal data from the sources listed in the [Personal data we collect](#) section, such as developers who create experiences through or for Microsoft products. Similarly, we process all categories of personal data for the purposes described in the [How we use personal data](#) section, such as meeting our legal obligations, developing our workforce, and doing research.

Disclosures of personal data for business or commercial purposes. As indicated in the [Reasons we share personal data](#) section, we share personal data with third parties for various business and commercial purposes. The primary business and commercial purposes for which we share personal data are the purposes of processing listed in the table above. However, we share all categories of personal data for the business and commercial purposes in the [Reasons we share personal data](#) section.

See our [CCPA Notice](#) for additional information.

Advertising

Advertising allows us to provide, support, and improve some of our products. Microsoft does not use what you say in email, chat, video calls or voice mail, or your documents, photos, or other personal files to target ads to you. We use other data, detailed below, for advertising in our products and on third-party properties. For example:

- ◆ Microsoft may use data we collect to select and deliver some of the ads you see on Microsoft web properties, such as [Microsoft.com](#), MSN, and Bing.
- ◆ When the advertising ID is enabled in Windows as part of your privacy settings, third parties can access and use the advertising ID (much the same way that websites can access and use a unique identifier stored in a cookie) to select and deliver ads in such apps.
- ◆ We may share data we collect with partners, such as Verizon Media, AppNexus, or Facebook (see below), so that the ads you see in our products and their products are more relevant and valuable to you.
- ◆ Advertisers may choose to place our web beacons on their sites, or use similar technologies, in order to allow Microsoft to collect information on their sites such as

activities, purchases, and visits; we use this data on behalf of our advertising customers to provide ads.

The ads that you see may be selected based on data we process about you, such as your interests and favorites, your location, your transactions, how you use our products, your search queries, or the content you view. For example, if you view content on MSN about automobiles, we may show advertisements about cars; if you search "pizza places in Seattle" on Bing, you may see advertisements in your search results for restaurants in Seattle.

The ads that you see may also be selected based on other information learned about you over time using demographic data, location data, search queries, interests and favorites, usage data from our products and sites, and the information we collect about you from the sites and apps of our advertisers and partners. We refer to these ads as "personalized advertising" in this statement. For example, if you view gaming content on [xbox.com](https://www.xbox.com), you may see offers for games on MSN. To provide personalized advertising, we combine cookies placed on your device using information that we collect (such as IP address) when your browser interacts with our websites. If you opt out of receiving personalized advertising, data associated with these cookies will not be used.

We may use information about you to serve you with personalized advertising when you use Microsoft services. If you are logged in with your Microsoft account and have consented to allow Microsoft Edge to use your online activity for personalized advertising, you will see offers for products and services based on your online activity while using Microsoft Edge. To configure your privacy settings for Edge, go to Microsoft Edge > Settings > Privacy and Services. To configure your privacy and ad settings for your Microsoft account with respect to your online activity across browsers, including Microsoft Edge, or when visiting third-party websites or apps, go to your dashboard at privacy.microsoft.com.

Further details regarding our advertising-related uses of data include:

- ♦ **Advertising industry best practices and commitments.** Microsoft is a member of the [Network Advertising Initiative](#) (NAI) and adheres to the NAI Code of Conduct. We also adhere to the following self-regulatory programs:
 - In the US: [Digital Advertising Alliance \(DAA\)](#)
 - In Europe: [European Interactive Digital Advertising Alliance \(EDAA\)](#)
 - In Canada: [Ad Choices: Digital Advertising Alliance of Canada \(DAAC\)](#) / [Choix de Pub: l'Alliance de la publicité numérique du Canada \(DAAC\)](#)
- ♦ **Health-related ad targeting.** In the United States, we provide personalized advertising based on a limited number of standard, non-sensitive health-related interest categories, including allergies, arthritis, cholesterol, cold and flu, diabetes, gastrointestinal health, headache / migraine, healthy eating, healthy heart, men's health, oral health, osteoporosis, skin health, sleep, and vision / eye care. We will also personalize ads based on custom, non-sensitive health-related interest categories as requested by advertisers.
- ♦ **Children and advertising.** We do not deliver personalized advertising to children whose birthdate in their Microsoft account identifies them as under 18 years of age.
- ♦ **Data retention.** For personalized advertising, we retain data for no more than 13 months, unless we obtain your consent to retain the data longer.

- **Data sharing.** In some cases, we share with advertisers reports about the data we have collected on their sites or ads.

Data collected by other advertising companies. Advertisers sometimes include their own web beacons (or those of their other advertising partners) within their advertisements that we display, enabling them to set and read their own cookie. Additionally, Microsoft partners with third-party ad companies to help provide some of our advertising services, and we also allow other third-party ad companies to display advertisements on our sites. These third parties may place cookies on your computer and collect data about your online activities across websites or online services. These companies currently include, but are not limited to: [AppNexus](#), [Facebook](#), [Media.net](#), [Outbrain](#), [Taboola](#) and [Verizon Media](#). Select any of the preceding links to find more information on each company's practices, including the choices it offers. Many of these companies are also members of the [NAI](#) or [DAA](#), which each provide a simple way to opt out of ad targeting from participating companies.

Speech recognition technologies

Speech recognition technologies are integrated into many Microsoft products and services. Microsoft provides both device-based speech recognition features and cloud-based (online) speech recognition features. Microsoft's speech recognition technology transcribes voice data into text. With your permission, Microsoft employees and vendors working on behalf of Microsoft, will be able to review snippets of your voice data or voice clips in order to build and improve our speech recognition technologies. These improvements allow us to build better voice-enabled capabilities that benefit users across all our consumer and enterprise products and services. Prior to employee or vendor review of voice data, we protect users' privacy by taking steps to de-identify the data, requiring non-disclosure agreements with relevant vendors and their employees, and requiring that employees and vendors meet high privacy standards. [Learn more about Microsoft and your voice data.](#)

Preview or free-of-charge releases

Microsoft offers preview, insider, beta or other free-of-charge products and features ("previews") to enable you to evaluate them while providing Microsoft with data about your use of the product, including feedback and device and usage data. As a result, previews can automatically collect additional data, provide fewer controls, and otherwise employ different privacy and security measures than those typically present in our products. If you participate in previews, we may contact you about your feedback or your interest in continuing to use the product after general release.

Changes to this privacy statement

We update this privacy statement when necessary to provide greater transparency or in response to:

- ♦ Feedback from customer, regulators, industry, or other stakeholders.
- ♦ Changes in our products.
- ♦ Changes in our data processing activities or policies.

When we post changes to this statement, we will revise the "last updated" date at the top of the statement and describe the changes on the [Change history](#) page. If there are material changes to the statement, such as a change to the purposes of processing of personal data that is not consistent with the purpose for which it was originally collected, we will notify you either by prominently posting a notice of such changes before they take effect or by directly sending you a notification. We encourage you to periodically review this privacy statement to learn how Microsoft is protecting your information.

How to contact us

If you have a privacy concern, complaint, or question for the Microsoft Chief Privacy Officer or the Data Protection Officer for your region, please contact us by using our [web form](#). We will respond to questions or concerns as required by law and within a period no longer than 30 days. You can also raise a concern or lodge a complaint with a data protection authority or other official with jurisdiction.

When Microsoft is a controller, unless otherwise stated, Microsoft Corporation and, for those in the European Economic Area, the United Kingdom, and Switzerland, Microsoft Ireland Operations Limited are the data controllers for personal data we collect through the products subject to this statement. Our addresses are:

- ♦ Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA. Telephone: +1 (425) 882 8080.
- ♦ Microsoft Ireland Operations Limited, Attn: Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117.

To find the Microsoft subsidiary in your country or region, see the list of [Microsoft office locations around the world](#).

If you would like to exercise your rights under the California Consumer Privacy Act, you may contact Microsoft at the address above, use our [web form](#), or call our US toll free number 1.844.931.2038.

Where French law applies, you can also send us specific instructions regarding the use of your personal data after your death, by using our [web form](#).

If you have a technical or support question, please visit [Microsoft Support](#) to learn more about Microsoft Support offerings. If you have a personal Microsoft account password question, please visit [Microsoft account support](#).

Enterprise and developer products

Enterprise and Developer Products are Microsoft products and related software offered to and designed primarily for use by organizations and developers. They include:

- Cloud services, referred to as Online Services in the Product Terms, such as Microsoft 365 and Office 365, Microsoft Azure, Microsoft Dynamics365, and Microsoft Intune for which an organization (our customer) contracts with Microsoft for the services ("Enterprise Online Services").
- Other enterprise and developer tools and cloud-based services, such as Azure PlayFab Services (to learn more see [Azure PlayFab Terms of Service](#)).
- Server, developer, and hybrid cloud platform products, such as Windows Server, SQL Server, Visual Studio, System Center, Azure Stack and open source software like Bot Framework solutions ("Enterprise and Developer Software").
- Appliances and hardware used for storage infrastructure, such as StorSimple ("Enterprise Appliances").
- Professional services referred to in the Product Terms that are available with Enterprise Online Services, such as onboarding services, data migration services, data science services, or services to supplement existing features in the Enterprise Online Services.

In the event of a conflict between this Microsoft privacy statement and the terms of any agreement(s) between a customer and Microsoft for Enterprise and Developer Products, the terms of those agreement(s) will control.

You can also learn more about our Enterprise and Developer Products' features and settings, including choices that impact your privacy or your end users' privacy, in product documentation.

If any of the terms below are not defined in this Privacy Statement or the Product Terms, they have the definitions below.

General. When a customer tries, purchases, uses, or subscribes to Enterprise and Developer Products, or obtains support for or professional services with such products, Microsoft receives data from you and collects and generates data to provide the service (including improving, securing, and updating the service), conduct our business operations, and communicate with the customer. For example:

- When a customer engages with a Microsoft sales representative, we collect the customer's name and contact data, along with information about the customer's organization, to support that engagement.
- When a customer interacts with a Microsoft support professional, we collect device and usage data or error reports to diagnose and resolve problems.
- When a customer pays for products, we collect contact and payment data to process the payment.
- When Microsoft sends communications to a customer, we use data to personalize the content of the communication.
- When a customer engages with Microsoft for professional services, we collect the name and contact data of the customer's designated point of contact and use information provided by the customer to perform the services that the customer has requested.

The Enterprise and Developer Products enable you to purchase, subscribe to, or use other products and online services from Microsoft or third parties with different privacy practices, and those other products and online services are governed by their respective privacy statements and policies.

Enterprise online services

To provide the Enterprise Online Services, Microsoft uses data you provide (including Customer Data, Personal Data, Administrator Data, Payment Data, and Support Data) and data Microsoft collects or generates associated with your use of the Enterprise Online Services. We process data as described in the [Product Terms](#), [Microsoft Products and Services Data Protection Addendum](#) and the [Microsoft Trust Center](#).

Personal Data. Customer is the controller of Personal Data and Microsoft is the processor of such data, except when (a) Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor or (b) as stated otherwise in the standard [Products and Services DPA](#). In addition, as provided in the standard [Products and Services DPA](#), Microsoft has taken on the added responsibilities of a data controller under GDPR when processing Personal Data in connection with its business operations incident to providing its services to Microsoft's commercial customers, such as billing and preparing invoices; account management; compensation; financial reporting; business planning and product strategy; improving core functionality for accessibility, privacy, and energy efficiency; and combatting fraud, cybercrime, and cyberattacks that may affect Microsoft or Microsoft products. We use Personal Data in the least identifiable form that will support processing necessary for these business operations. We generally aggregate Personal Data before using it for our business operations, removing the ability to identify specific individuals.

Administrator Data. Administrator Data is the information provided to Microsoft during sign-up, purchase, or administration of Enterprise Online Services. We use Administrator Data to provide the Enterprise Online Services, complete transactions, service the account, detect and prevent fraud, and comply with our legal obligations. Administrator Data includes the name, address, phone number, and email address you provide, as well as aggregated usage data related to your account, such as the controls you select. Administrator Data also includes contact information of your colleagues and friends if you agree to provide it to Microsoft for the limited purpose of sending them an invitation to use the Enterprise Online Services; we contact those individuals with communications that include information about you, such as your name and profile photo.

As needed, we use Administrator Data to contact you to provide information about your account, subscriptions, billing, and updates to the Enterprise Online Services, including information about new features, security, or other technical issues. We also contact you regarding third-party inquiries we receive regarding use of the Enterprise Online Services, as described in your agreement. You cannot unsubscribe from these non-promotional communications. We may also contact you regarding information and offers about other products and services, or share your contact information with Microsoft's partners. When such a partner has specific services or solutions to meet your needs, or to optimize your use of the Enterprise Online Services, we may share limited, aggregated information about your

organization's account with the partner. Microsoft will not share your confidential information or contact information with the authorized partner unless we have sufficient rights to do so. You can manage your contact preferences or update your information in your account profile.

Payment Data. We use payment data to complete transactions, as well as to detect and prevent fraud.

Support Data. Customers provide or authorize Microsoft to collect data in connection with obtaining technical support for the Enterprise Online Services. We process Support Data to provide technical support and as described in the [Products and Services DPA](#).

Local Software and Diagnostic Data. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications). The local software may collect Diagnostic Data (as defined in the [Products and Services DPA](#)) about the use and performance of that software. That data may be transmitted to Microsoft and used for the purposes described in the [Products and Services DPA](#).

Bing Search Services Data. Bing Search Services, as defined in the Product Terms, use data such as search queries as described in the [Bing](#) section of this privacy statement.

Enterprise and developer software and enterprise appliances

Enterprise and developer software and enterprise appliances collect data to operate effectively and provide you the best experiences. The data we collect depends on the features you use, as well as your configuration and settings, but it is generally limited to device and usage data. Customers have choices about the data they provide. Here are examples of the data we collect:

- ♦ During installation or when you upgrade an enterprise and developer software, we may collect device and usage data to learn whether you experience any difficulties.
- ♦ When you use enterprise software or enterprise appliances, we may collect device and usage data to learn about your operating environment to improve security features.
- ♦ When you experience a crash using enterprise software or enterprise appliances, you may choose to send Microsoft an error report to help us diagnose the problem and deliver customer support.

Microsoft uses the data we collect from enterprise and developer software and enterprise appliances to provide and improve our products, to deliver customer support, to activate the product, to communicate with you, and to operate our business.

Microsoft SQL Server is a relational database management platform and includes products that can be installed separately (such as SQL Server Management Studio). For detailed information about what data we collect, how we use it, and how to manage your privacy options, visit the [SQL Server privacy page](#). If you work in an organization, your administrator can set certain telemetry settings in SQL Server via Group Policy.

HoloLens. HoloLens headsets are self-contained Windows computers with Wi-Fi connectivity that enable a mixed reality experience for apps and solutions. Microsoft collects diagnostic data to solve problems and to keep Windows running on HoloLens up to date, secure, and operating properly. Diagnostic data also helps us improve HoloLens and related Microsoft products and services depending on the diagnostic data settings you've chosen for your device. [Learn more about Windows diagnostic data.](#)

HoloLens also processes and collects data related to the HoloLens experience and device, which include cameras, microphones, and infrared sensors that enable motions and voice to navigate.

- ♦ If you choose, cameras can be used to sign you in automatically using your iris. To do this, HoloLens takes an image of your iris and measures distances between key points to create and store a numeric value that represents only you. This data stays on the HoloLens and is not shared with anyone, and you can choose to delete this data from your HoloLens at any time.
- ♦ HoloLens also detects hand gestures intended for system interactions (such as menu navigation, pan/zoom, and scroll). This data is processed on your HoloLens device and is not stored.
- ♦ HoloLens derives tracking points based on your environment which allows it to understand surfaces in space and allows you to place digital assets on them. There are no images associated with this environmental data and it is stored locally on the HoloLens device. You can choose to delete this data from your HoloLens at any time.

The headset's microphones enable voice commands for navigation, controlling apps, or to enter search terms. [Learn more about voice data collection.](#)

Productivity and communications products

Productivity and communications products are applications, software, and services you can use to create, store, and share documents, as well as communicate with others.

Microsoft 365

Microsoft 365, previous versions called Office 365, is a collection of productivity services and Office applications including Word, Excel, PowerPoint, and Outlook, among others. For more details about Outlook, see the [Outlook](#) section of this privacy statement. Microsoft 365 is a service that is comprised of client software applications and connected online services that span many platforms and have numerous interdependent experiences. Various Microsoft 365 services enable you to use your file content for designs and recommendations, collaborate with others within your documents, and provide you functionality from other Microsoft products, such as Bing and Cortana, and third-party connected products. If you work in an organization, your administrator may turn off or disable these connected services. You can access the privacy controls within your Office apps by selecting **File > Account > Account Privacy**. See [Account Privacy Settings](#) for more information.

Office Roaming Service. The Office Roaming Service helps keep your Microsoft 365 settings up to date across your devices running Microsoft 365. When you sign in to Microsoft 365 with your Microsoft account or an account issued by your organization, the Office Client Policy Service is turned on and syncs some of your customized Microsoft 365 settings to Microsoft servers (such as a list of most recently used documents and the last location viewed within a document). When you sign in to Microsoft 365 on another device with the same account, the Office Roaming Service downloads your settings from Microsoft servers and applies them to the additional device. The Office Roaming Service also applies some of your customized Microsoft 365 settings when you sign in to Office.com. When you sign out of Microsoft 365, the Office Roaming Service removes your Microsoft 365 settings from your device. Any changes you make to your customized Microsoft 365 settings are sent to Microsoft servers.

Microsoft Updates. Microsoft uses services such as Click-to-Run or Microsoft AutoUpdate to provide you with security and other important updates.

Click-to-Run Update Service. The Click-to-Run Update Service allows you to install certain Microsoft 365 products over the internet. The Click-to-Run Update Service also automatically detects online updates to Click-to-Run-enabled products on your device and downloads and installs them automatically.

Translator. Translator used in Office apps is designed as a no-trace connected experience. With [no trace](#) connected experience, no portion of your translation request that gets sent to Microsoft Translator API service will be logged, your submitted text will not be used to improve the quality of the Microsoft Translator service, and there will not be any record of any portion of your data retained by Microsoft.

Diagnostic Data. Diagnostic data is used to (i) keep your Office apps secure and up to date; (ii) detect, diagnose, and remediate problems; and (iii) make product improvements. This data does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Office. Users have a choice between two different levels of diagnostic data collection, Required and Optional.

- ♦ **Required.** The minimum data necessary to help keep Office apps secure, up to date, and performing as expected on the device it's installed on.
- ♦ **Optional.** Additional data that helps us make product improvements and provides enhanced information to help us detect, diagnose, and remediate issues.

See [Diagnostic Data in Office](#) for more information.

Connected Experiences. Microsoft 365 continues to provide more experiences in client applications that are connected to and backed by cloud-based services. If you choose to use connected experiences, required service data will be collected to help keep these connected experiences reliable, up to date, secure, and performing as expected.

Microsoft 365 consists of client software applications and connected experiences designed to enable you to create, communicate, and collaborate more effectively. Working with others on a document stored on OneDrive for Business or translating the contents of a Word document

into a different language are examples of connected experiences. There are two types of connected experiences.

- ♦ **Experiences that analyze your content.** Experiences that use your Office content to provide you with design recommendations, editing suggestions, data insights, and similar features. For example, PowerPoint Designer or Editor in Word.
- ♦ **Experiences that download online content.** Experiences that allow you to search and download online content including templates, images, 3D models, videos, and reference materials to enhance your documents. For example, templates or PowerPoint QuickStarter.

You can access the privacy controls within your Office apps by selecting **File > Account > Account Privacy**. These privacy settings allow you to configure your connected experiences. For example, you can choose to enable connected experiences that download online content, but not connected experiences that analyze content. Turning off connected experiences will also turn off additional experiences, such as document co-authoring and online file storage. But even if you use this privacy setting to turn off connected experiences, certain functionality will remain available, such as syncing your mailbox in Outlook, as well as essential services described below.

If you choose to disable certain types of connected experiences, either the ribbon or menu command for those connected experiences will be grayed out or you will get an error message when you try to use those connected experiences.

There are a set of services that are essential to how Microsoft 365 functions and cannot be disabled. For example, the licensing service that confirms that you are properly licensed to use Microsoft 365 is essential. Required service data about these services is collected and sent to Microsoft, regardless of any other settings that you have configured. See [Essential Services](#) for more information.

Required service data for connected experiences. As you use a connected experience, data is sent to and processed by Microsoft to provide you that connected experience. This data is necessary because this information enables us to deliver these cloud-based connected experiences. We refer to this data as required service data.

Required service data can include information related to the operation of the connected experience that is needed to keep the underlying service secure, up to date, and performing as expected. If you choose to use a connected experience that analyzes your content, for example Translate in Word, the text you typed and selected to translate is also sent and processed to provide you the connected experience. Your text and the translation are not stored by our service. Required service data can also include information needed by a connected experience to perform its task, such as configuration information about the Office app.

See [Required service data for Office](#) for more information.

Microsoft Teams

This section applies to the consumer offering of Teams; if you are using Teams with a school or work account, see the [Enterprise and developer products](#) of this privacy statement.

Teams is an all-in-one collaboration and communication hub. Teams lets you stay organised and connected across your entire life. Teams allows you to call people with voice or video calling. Teams allows you to easily find people, files, photos, conversations, tasks, and calendars in one convenient and secure place. Teams allows you to store confidential information like passwords, rewards numbers, or login information and share it with others within Teams. With your consent, you can share your location with friends and family.

As part of providing these features, Microsoft collects data about the usage of the features as well as information about your communications, including the time and date of the communication and users that are part of the communication.

Teams profile. Your Teams profile includes information you provided when you set up a Microsoft account. To enable other people to find you on Teams (or products that interact with Teams for personal use, including Teams for enterprise) your display name and picture are visible to other users on Teams that have your contact information.

Teams contacts. With your permission, Teams will sync your device, Outlook, and Skype contacts periodically and check for other Teams users that match contacts in your device, Outlook, or Skype address books. You are always in control of your contacts and can stop syncing at any time. If you choose to stop syncing your device, Outlook, or Skype contacts, or you are inactive on your device, any contacts that have not been matched during the synchronization process will be deleted from Teams. If you wish to invite any of your device, Outlook, or Skype contacts to join a conversation, you can invite users to a 1:1 directly, or Microsoft can send an invitation on your behalf via SMS or email for invitations to group conversations. You can block users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Notice to non-user contacts. If your information appears in the device, Outlook, or Skype address books of a Teams user who chooses to sync their device, Outlook, or Skype contacts with their Teams contacts, Microsoft may process your data in order to determine whether you are a current Teams user and to allow Teams users to invite you to the service, including via SMS and email. As long as the Teams user continues to be active on Teams on their device and continues to enable contact syncing with the applicable device or service, your information will be stored on our servers and we will periodically process your information as a part of the Teams user's contact syncing experience to check whether you have subsequently joined Teams.

[Learn more about how we process your information in connection with the contact syncing feature offered to Teams users.](#)

If you do choose to join Teams, you will appear as a suggested new Teams contact for any Teams users with your information in their device, Outlook, or Skype address books. As a Teams user, you will be able to block other Teams users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Third-party contacts. You can also choose to sync contacts from third-party providers. If you choose to unsync your third-party contacts on Teams, all third-party contacts are deleted from Teams. If you gave your consent to use those third-party contacts on other Microsoft apps and services, these contacts will still be available to those other Microsoft apps and services.

You can remove third-party contacts from all Microsoft apps and services by removing third-party accounts from Teams. Please note that removing a third-party account from Teams may impact your experiences on other Microsoft apps and services that also use that third-party account.

Teams calendar. You can also choose to sync your Teams calendar with calendars from third-party providers. You can stop syncing your Teams calendar anytime by removing a third-party account from Teams. If you have consented to use third-party data on other Microsoft apps and services, please note that removing this third-party account data in Teams may impact your experiences on other Microsoft apps and services.

Location sharing. You can share your static or live location with individuals or groups within Teams. You are in control and can stop sharing at any time. Sharing location for children is permitted with parental consent and in groups where an adult from the Microsoft family group is present.

Push notifications. To let you know of incoming calls, chats, and other messages, Teams uses the notification service on your device. For many devices, these services are provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Teams has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by the company providing the notification service.

If you do not want to use the notification services for incoming Teams calls and messages, turn it off in the settings found on your device.

OneDrive

OneDrive lets you store and access your files on virtually any device. You can also share and collaborate on your files with others. Some versions of the OneDrive application enable you to access both your personal OneDrive by signing in with your personal Microsoft account and your OneDrive for Business by signing in with your work or school Microsoft account as part of your organization's use of Microsoft 365 or Office 365.

When you use OneDrive, we collect data about your usage of the service, as well as the content you store, to provide, improve, and protect the services. Examples include indexing the contents of your OneDrive documents so that you can search for them later and using location information to enable you to search for photos based on where the photo was taken. We also collect device information so we can deliver personalized experiences, such as enabling you to sync content across devices and roam customized settings.

When you store content in OneDrive, that content will inherit the sharing permissions of the folder in which you store it. For example, if you decide to store content in the public folder, the content will be public and available to anyone on the internet who can find the folder. If you store content in a private folder, the content will be private.

When you share content to a social network like Facebook from a device that you have synced with your OneDrive account, your content is either uploaded to that social network, or a link to that content is posted to that social network. Doing this makes the content accessible to anyone on that social network. To delete the content, you need to delete it from the social network (if it was uploaded there, rather than a link to it) and from OneDrive.

When you share your OneDrive content with your friends via a link, an email with the link is sent to those friends. The link contains an authorization code that allows anyone with the link to access your content. If one of your friends sends the link to other people, they will also be able to access your content, even if you did not choose to share the content with them. To revoke permissions for your content on OneDrive, sign in to your account and then select the specific content to manage the permission levels. Revoking permissions for a link effectively deactivates the link. No one will be able to use the link to access the content unless you decide to share the link again.

Files managed with OneDrive for Business are stored separately from files stored with your personal OneDrive. OneDrive for Business collects and transmits personal data for authentication, such as your email address and password, which will be transmitted to Microsoft and/or to the provider of your Microsoft 365 or Office 365 service.

Outlook

Outlook products are designed to improve your productivity through improved communications and include Outlook.com, Outlook applications, and related services.

Outlook.com. Outlook.com is the primary consumer email service from Microsoft and includes email accounts with addresses that end in outlook.com, live.com, hotmail.com, and msn.com. Outlook.com provides features that let you connect with your friends on social networks. You will need to create a Microsoft account to use Outlook.com.

When you delete an email or item from a mailbox in Outlook.com, the item generally goes into your Deleted Items folder where it remains for approximately 7 days unless you move it back to your inbox, you empty the folder, or the service empties the folder automatically, whichever comes first. When the Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion, unless we are legally required to retain the data for longer.

Outlook applications. Outlook client applications are software you install on your device that permits you to manage email, calendar items, files, contacts, and other data from email, file storage, and other services, like Exchange Online or Outlook.com, or servers, like Microsoft

Exchange. You can use multiple accounts from different providers, including third-party providers, with Outlook applications.

To add an account, you must provide permission for Outlook to access data from the email or file storage services.

When you add an account to Outlook, your mail, calendar items, files, contacts, settings and other data from that account will automatically sync to your device. If you are using the mobile Outlook application, that data will also sync to Microsoft servers to enable additional features such as faster search, personalized filtering of less important mail, and an ability to add email attachments from linked file storage providers without leaving the Outlook application. If you are using the desktop Outlook application, you can choose whether to allow the data to sync to our servers. At any time, you can remove an account or make changes to the data that is synced from your account.

If you add an account provided by an organization (such as your employer or school), the owner of the organizational domain can implement policies and controls (for example, requiring multi-factor authentication or the ability to remotely wipe data from your device) that can affect your use of Outlook.

To learn more about the data the Outlook applications collect and process, please see the [Microsoft 365](#) section of this privacy statement.

Skype

Skype lets you send and receive voice, video, SMS, and instant message communications. This section applies to the consumer version of Skype; if you are using Skype for Business, see the [Enterprise and developer products](#) section of this privacy statement.

As part of providing these features, Microsoft collects usage data about your communications that includes the time and date of the communication and the numbers or user names that are part of the communication.

Skype profile. Your Skype profile includes information you provided when you set up a Microsoft account. To enable other people to find you on Skype (or products that interact with Skype, such as Skype for Business), depending on your profile settings, your Skype profile is included in the Skype public search. Your profile includes your user name, avatar, and any other data you choose to add to your profile or display to others.

Emergency calling in the United States. If you enable location sharing for emergency calling, your location will be periodically collected to enable Microsoft to share your location with emergency calling service providers if you dial 911. Your location information is only shared if you enable location sharing for emergency calling and you initiate a 911 call.

Skype contacts. If you use Outlook.com to manage contacts, Skype will automatically add the people you know to your Skype contact list until you tell the application to stop. With your permission, Skype will sync your device contacts periodically and check for other Skype users

that match contacts in your device or Outlook address books. You are always in control of your contacts and can stop syncing at any time. You can block users if you do not want to receive their communications. If you choose to stop syncing your device contacts, or you are inactive on your device, any contacts that have not been matched during the synchronization process will be deleted from Skype. If you wish to invite any of your device or Outlook contacts to join a conversation, you can invite users to a 1:1 directly, or Microsoft can send an invitation on your behalf via SMS or email for invitations to group conversations. You can block users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Notice to non-user contacts. If your information appears in the device or Outlook address book of a Skype user who chooses to sync their device or Outlook contacts with their Skype contacts, Microsoft may process your data in order to determine whether you are a current Skype user and to allow Skype users to invite you to the service, including via SMS and email. As long as the Skype user continues to be active on Skype on their device and continues to enable contact syncing, your information will be stored on our servers and we will periodically process your information as a part of the Skype user's contact syncing experience to check whether you have subsequently joined Skype.

[Learn more about how we process your information in connection with the contact syncing feature offered to Skype users.](#)

If you do choose to join Skype, you will appear as a suggested new Skype contact for any Skype users with your information in their device or Outlook address books. As a Skype user, you will be able to block other Skype users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Partner companies. To make Skype available to more people, we partner with other companies to allow Skype to be offered via those companies' services. If you use Skype through a company other than Microsoft, that company's privacy policy governs how it handles your data. To comply with applicable law or respond to valid legal process, or to help our partner company or local operator comply or respond, we may access, transfer, disclose, and preserve your data. That data could include, for example, your private content, such as the content of your instant messages, stored video messages, voicemails, or file transfers.

Skype Manager. Skype Manager lets you manage a group's (such as your family's) Skype usage from one central place. When you set up a group, you will be the Skype Manager Administrator and can see the patterns of usage, including detailed information, like traffic data and details of purchases, of other members of the group who have consented to such access. If you add information like your name, other people in the group will be able to see it. Members of the group can withdraw consent for Skype Manager by visiting their [Skype account page](#).

Push notifications. To let you know of incoming calls, chats, and other messages, Skype apps use the notification service on your device. For many devices, these services are provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Skype has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information

in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by the company providing the notification service. If you do not want to use the notification services for incoming Skype calls and messages, turn it off in the settings found in the Skype application or your device.

Translation features. When you use Skype's translation features, Skype collects and uses your conversation to provide the translation service. With your permission, your data may be used to help improve Microsoft products and services. To help the translation and speech recognition technology learn and grow, sentences and automatic transcripts are analyzed and any corrections are entered into our system, to build better performing services. This data may include manual transcription of your voice clips. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#).

Recording features. Some versions of Skype have a recording feature that allows you to capture and share all or part of your audio / video call. The recording will be stored and shared as part of your conversation history with the person or group with whom the call occurred. **You should understand your legal responsibilities before recording any communication. This may include obtaining the prior consent of everyone participating in the conversation or any other authorizations as required.** Microsoft is not responsible for how you use your recordings or the recording features.

Skype bots. Bots are programs offered by Microsoft or third parties that can do many useful things like search for news, play games, and more. Depending on their capabilities, bots may have access to your display name, Skype ID, country, region, language, and any messages, audio, video, or content that you share with the bot. Please review the bot profile and its privacy statement before engaging in a one-to-one or group conversation with a bot. You can delete a bot that you no longer wish to engage with. Prior to adding a bot to a group, please ensure that your group participants have consented to their information being shared with the bot.

Captioning. Certain Skype features include accessibility functionality such as captioning. During Skype calls, a call participant can activate a voice-to-text feature, which allows the user to view the audio chat as text. If a user activates this feature, other call participants will not receive a notification. Microsoft uses this voice and text data to provide captioning of audio for users.

Surface Duo

The Surface Duo is a device featuring two screens that fits in your pocket for productivity on the go. Powered by the Google Android operating system, Surface Duo supports cellular and Wi-Fi connectivity and can be used for email, internet browsing, games, and business connectivity.

Microsoft provides a core Surface Duo experience that runs on the Android operating system. The core Surface Duo experience includes apps such as the Microsoft Launcher, Setup Wizard, and Your Phone Companion. You can sign in with a Google ID and enable various Google

services; you can then also sign in with your Microsoft account (MSA) and enable Microsoft's services. Microsoft apps and services may rely on information provided by Google. Some features, such as location, require that you enable this functionality for Google and separately allow Microsoft to leverage this information.

Diagnostic data. Surface Duo collects diagnostic data to solve problems and to keep the core Surface Duo experience up to date, secure, and operating properly. This data also helps us improve Surface Duo and related Microsoft products and services. The data does not include your user name, email address, or the content of your files. There are two levels of diagnostic data: Required diagnostic data and Optional diagnostic data.

- ♦ **Required.** The minimum data necessary to help keep the core Surface Duo experience secure, up to date, and performing as expected.
- ♦ **Optional.** Additional data that helps us make product improvements and provides enhanced information to help Microsoft detect, diagnose, and remediate issues.

[Learn more in Surface Duo Privacy Settings.](#)

Surface Duo location settings. Surface Duo relies on Google location services to determine the device's precise geographic location to display the local weather. The location of your Surface Duo can be determined with varying degrees of accuracy and may in some cases be determined precisely. If you want Microsoft apps to be able to reference or display weather or other location related information, you need to enable Google location services and Microsoft location access. Some apps may require these settings be enabled independently for the app and can be set or changed in the Surface Duo's Settings. The [Google Privacy Policy](#) provides details about Google's location service and related data privacy practices. See [Surface Duo Location Settings](#) for more information.

Microsoft apps included with the Surface Duo. The diagnostic data options for the core Surface Duo experience are configured when you initially set up your Surface Duo and can be changed in the Surface Duo's Settings under the Diagnostic Data section.

The other Microsoft apps on your Surface Duo may prompt you to enable functionality to enable the full experience of the app or you may be asked to allow optional diagnostic data collection. You can change the settings for these apps in the Surface Duo Settings under the app name. More information about these apps is available in the [Productivity and communications products](#) and [Search, Microsoft Edge, and artificial intelligence](#) sections of this Privacy Statement.

LinkedIn

To learn about the data LinkedIn collects and how it is used and shared, please see LinkedIn's [Privacy Policy](#).

Search, Microsoft Edge, and artificial intelligence

Search and artificial intelligence products connect you with information and intelligently sense, process, and act on information—learning and adapting over time.

Bing

Bing services include search and mapping services, as well as the Bing Toolbar and Bing Desktop apps. Bing services collect and process data in many forms, including text that has been inked or typed, voice data, and images. Bing services are also included within other Microsoft services, such as Microsoft 365, Cortana, and certain features in Windows (which we refer to as Bing-powered experiences).

When you conduct a search, or use a feature of a Bing-powered experience that involves conducting a search or entering a command on your behalf, Microsoft will collect the searches or commands you provide (which may be in the form of text, voice data, or an image), along with your IP address, location, the unique identifiers contained in our cookies or similar technologies, the time and date of your search, and your browser configuration. For example, if you use Bing voice-enabled services, your voice input and performance data associated with the speech functionality will be sent to Microsoft. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#). And, if you use Bing image-enabled services, the image you provide will be sent to Microsoft. When you use Bing-powered experiences, such as Bing Lookup to search a particular word or phrase within a webpage or document, that word or phrase is sent to Bing along with some surrounding content in order to provide contextually relevant search results.

Search suggestions. For the search suggestions feature, the characters that you type into a Bing-powered experience (such as search and site suggestions in the Microsoft Edge browser) to conduct a search and what you click on will be sent to Microsoft. This allows us to provide you with relevant suggestions as you type your searches. To turn this feature on or off, while using Bing Search, go to [Bing Settings](#). There are other methods to control this feature in other Bing-powered experiences, such as the Microsoft Edge browser. Search Suggestions cannot be turned off in the search box in Windows 10 and Windows 11. If you choose, you can always hide the search box or icon on the taskbar.

Bing experience improvement program for Bing Desktop and Bing Toolbar. If you are using Bing Desktop or Bing Toolbar and choose to participate in the Bing Experience Improvement Program, we also collect additional data about how you use these specific Bing apps, such as the addresses of the websites you visit, to help improve search ranking and relevance. To help protect your privacy, we do not use the data collected through the Bing Experience Improvement Program to identify or contact you or target advertising to you. You can turn off the Bing Experience Improvement Program at any time in the Bing Desktop or Bing Toolbar settings. Finally, we delete the information collected through the Bing Experience Improvement Program after 18 months.

Retention and de-identification. We de-identify stored search queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers that are used to identify a particular account or device after 18 months.

Personalization through Microsoft account. Some Bing services provide you with an enhanced experience when you sign in with your personal Microsoft account, for example, syncing your search history across devices. You can use these personalization features to customize your interests, favorites, and settings, and to connect your account with third-party services. Visit [Bing Settings](#) to manage your personalization settings, or the [Microsoft privacy dashboard](#) to manage your data.

Managing search history. When you're signed-in to a personal Microsoft account, you can erase your search history on the [Microsoft privacy dashboard](#). The Search History service from Bing, located in Bing Settings, provides another method of revisiting the search terms you've entered and results you've clicked when using Bing search through your browser. You may clear your search history on a device through this service. Clearing your history prevents that history from being displayed on the Search History site, but does not delete information from our search logs, which are retained and de-identified as described above or as you have instructed through the privacy dashboard. If you are signed-in to a work or school Microsoft account using Microsoft Search in Bing, you can export your Microsoft Search in Bing search history, but you cannot delete it. Your Microsoft Search in Bing service administrator can see aggregated search history across all enterprise users but cannot see specific searches by user.

Third-party services that use Bing. You may access Bing-powered experiences when using third-party services, such as those from Yahoo!. In order to provide these services, Bing receives data from these and other partners, including your search query and related data (such as date, time, IP address, and a unique identifier). This data will be sent to Microsoft to provide the search service. Microsoft will use this data as described in this statement or as further limited by our contractual obligations with our partners. You should refer to the privacy policies of the third-party services for any questions about how they collect and use data.

Data passed to destination website. When you select a search result or advertisement from a Bing search results page and go to the destination website, the destination website will receive the standard data your browser sends to every web site you visit—such as your IP address, browser type and language, and the host name of the site you came from (in this case, <https://www.bing.com/>).

Sharing data from Bing and Bing-powered experiences with third parties. We share some de-identified data (data where the identity of a specific person is not known) from Bing and Bing-powered experiences with selected third parties. Before we do so, we run the data through a process designed to remove certain sensitive data that users may have included in the search terms themselves (such as social security numbers or credit card numbers). Additionally, we require these third parties to keep the data secure and to not use the data for purposes other than for which it is provided.

Cortana

Cortana is your personal productivity assistant in Microsoft 365. As a digital assistant, Cortana is designed to help you achieve more with less effort so you can focus on what matters and can answer a wide range of questions about things such as weather, sports, stocks, and

general information. When you ask questions, the data Cortana collects depends on whether you are using the consumer or enterprise version.

This section applies to the consumer version of Cortana experiences in Windows 10 and Windows 11. If you are using Cortana with an account provided by an organization, such as a work or school account, see the [Notice to end users](#) section of this privacy statement. [Learn more about the enterprise version of Cortana in Microsoft 365](#).

When you ask Cortana a question, whether you are speaking or typing, Cortana collects that question as a text string. To answer your questions Cortana uses the Bing service. For information about the data Bing collects, see the [Bing](#) section of this privacy statement.

By default, if you speak your question, Cortana also collects speech transcription data and does not collect voice clips. You have the option to provide your consent and allow Microsoft to collect voice clips. If you choose to opt in and allow Microsoft to collect voice clips, the voice clip files are stored and anonymized and will not be associated with your Microsoft account or any other Microsoft IDs. This anonymous data is used to improve the product. For more information about Microsoft and your voice data, see the [Speech Recognition Technologies](#) section of this privacy statement.

Cortana legacy. Cortana in Windows 10 version 1909 and earlier collects user query data (a text transcription of the question the user asked), which is anonymized and used for product maintenance. Cortana in Windows 10 version 1909 also uses the Bing service to answer your questions. For information about the data Bing collects, see the [Bing](#) section of the Privacy Statement.

[Learn more about Cortana and privacy](#).

Microsoft Edge

Whenever you use a web browser to access the internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address, browser type and language, access times, and referring website addresses. This data might be logged on those websites' or online services' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use. Certain features in Microsoft Edge, such as when you open a new tab in the browser, connect you to MSN Content and your experiences with such content is covered by the MSN section of this privacy statement. Additionally, Microsoft Edge sends a unique browser ID to certain websites to enable us to develop aggregate data used to improve browser features and services.

Microsoft Edge for Windows, Linux, and macOS. Microsoft Edge is the default web browser for Windows 10 and later and is also available on other supported versions of Windows and macOS.

Data about how you use your browser, such as your browsing history, web form data, temporary internet files, and cookies, is stored on your device. You can delete this data from

your device using Clear Browsing History.

Microsoft Edge allows you to capture and save content on your device, such as:

- ♦ **Settings and More.** Allows you to manage your favorites, downloads, history, extensions, and collections.
- ♦ **Collections.** Allows you to collect text, images, videos, and other content in a note page in your browser. When you drag content into your collection, it is cached on your device and can be deleted through your collection.
- ♦ **Website Pin to Taskbar.** Allows you to pin your favorite websites to the Windows taskbar. Websites will be able to see which of their webpages you have pinned, so they can provide you a notification badge letting you know there is something new for you to check out on their websites.

Microsoft collects data necessary to provide features you request in Microsoft Edge. For example, you may choose to sync browser information saved on your device across other devices when you are signed in with your Microsoft account. You may choose which browser data to sync, including your favorites, browsing history, extensions and associated data, settings, open tabs, autofill form entries (such as your name, address, and phone number), passwords, payment information, and other data types as they become available. If you choose to sync extensions that you acquired from third-party web stores, a copy of those extensions will be downloaded directly from those web stores on your synced device(s). If you have turned on Password Monitor, your saved credentials are hashed, encrypted and sent to Microsoft's Password Monitor service to warn you if your credentials were detected as part of a malicious attack or a breach. Microsoft does not retain this data after the check is complete. You can disable or configure syncing in the Microsoft Edge settings.

Microsoft Edge's **Search and site suggestions** uses your search queries and browsing history to provide you with faster browsing and more relevant search recommendations. Microsoft Edge sends the information you type into the browser address bar to the default search provider configured in the address bar to offer search recommendations as you type each character. You can turn off these features at any time in the browser settings. In order to provide search results, Microsoft Edge sends your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the Bing section of this privacy statement.

Microsoft Edge collects and uses data from your search activity across the web, including websites Microsoft does not own or operate, to improve Microsoft services, such as Microsoft Edge, Microsoft Bing and Microsoft News. This data may include the search query, the search results that are displayed to you, demographic information that is part of the search results, and the interaction you have with those search results, such as the links you click. Microsoft Edge takes steps to de-identify the data it collects by removing data that identifies the person or device from which it was collected and retains this data for one year from when it is collected. Microsoft does not use this collected data to personalize or provide ads to you. You can turn off the collection of this data at any time in the browser settings.

Microsoft Edge downloads content from Microsoft services to enhance your browsing experiences; for example, when data is downloaded to prerender site content for faster browsing or to provide content required to power features you choose to use, such as providing templates for Collections.

You may also choose to share your Microsoft Edge browsing activity to allow us to personalize Microsoft Edge and Microsoft services like ads, search, shopping, and news. Microsoft Edge browsing activity includes your history, favorites, usage data, and other browsing data. For more information about our **advertising privacy policies** see the Advertising section of the privacy statement. In the Microsoft privacy dashboard you can control the use of your browsing activity for personalized ads in the **See ads that interest you** setting. If you disable this setting in the Microsoft privacy dashboard you will continue to receive personalized web experiences like search and news based on your browsing activity if you have **Allow Microsoft to use your browsing activity including history, favorites, usage and other browsing data to personalize Microsoft Edge and Microsoft services like ads, search, shopping and news** turned on in Microsoft Edge settings. You may disable this browser setting in Microsoft Edge at any time to stop receiving personalized web experiences based on your browsing activity.

Microsoft Edge collects required diagnostic data to solve problems and to keep Microsoft Edge up to date, secure, and operating properly. Required diagnostic data also helps us improve Microsoft Edge and Windows.

Separate from your search activity data mentioned above, you can choose to send optional diagnostic data about how you use Microsoft Edge and information about your browser activity, including browsing history and search terms to Microsoft to help us improve Microsoft Edge and other Microsoft products and services. For Microsoft Edge on Windows 10 and later, this information is provided when you have enabled optional diagnostic data. For details, see the Windows Diagnostics section of the privacy statement. For Microsoft Edge on other operating systems, optional diagnostic information is provided when you enable **Improve Microsoft products by sending data about how you use the browser** or **Make searches and Microsoft products better by sending info about websites you visit in Microsoft Edge** in the browser settings.

The diagnostic data collected by Microsoft Edge is transmitted to Microsoft and is stored with one or more unique identifiers that help us recognize an individual browser installation on a device and understand the browser's service issues and use patterns.

[Learn more about Microsoft Edge, browsing data, and privacy.](#)

Microsoft Edge on iOS and Android. Microsoft Edge on iOS and Android devices collects data necessary to provide features you request in Microsoft Edge. Microsoft also collects required diagnostic data to solve problems and to keep Microsoft Edge up to date, secure, and operating properly. Required diagnostic data also helps us improve Microsoft Edge.

Additionally, you may share optional diagnostic data about how you use Microsoft Edge and information about websites you visit (browsing history) for personalized experiences on your browser, Windows, and other Microsoft products and services. This information also helps us

improve Microsoft Edge and other Microsoft products and services. This optional diagnostic data is sent to us when you enable **Share usage data for personalization** or **Share info about websites you visit** in the browser settings.

The diagnostic data collected by Microsoft Edge is transmitted to Microsoft and is stored with one or more unique identifiers that help us recognize an individual user on a device and understand the browser's service issues and use patterns.

For information about the privacy practices of legacy versions Microsoft Edge (versions 44 and below), see the Web browsers—Microsoft Edge Legacy and Internet Explorer section of the privacy statement.

Microsoft Translator

Microsoft Translator is a machine translation system and service designed to automatically translate text and voice input between numerous supported languages. Microsoft Translator is made available as a stand-alone consumer app for Android, iOS, and Windows and its service capabilities are also integrated in a variety of Microsoft products and services, such as Translator Hub, Translator for Bing, and Translator for Microsoft Edge. Microsoft Translator processes the text, image, and voice data you submit, as well as device and usage data. We use this data to provide Microsoft Translator, personalize your experiences, and improve our products and services. Microsoft has implemented business and technical measures designed to help de-identify the data you submit to Microsoft Translator. For example, when we randomly sample text and audio to improve Microsoft Translator and Microsoft's speech recognition technologies, we delete identifiers and certain text, such as email addresses and some number sequences, detected in the sample that could contain personal data. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#).

Separate from Microsoft Translator, Microsoft translation services are available as features in other Microsoft products and services that have different privacy practices than Microsoft Translator. For more information on the Microsoft Azure Cognitive Services Translator Text API, Custom Translator, and Translator Speech API, see the [Enterprise and developer products](#) section of this privacy statement. For the Translate feature in Office apps and Skype, see the [Productivity and communications products](#) section of this privacy statement.

SwiftKey

The Microsoft Swiftkey keyboard and related cloud-based services (collectively, the "SwiftKey Services") process data about words you use and how you type and use this data to learn your writing style and provide personalized autocorrection and predictive text that adapts to you. We also use this data to offer a range of other features, such as hashtag and emoji predictions.

SwiftKey prediction technology learns from the way you use language to build a personalized language model. This model is an optimized view of the words and phrases that you use most

often in context and reflects your unique writing style. The model itself contains the words you commonly type arranged in a way that enables SwiftKey's algorithms to make predictions, based on text you have already entered. The model draws from all scenarios in which you use your keyboard, including when you type while using apps or visiting websites. The SwiftKey keyboard and model attempt to avoid collecting sensitive data, by not collecting data from certain fields such as those recognized as containing password or payment data. SwiftKey Services do not log, store, or learn from data you type, or the data contained in your model, unless you choose to share your data with us (as described further below). When you use SwiftKey Services, we also collect device and usage data. We use de-identified device and usage data to analyze service performance and help improve our products.

The SwiftKey Services also include an optional cloud component called a SwiftKey Account. If you choose to create a SwiftKey Account, your language model will be synced with the SwiftKey Account cloud service, so you can benefit from that model on the different devices you use and access additional services such as prediction synchronization and backup. When you create a SwiftKey Account, Microsoft will also collect your email address and basic demographic data. All data collected is transferred to our servers over encrypted channels.

You may also opt in to share your language, typing data, and/or voice clips for the purposes of improving Microsoft products and services. Depending on the opt-ins you choose, SwiftKey may send short snippets of data about what and how you type and/or your voice clips, and related correction data to our servers for processing. These text snippets and/or voice clips are used in various automated processes to validate that our prediction services are working correctly and to make product improvements. To preserve your privacy, SwiftKey Services de-identify these text snippets, and even if you have a SwiftKey Account, these text snippets and/or voice clips will not be linked to it. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#).

If you sign into your SwiftKey Account and opt to share your language and typing data or voice clips, Microsoft will process your shared data in order to look for new patterns of language usage across our user base. This allows us to improve our basic models for individual languages. Language and typing data used in this process is aggregated and any words or combinations of words that might be personal to individuals or small groups of users are filtered out.

You can withdraw your consent to share your language and typing data or voice clips for product improvement at any time in SwiftKey Settings. You can also withdraw your consent for SwiftKey Services to retain your personal data in SwiftKey Settings. When you withdraw consent for SwiftKey to retain your personal data, all personal data collected through your use of the SwiftKey Services will be deleted.

You may receive occasional notifications on your device alerting you to product updates and features that may be of interest to you. You can disable these notifications at any time in the SwiftKey Settings.

Windows

Windows is a personalized computing environment that enables you to seamlessly roam and access services, preferences, and content across your computing devices from phones to tablets to the Surface Hub. Rather than residing as a static software program on your device, key components of Windows are cloud-based, and both cloud and local elements of Windows are updated regularly, providing you with the latest improvements and features. In order to provide this computing experience, we collect data about you, your device, and the way you use Windows. And because Windows is personal to you, we give you choices about the personal data we collect and how we use it. Note that if your Windows device is managed by your organization (such as your employer or school), your organization may use centralized management tools provided by Microsoft or others to access and process your data and to control device settings (including privacy settings), device policies, software updates, data collection by us or the organization, or other aspects of your device. Additionally, your organization may use management tools provided by Microsoft or others to access and process your data from that device, including your interaction data, diagnostic data, and the contents of your communications and files. For more information about data collection in Windows, see [Data collection summary for Windows](#). This statement discusses Windows 10 and Windows 11 and references to Windows in this section relate to those product versions. Earlier versions of Windows (including Windows Vista, Windows 7, Windows 8, and Windows 8.1) are subject to their own privacy statements.

Activation

When you activate Windows, a specific product key is associated with the device on which your software is installed. The product key and data about the software and your device is sent to Microsoft to help validate your license to the software. This data may be sent again if there is a need to re-activate or validate your license. On phones running Windows, device and network identifiers, as well as device location at the time of the first power-up of the device, are also sent to Microsoft for the purpose of warranty registration, stock replenishment, and fraud prevention.

Activity history

Activity history helps keep track of the things you do on your device, such as the apps and services you use, the files you open, and the websites you browse. Your activity history is created when using different apps and features such as Microsoft Edge Legacy, some Microsoft Store apps, and Microsoft 365 apps and is stored locally on your device. If you've signed in to your device with a work or school account and give your permission, Windows sends your activity history to Microsoft. Once your activity history is in the cloud, Microsoft uses that data to enable cross-device experiences, to provide you with the ability to continue those activities on other devices, to provide personalized experiences (such as ordering your activities based on duration of use) and relevant suggestions (such as anticipating what your needs might be based on your activity history), and to help improve Microsoft products.

You can turn settings off or on for sending your activity history to Microsoft and storing activity history locally on your device, and you can also clear your device's activity history at

any time by going to **Privacy > Activity history** in the Windows settings app. [Learn more about activity history in Windows.](#)

Advertising ID

Windows generates a unique advertising ID for each person using a device, which app developers and advertising networks can then use for their own purposes, including providing relevant advertising in apps. When the advertising ID is enabled, both Microsoft apps and third-party apps can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. Thus, your advertising ID can be used by app developers and advertising networks to provide more relevant advertising and other personalized experiences across their apps and on the web. Microsoft collects the advertising ID for the uses described here only when you choose to enable the advertising ID as part of your privacy setting.

The advertising ID setting applies to Windows apps using the Windows advertising identifier. You can turn off access to this identifier at any time by turning off the advertising ID in the Windows settings app. If you choose to turn it on again, the advertising ID will be reset and a new identifier will be generated. When a third-party app accesses the advertising ID, its use of the advertising ID will be subject to its own privacy policy. [Learn more about advertising ID in Windows.](#)

The advertising ID setting does not apply to other methods of interest-based advertising delivered by Microsoft or third parties, such as cookies used to provide interest-based display ads on websites. Third-party products accessed through or installed on Windows may also deliver other forms of interest-based advertising subject to their own privacy policies. Microsoft delivers other forms of interest-based ads in certain Microsoft products, both directly and by partnering with third-party ad providers. For more information on how Microsoft uses data for advertising, see the [How we use personal data](#) section of this statement.

Diagnostics

Microsoft collects Windows diagnostic data to solve problems and to keep Windows up to date, secure, and operating properly. It also helps us improve Windows and related Microsoft products and services and, for customers who have turned on the “Tailored experiences” setting, to provide more relevant tips and recommendations to tailor Microsoft and third-party products and services for Windows to the customer’s needs. This data is transmitted to Microsoft and stored with one or more unique identifiers that can help us recognize an individual user on an individual device and understand the device’s service issues and use patterns.

There are two levels of diagnostic and activity data: Required diagnostic data and Optional diagnostic data. Certain product documentation and other materials refer to Required

diagnostic data as Basic diagnostic data and to Optional diagnostic data as Full diagnostic data.

If an organization (such as your employer or school) uses Azure Active Directory (AAD) to manage the account it provides to you and enrolls your device in the Windows diagnostic data processor configuration, Microsoft's processing of diagnostic data in connection with Windows is governed by a contract between Microsoft and the organization. If an organization uses Microsoft management tools or engages Microsoft to manage your device, Microsoft and the organization will use and process diagnostic and error data from your device to allow the management, monitoring, and troubleshooting of your devices managed by the organization, and for other purposes of the organization.

Required diagnostic data includes information about your device, its settings and capabilities, and whether it is performing properly. We collect the following Required diagnostic data:

- ◆ Device, connectivity, and configuration data:
 - Data about the device such as the processor type, OEM manufacturer, type of battery and capacity, number and type of cameras, firmware, and memory attributes.
 - Network capabilities and connection data such as the device's IP address, mobile network (including IMEI and mobile operator), and whether the device is connected to a free or paid network.
 - Data about the operating system and its configuration such as the OS version and build number, region and language settings, diagnostics data settings, and whether the device is part of the Windows Insider program.
 - Data about connected peripherals such as model, manufacturer, drivers, and compatibility data.
 - Data about the applications installed on the device such as application name, version, and publisher.
- ◆ Whether a device is ready for an update and whether there are factors that may impede the ability to receive updates, such as low battery, limited disk space, or connectivity through a paid network.
- ◆ Whether updates complete successfully or fail.
- ◆ Data about the reliability of the diagnostics collection system itself.
- ◆ Basic error reporting, which is health data about the operating system and applications running on your device. For example, basic error reporting tells us if an application, such as Microsoft Paint or a third-party game, hangs or crashes.

Optional diagnostic data includes more detailed information about your device and its settings, capabilities, and device health. Optional diagnostic data also includes data about the websites you browse, device activity (also sometimes referred to as usage), and enhanced error reporting that helps Microsoft to fix and improve products and services for all users. When you choose to send Optional diagnostic data, Required diagnostic data will always be included, and we collect the following additional information:

- ◆ Additional data about the device, connectivity, and configuration, beyond that collected under Required diagnostic data.
- ◆ Status and logging information about the health of operating system and other system components beyond that collected about the update and diagnostics systems under Required diagnostic data.
- ◆ App activity, such as which programs are launched on a device, how long they run, and how quickly they respond to input.
- ◆ Browser activity, including browsing history and search terms, in Microsoft browsers (Microsoft Edge or Internet Explorer).
- ◆ Enhanced error reporting, including the memory state of the device when a system or app crash occurs (which may unintentionally contain user content, such as parts of a file you were using when the problem occurred). Crash data is never used for Tailored experiences as described below.

Some of the data described above may not be collected from your device even if you choose to send Optional diagnostic data. Microsoft minimizes the volume of Optional diagnostic data it collects from all devices by collecting some of the data from only a subset of devices (sample). By running the Diagnostic Data Viewer tool, you can see an icon which indicates whether your device is part of a sample and also which specific data is collected from your device. Instructions for how to download the Diagnostic Data Viewer tool can be found in the Windows settings app under Diagnostics & feedback.

Specific data items collected in Windows diagnostics are subject to change to give Microsoft flexibility to collect the data needed for the purposes described. For example, to enable Microsoft to troubleshoot the latest performance issue impacting users' computing experience or update a Windows device that is new to the market, Microsoft may need to collect data items that were not collected previously. For a current list of data types collected at **Required diagnostic data** and **Optional diagnostic data**, see [Windows Required \(Basic level\) diagnostic events and fields](#) or [Windows Optional \(Full level\) diagnostic data](#). We provide limited portions of error report information to partners (such as the device manufacturer) to help them troubleshoot products and services which work with Windows and other Microsoft product and services. They are only permitted to use this information to repair or improve those products and services. We may also share some aggregated, de-identified diagnostic data, such as general usage trends for Windows apps and features, with selected third parties. [Learn more about diagnostic data in Windows.](#)

Inking and typing Recognition. You also can choose to help Microsoft improve inking and typing recognition by sending inking and typing diagnostic data. If you choose to do so, Microsoft will collect samples of the content you type or write to improve features such as handwriting recognition, autocompletion, next word prediction, and spelling correction in the many languages used by Microsoft customers. When Microsoft collects inking and typing diagnostic data, it is divided into small samples and processed to remove unique identifiers, sequencing information, and other data (such as email addresses and numeric values) which could be used to reconstruct the original content or associate the input to you. It also includes associated performance data, such as changes you manually make to text, as well as words you've added to the dictionary. [Learn more about improving inking and typing in Windows.](#)

If you choose to turn on **Tailored experiences**, we will use your Windows diagnostic data (Required or Optional as you have selected) to offer you personalized tips, ads, and recommendations to enhance Microsoft experiences. If you have selected Required as your diagnostic data setting, personalization is based on information about your device, its settings and capabilities, and whether it is performing properly. If you have selected Optional, personalization is also based on information about how you use apps and features, plus additional information about the health of your device. However, we do not use information about the websites you browse, the content of crash dumps, speech, typing, or inking input data for personalization when we receive such data from customers who have selected Optional.

Tailored experiences include suggestions on how to customize and optimize Windows, as well as ads and recommendations for Microsoft and third-party products and services, features, apps, and hardware for your Windows experiences. For example, to help you get the most out of your device, we may tell you about features you may not know about or that are new. If you are having a problem with your Windows device, you may be offered a solution. You may be offered a chance to customize your lock screen with pictures, or to be shown more pictures of the kind you like, or fewer of the ones you do not. If you stream movies in your browser, you may be recommended an app from the Microsoft Store that streams more efficiently. Or, if you are running out of space on your hard drive, Windows may recommend you try OneDrive or purchase hardware to gain more space. [Learn more about tailored experiences in Windows.](#)

Feedback Hub

Feedback Hub is a preinstalled app that provides a way to gather feedback on Microsoft products and installed first party and third-party apps. You can sign into Feedback Hub using either your personal Microsoft account or an account provided by your organization (such as your employer or school) that you use to sign into Microsoft products. Signing in with your work or school account allows you to submit feedback to Microsoft in association with your organization.

Any feedback you provide whether using your work or school account or personal Microsoft account may be publicly viewable depending on the settings configured by your organization's administrators. Additionally, if feedback is provided using your work or school account, your feedback can be viewed through the Feedback Hub by your organization's administrators.

When you submit feedback to Microsoft about a problem or add more details to a problem, diagnostic data will be sent to Microsoft to improve Microsoft products and services. Depending on your Diagnostic data settings in the **Diagnostics & feedback** section of the Windows settings app, Feedback Hub will either send diagnostic data automatically or you will have the option to send it to Microsoft at the time you provide feedback. Based on the category chosen when submitting feedback, there may be additional personal data collected that helps to further troubleshoot issues; for example, location related information when submitting feedback about location services or gaze related information when submitting feedback on Mixed Reality. Microsoft may also share your feedback along with the data

collected when you submit your feedback with Microsoft partners (such as a device manufacturer, or firmware developer) to help them troubleshoot products and services that work with Windows and other Microsoft products and services. [Learn more about diagnostic data in Windows.](#)

Location services and recording

Windows location service. Microsoft operates a location service that helps determine the precise geographic location of a specific Windows device. Depending on the capabilities of the device, the device's location can be determined with varying degrees of accuracy and may in some cases be determined precisely. When you have enabled location on a Windows device, or you have given permission for Microsoft apps to access location information on non-Windows devices, data about cell towers and Wi-Fi access points and their locations is collected by Microsoft and added to the location database after removing any data identifying the person or device from which it was collected. This de-identified location information is used to improve Microsoft's location services and, in some instances, shared with our location service provider partners, currently HERE (see <https://www.here.com/>) and Skyhook (see <https://www.skyhook.com>) to improve the location services of the provider.

Windows services and features, apps running on Windows, and websites opened in Windows browsers can access the device's location through Windows if your settings allow them to do so. Some features and apps request location permission when you first install Windows, some ask the first time you use the app, and others ask every time you access the device's location. For information about certain Windows apps that use the device's location, see the [Windows apps](#) section of this privacy statement.

When an app or feature accesses the device's location and you are signed in with a Microsoft account, your Windows device will also upload its location to the cloud where it is available across your devices to other apps or services that use your Microsoft account and for which you've granted permission. We will retain only the last known location (each new location replaces the previous one). Data about a Windows device's recent location history is also stored on the device even if not using a Microsoft account, and certain apps and Windows features can access this location history. You can clear your device's location history at any time in the Windows settings app.

In the Windows settings app, you can also view which apps have access to the device's precise location or your device's location history, turn off or on access to the device's location for particular apps, or turn off access to the device's location. You can also set a default location, which will be used when the location service can't detect a more exact location for your device.

Even when you've turned off access to the device's location, some third-party desktop apps and services could use other technologies (such as Bluetooth, Wi-Fi, cellular modem, etc.) to determine the device's precise location. [Learn more about third-party desktop apps and how they may still be able to determine your device's location when the device's location setting is off.](#)

In addition, to facilitate getting help in an emergency, whenever you make an emergency call, Windows will attempt to determine and share your precise location, regardless of your location settings. If your device has a SIM card or is otherwise using cellular service, your mobile operator will have access to your device's location. [Learn more about location in Windows.](#)

General Location. If you turn on Location services, apps that cannot use your precise location may still have access to your general location, such as your city, postal code, or region.

Find my device. The Find my device feature allows an administrator of a Windows device to find the location of that device from account.microsoft.com/devices. To enable Find my device, an administrator needs to be signed in with a Microsoft account and have the location setting enabled. This feature will work even if other users have denied access to location for all their apps. When the administrator attempts to locate the device, users will see a notification in the notification area. [Learn more about Find my device in Windows.](#)

Recording. Some Windows devices have a recording feature that allows you to capture audio and video clips of your activity on the device, including your communications with others. If you choose to record a session, the recording will be saved locally on your device. In some cases, you may have the option to transmit the recording to a Microsoft product or service that broadcasts the recording publicly. **Important: You should understand your legal responsibilities before recording and/or transmitting any communication. This may include obtaining the prior consent of everyone participating in the conversation or any other authorizations as required.** Microsoft is not responsible for how you use recording features or your recordings.

Phone Link

The Phone Link app lets you link your Android phone with your Windows device, enabling a variety of cross-device experiences. You can use Phone Link to see recent photos from your Android phone on your Windows device; make and receive calls from your Android phone on your Windows device; view and send text messages from your Windows device; view, dismiss, or perform other actions to your Android phone notifications from your Windows device; and share your phone screen on your Windows device through Phone Link's mirroring function.

To use Phone Link, the Phone Link app must be installed on your Windows device and the Link to Windows app must be installed on your Android phone. Upon launching the Phone Link app on your Windows device, you will be prompted to provide your mobile phone number. We use this mobile phone number solely to send you a link with information about downloading the Link to Windows app.

To use Phone Link, you must log into your Microsoft account on the Phone Link app on your Windows device and on the Link to Windows app on your Android phone. Your Android phone must be connected to Wi-Fi and your Windows device must be connected to the internet and permit Phone Link to run in the background. To use Phone Link's mirroring

function, your Android phone must also have Bluetooth enabled. Phone Link also requires your Windows device to be set up with Windows Hello, as an additional security measure.

As part of providing Phone Link's features to you, Microsoft collects performance, usage, and device data that includes, for example, the hardware capabilities of your mobile phone and Windows device, the number and duration of your sessions on Phone Link, and the amount of time you spent during setup.

You can unlink your Android phone from your Windows device at any time by logging in with your Microsoft account at accounts.microsoft.com/devices and updating the Settings on your Android phone. For detailed information, see [our support page](#).

Text Messages. Phone Link allows you to view text messages delivered to your Android phone on your Windows device and send text messages from your Windows device. Only text messages received and sent within the last 30 days are visible on your Windows device. These text messages are temporarily stored on your Windows device. We never store your text messages on our servers or change or delete any text messages on your Android phone. You can see messages sent via SMS (Short Message Service) and MMS (Multimedia Messaging Service) but not messages sent via RCS (Rich Communication Services). To provide this functionality, Phone Link accesses the content of your text messages and the contact information of the individuals or businesses from whom you are receiving or sending text messages.

Calls. Phone Link allows you to make and receive calls from your Android phone on your Windows device. Through Phone Link, you can also view your recent calls on your Windows device. To activate this feature, you must enable certain permissions on both your Windows device and Android phone, such as call logs access and permission to make phone calls from your PC. These permissions can be revoked at any time under the Phone Link Settings page on your Windows device and your Android phone's settings. Only calls received and dialed within the last 30 days are visible under call logs on your Windows device. These call details are temporarily stored on your Windows device. We do not change or delete your call history on your Android phone.

Photos. Phone Link allows you to copy, share or edit photos from your Android phone on your Windows device. Only a limited number of your most recent photos from the Camera Roll and Screenshots folders on your Android phone will be visible on your Windows device at any given time. These photos are temporarily stored on your Windows device and as you take more photos on your Android phone, we remove the temporary copies of the older photos from your Windows device. We never store your photos on our servers or change or delete any photos on your Android phone.

Notifications. Phone Link allows you to view your Android phone's notifications on your Windows device. Through Phone Link, you can read and dismiss your Android phone's notifications from your Windows device or perform other actions related to the notifications. To activate this Phone Link feature, you must enable certain permissions, such as sync notifications, on both your Windows device and Android phone. These permissions can be revoked at any time under the Phone Link Settings page on your Windows device and your Android phone's settings. For detailed information, see [our support page](#).

Mirroring. Phone Link allows you to view your Android phone's screen on your Windows device. Your Android phone screen will be visible on your Windows device as a pixel stream and any audio that you enable on your Android phone screen while it is linked to your Windows device through Phone Link will play through your Android phone.

Text-to-voice. Phone Link features include accessibility functionality such as text-to-voice. You can activate a text-to-voice feature, which allows you to hear the contents of a text message or notification as audio. If you activate this feature, your text messages and notifications will be read out loud as they are received.

Security and safety features

Device encryption. Device encryption helps protect the data stored on your device by encrypting it using BitLocker Drive Encryption technology. When device encryption is on, Windows automatically encrypts the drive Windows is installed on and generates a recovery key. The BitLocker recovery key for your personal device is automatically backed up online in your personal Microsoft OneDrive account. Microsoft doesn't use your individual recovery keys for any purpose.

Malicious Software Removal Tool. The Malicious Software Removal Tool (MSRT) runs on your device at least once per month as part of Windows Update. MSRT checks devices for infections by specific, prevalent malicious software ("malware") and helps remove any infections found. When the MSRT runs, it will remove the malware listed on the Microsoft Support website if the malware is on your device. During a malware check, a report will be sent to Microsoft with specific data about malware detected, errors, and other data about your device. If you do not want MSRT to send this data to Microsoft, you can disable MSRT's reporting component.

Microsoft Family. Parents can use Microsoft Family to understand and set boundaries on how their child is using their device. There are many features available to Family members, so please carefully review the information provided when you create or join a Family. If you live in a region that requires permission to create an account to access Microsoft services, you may be prompted to request or give parental consent. If a user is under the statutory age in your region, during the registration process they will be prompted to request consent from a parent or guardian by entering an adult's email. When Family activity reporting is turned on for a child, Microsoft will collect details about how the child uses their device and provide parents with reports of that child's activities. Activity reports are routinely deleted from Microsoft servers after a short period of time.

Microsoft Defender SmartScreen. Microsoft Defender SmartScreen helps protect you when using our services by checking downloaded files and web content for malicious software, potentially unsafe web content, and other threats to you or your device. When checking a file, data about that file is sent to Microsoft, including the file name, a hash of the file's contents, the download location, and the file's digital certificates. If Microsoft Defender SmartScreen identifies the file as unknown or potentially unsafe, you will see a warning prior to opening the file. When checking web content, data about the content and your device is sent to Microsoft,

including the full web address of the content. If Microsoft Defender SmartScreen detects that content is potentially unsafe, you will see a warning in place of the content. Microsoft Defender SmartScreen can be turned on or off in Settings.

Microsoft Defender Antivirus. Microsoft Defender Antivirus looks for malware and other unwanted software, potentially unwanted apps, and other malicious content on your device. Microsoft Defender Antivirus is automatically turned on to help protect your device if no other antimalware software is actively protecting your device. If Microsoft Defender Antivirus is turned on, it will monitor the security status of your device. When Microsoft Defender Antivirus is turned on, or is running because Limited Periodic Scanning is enabled, it will automatically send reports to Microsoft that contain data about suspected malware and other unwanted software, potentially unwanted apps, and other malicious content, and it may also send files that could contain malicious content, such as malware or unknown files for further inspection. If a report is likely to contain personal data, the report is not sent automatically, and you'll be prompted before it is sent. You can configure Microsoft Defender Antivirus not to send reports and suspected malware to Microsoft.

Speech, Voice Activation, Inking, and Typing

Speech. Microsoft provides both a device-based speech recognition feature and cloud-based (online) speech recognition technologies.

Turning on the Online speech recognition setting lets apps use Microsoft cloud-based speech recognition. Additionally, in Windows 10, the Online speech recognition setting enables your ability to use dictation within Windows.

Turning on speech while setting up a HoloLens device or installing Windows Mixed Reality allows you to use your voice for commands, dictation, and app interactions. Both device-based speech recognition and online speech recognition settings will be enabled. With both settings enabled, while your headset is turned on the device will always be listening to your voice input and will send your voice data to Microsoft's cloud-based speech recognition technologies.

When you use cloud-based speech recognition technologies from Microsoft, whether enabled by the Online speech recognition setting or when you interact with HoloLens or voice typing, Microsoft collects and uses your voice recordings to provide the speech recognition service by creating a text transcription of the spoken words in the voice data. Microsoft will not listen to your voice recording without your permission. To learn more about how Microsoft manages your voice data, see [Speech recognition technologies](#).

You can use device-based speech recognition without sending your voice data to Microsoft. However, Microsoft cloud-based speech recognition technologies provide more accurate recognition than the device-based speech recognition. When the online speech recognition setting is turned off, speech services that do not rely on the cloud and only use device-based recognition—like the Narrator app or the Windows Speech Recognition app—will still work and Microsoft won't collect any voice data.

You can turn off online speech recognition at any time. This will stop any apps that rely on the Online speech recognition setting from sending your voice data to Microsoft. If you are using a HoloLens or Windows Mixed Reality headset, you can also turn off device-based speech recognition at any time. This will stop the device from listening for your voice input. [Learn more about speech recognition in Windows.](#)

Voice Activation. Windows provides supported apps with the ability to respond and take action based on voice keywords that are specific to that app—for example allowing Cortana to listen and respond when you say “Cortana.”

If you’ve given permission for an app to listen for voice keywords, Windows will be actively listening to the microphone for these keywords. Once a keyword is recognized, the app will have access to your voice recording, can process the recording, take action, and respond, such as with a spoken answer. The app may send the voice recording to its own services in the cloud to process the commands. Each app should ask you for permission before accessing voice recordings.

Additionally, voice activation can be enabled when the device is locked. If enabled, the relevant app will continue listening to the microphone for voice keywords when you have locked your device and can activate for anyone who speaks near the device. When the device is locked, the app will have access to the same set of capabilities and information as when the device is unlocked.

You can turn off voice activation at any time. [Learn more about voice activation in Windows.](#)

Even when you’ve turned off voice activation, some third-party desktop apps and services could still be listening to the microphone and collect your voice input. [Learn more about third-party desktop apps and how they may still be able to access your microphone even with these settings turned off.](#)

Voice typing. In Windows 11, dictation has been updated and renamed as voice typing. Like dictation, voice typing uses online speech recognition technologies to power its speech-to-text transcription service. You can also choose to contribute voice clips to help improve voice typing. If you choose not to contribute voice clips, you can still use voice typing. You can change your choice anytime in the voice typing settings. Microsoft will not listen to your voice recordings without your permission. [Learn more about voice typing in Windows.](#)

Inking & Typing Personalization. Your typed and handwritten words are collected to provide you with: a personal dictionary, better character recognition to help you type and write on your device, and text suggestions that appear as you type or write.

You can turn off Inking & typing personalization at any time. This will delete data stored on your device, such as your personal dictionary. [Learn more about inking & typing personalization in Windows.](#)

Sync and backup settings

When you sign into Windows with your Microsoft account or work or school account, Windows can store your settings, files, and device configuration data in Microsoft's servers. Windows will only use the stored settings, files, and device configuration data to make it easier for you to migrate your experience on a different device.

You can turn off this feature and stop Windows from storing your settings, files, and configuration data from the Windows settings app. You can also delete the sync and backup data Windows has stored in the settings app.

[Learn more about Windows backup and sync settings.](#)

Update Services

Update Services for Windows includes Windows Update and Microsoft Update. Windows Update is a service that provides you with software updates for Windows software and other supporting software, such as drivers and firmware supplied by device manufacturers. Microsoft Update is a service that provides you with software updates for other Microsoft software such as Microsoft 365.

Windows Update automatically downloads Windows software updates to your device. You can configure Windows Update to automatically install these updates as they become available (recommended) or have Windows notify you when a restart is required to finish installing updates. Apps available through the Microsoft Store are automatically updated through the Microsoft Store, as described in the [Microsoft Store](#) section of this privacy statement.

Web browsers—Microsoft Edge Legacy and Internet Explorer

This section applies to legacy versions of Microsoft Edge (versions 44 and below). See the [Microsoft Edge](#) section of the Privacy Statement for information about non-legacy versions of Microsoft Edge.

Microsoft Edge is the default web browser for Windows. Internet Explorer, the legacy browser from Microsoft, is also available in Windows. Whenever you use a web browser to access the internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address, browser type and language, access times, and referring website addresses. This data might be logged on those websites' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use. Additionally, Microsoft Edge sends a unique browser ID to certain websites to enable us to develop aggregate data used to improve browser features and services.

Additionally, data about how you use your browser, such as your browsing history, web form data, temporary internet files, and cookies, is stored on your device. You can delete this data from your device using Delete Browsing History.

Microsoft Edge allows you to capture and save content on your device, such as:

- ♦ **Web note.** Allows you to create ink and text annotations on the webpages you visit, and clip, save, or share them.
- **Active reading.** Allows you to create and manage reading lists, including websites or documents.
- ♦ **Hub.** Allows you to easily manage your reading lists, favorites, downloads, and history all in one area.
- ♦ **Website Pin to Taskbar.** Allows you to pin your favorite websites to the Windows taskbar. Websites will be able to see which of their webpages you have pinned, so they can provide you a notification badge letting you know there is something new for you to check out on their websites.

Some Microsoft browser information saved on your device will be synced across other devices when you sign in with your Microsoft account. For instance, in Internet Explorer, this information includes your browsing history and favorites; and in Microsoft Edge, it includes your favorites, reading lists, autofill form entries (such as your name, address, and phone number), and may include data for extensions that you have installed. As an example, if you sync your Microsoft Edge reading list across devices, copies of the content you choose to save to your reading list will be sent to each synced device for later viewing. You can disable syncing in Internet Explorer by going to **Start > Settings > Accounts > Sync your settings**. (For more information, see the [Sync settings](#) section of this privacy statement.) You can also disable syncing of Microsoft Edge browser information by turning off the sync option in Microsoft Edge Settings.

Microsoft Edge and Internet Explorer use your search queries and browsing history to provide you with faster browsing and more relevant search results. These features include:

- ♦ **Search suggestions** in Internet Explorer automatically sends the information you type into the browser address bar to your default search provider (such as Bing) to offer search recommendations as you type each character.
- ♦ **Search and site suggestions** in Microsoft Edge automatically sends the information you type into the browser address bar to Bing (even if you have selected another default search provider) to offer search recommendations as you type each character.

You can turn off these features at any time. In order to provide search results, Microsoft Edge and Internet Explorer send your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the [Bing](#) section of this privacy statement.

Cortana can assist you with your web browsing in Microsoft Edge with features such as Ask Cortana. You can disable Cortana assistance in Microsoft Edge at any time in Microsoft Edge Settings. To learn more about how Cortana uses data and how you can control that, go to the [Cortana](#) section of this privacy statement.

Windows apps

A number of Microsoft apps are included with Windows and others are available in Microsoft Store. Some of those apps include:

Maps app. The Maps app provides location-based services and uses Bing services to process your searches within the Maps app. When the Maps app has access to your location, and you have enabled location-based services in Windows, when you use the "@" key to initiate a search in supported text boxes in Windows apps, Bing services collect the text you type after the "@" key to provide location-based suggestions. To learn more about these Bing-powered experiences, see the [Bing](#) section of this privacy statement. When the Maps app has access to your location, even when the app is not in use, Microsoft may collect de-identified location data from your device to improve Microsoft services. You can disable the Maps app's access to your location by turning off the location service or turning off the Maps app's access to the location service.

You can keep track of your favorite places and recent map searches in the Maps app. Your favorite places and search history will be included as search suggestions. If you're signed in with your Microsoft account, your favorite places, search history, and certain app settings will be synced across other devices and services (for example, Cortana). For more information, see the [Sync and backup settings](#) section of this privacy statement.

Camera app. If you allow the Camera app to use your location, location data is embedded in the photos and videos you take with your device. Other descriptive data, such as camera model and the date that the picture or video was taken, is also embedded in photos and videos. If you choose to share a photo or video, any embedded data will be accessible to the people and services you share with. Once enabled, you can always disable the Camera app's access to your location by turning off all access to the location service in your device's Settings menu or turning off the Camera app's access to the location service.

When the Camera app is open, it shows rectangles detected by the selected camera for areas in the image that are potentially used for image enhancement. The Camera app does not retain any image enhancing data. You can always change your camera access settings in the Camera app's Settings menu or the Windows Settings menu.

Photos app. The Photos app helps you organize and share your photos. For example, the Photos app presents different ways to group photos and videos by date, location, tags, and faces. The Collection tab displays photos and videos according to the date they are taken. The Album tab helps users organize their photos and videos by location and common tags. The People tab helps you organize your photos and videos by grouping photos and videos with similar faces, which you can then associate with contacts.

If you enable the People setting on the Photos app's settings page, the app will use face grouping technologies to organize your photos and videos into groups. The grouping feature can detect faces in a photo or video and determine whether they are visually similar to faces in other photos and videos in your local photo collection. You can choose to associate a facial grouping with a contact from your People app.

If you choose to share a photo or video using the Photos app, any embedded data (such as location, camera model, and date) will be accessible to the people and services you share the

photo or video. If enabled, facial groupings are only accessible to you, on that device, within the Photos app and the groups and grouping data are not embedded in any shared photos or videos. You, and not Microsoft, are responsible for ensuring you have appropriate permissions from the people in your photos and videos to use facial grouping technology to group your photos and videos in your personal albums.

Your groupings will be stored on your device for as long as you choose to keep the groupings or the photos or videos. If the People setting is turned on, you will be prompted to allow the Photos app to continue to permit facial groupings after three years of non-interaction with the Photos app. At any time, you can go to the Settings page in the Photos app to turn the People setting on or off. This will remove facial grouping data from the Photos app, but will not remove your photos or videos. [Learn more about the Photos app and facial grouping.](#)

People app. The People app lets you see and interact with all your contacts in one place. When you add an account to the People app, your contacts from your account will be automatically added to the People app. You can add other accounts to the People app, including your social networks (such as Facebook and Twitter) and email accounts. When you add an account, we tell you what data the People app can import or sync with the particular service and let you choose what you want to add. Other apps you install may also sync data to the People app, including providing additional details to existing contacts. When you view a contact in the People app, information about your recent interactions with the contact (such as emails and calendar events, including from apps that the People app syncs data from) will be retrieved and displayed to you. You can remove an account from the People app at any time.

Mail and Calendar app. The Mail and Calendar app allows you to connect all your email, calendars, and files in one place, including those from third-party email and file storage providers. The app provides location-based services, such as weather information in your calendar, but you can disable the app's use of your location. When you add an account to the Mail and Calendar app, your email, calendar items, files, contacts, and other settings from your account will automatically sync to your device and to Microsoft servers. At any time, you can remove an account or make changes to the data that's synced from your account. To configure an account, you must provide the app with the account credentials (such as user name and password), which will be sent over the internet to the third-party provider's server. The app will first attempt to use a secure (SSL) connection to configure your account but will send this information unencrypted if your email provider does not support SSL. If you add an account provided by an organization (such as a company email address), the owner of the organizational domain can implement certain policies and controls (for example, multi-factor authentication or the ability to remotely wipe data from your device) that may affect your use of the app.

Messaging app. When you sign in with a Microsoft account on your device, you can choose to back up your information, which will sync your SMS and MMS messages and store them in your Microsoft account. This allows you to retrieve the messages if you lose or change phones. After your initial device set-up, you can manage your messaging settings at any time. Turning off your SMS/MMS backup will not delete messages that have been previously backed up to your Microsoft account. To delete such messages, you must first delete them

from your device prior to turning off backup. If you allow the Messaging app to use your location, you can attach a link to your current location to an outgoing message. Location information will be collected by Microsoft as described in the Windows [Location services](#) section of this privacy statement.

Narrator. Narrator is a screen-reading app that helps you use Windows without a screen. Narrator offers intelligent image and page title description and web page summaries when you encounter undescribed images and ambiguous links.

When you choose to get an image description by pressing Narrator + Ctrl + D, the image will be sent to Microsoft to perform analysis of the image and generate a description. Images are used only to generate the description and are not stored by Microsoft.

When you choose to get page title descriptions by pressing Narrator + Ctrl + D, the URL of the site you are visiting will be sent to Microsoft to generate the page title description and to provide and improve Microsoft services, such as Bing services as described in the Bing section above.

When you choose to get a list of popular links for a web page by pressing Narrator + double press of S, the URL of the site you are visiting will be sent to Microsoft to generate the summary of popular links and to provide and improve Microsoft services, such as Bing.

You can disable these features at any time by going to **Narrator > Get image descriptions, page titles and popular links** in the Windows setting app.

You can also send feedback about Narrator to help Microsoft diagnose and resolve problems with Narrator and improve Microsoft products and services, such as Windows. Verbal feedback can be submitted at any time in Narrator by using Narrator Key + Alt + F. When you use this command, the Feedback Hub app will launch, giving you the opportunity to submit verbal feedback. If you enable the setting "Help Make Narrator Better" in the Windows settings app and submit verbal feedback through Feedback Hub, recent device and usage data, including event trace log (ETL) data, will be submitted along with your verbal feedback to improve Microsoft products and services, such as Windows.

Windows Media Player

Windows Media Player allows you to play CDs, DVDs, and other digital content (such as WMA and MP3 files), rip CDs, and manage your media library. To enrich your experience when you play content in your library, Windows Media player displays related media information, such as album title, song titles, album art, artist, and composer. To augment your media information, Windows Media player will send a request to Microsoft which contains standard computer information, an identifier for the media content, and the media information already contained in your Windows Media Player library (including information you may have edited or entered yourself) so that Microsoft can recognize the track and then return additional information that is available.

Windows Media Player also allows you to play back content that is streamed to you over a network. To provide this service, it is necessary for Windows Media Player to communicate with a streaming media server. These servers are typically operated by non-Microsoft content providers. During playback of streaming media, Windows Media Player will send a log to the streaming media server or other web server(s) if the streaming media server requests it. The log includes such details as: connection time, IP address, operating system version, Windows Media Player version, Player identification number (Player ID), date, and protocol. To protect your privacy, Windows Media Player defaults to sending a Player ID that is different for each session.

Windows Hello

Windows Hello provides instant access to your devices through biometric authentication. If you turn it on, Windows Hello uses your face, fingerprint, or iris to identify you based on a set of unique points or features that are extracted from the image and stored on your device as a template—but it does not store the actual image of your face, fingerprint, or iris. Biometric verification data that's used when you sign in doesn't leave your device. Your biometric verification data will remain on your device until you remove it. However, after a significant period of Windows Hello inactivity, you will be prompted to confirm that you want to continue to store your biometric verification data. You can delete your biometric verification data from within Settings. Learn more about [Windows Hello](#).

Windows Search

Windows Search lets you search your stuff and the web from one place. If you choose to use Windows Search to search "your stuff," it will provide results for items on your personal OneDrive, your OneDrive for Business if so enabled, other cloud storage providers to the extent supported by those third-party providers, and on your device. If you choose to use Windows Search to search the web, or get search suggestions with Windows Search, your search results will be powered by Bing and we will use your search query as described in the [Bing](#) section of this privacy statement. [Learn more about search in Windows](#).

Entertainment and related services

Entertainment and Related Services power rich experiences and enable you to access a variety of content, applications and games.

Xbox

The Xbox network is the online gaming and entertainment service from Microsoft that consists of software and enables online experiences across different platforms. This service lets you find and play games, view content, and connect with friends on Xbox and other gaming and

social networks. You can connect to the Xbox network using Xbox consoles, Windows devices, and mobile devices (Android and iPhone).

When you sign up for an Xbox profile, we assign you a gamertag (a public nickname) and a unique identifier. When you sign in on Xbox devices, apps, and services, the data we collect about your use is stored using these unique identifier(s).

Xbox consoles are devices you can use to find and play games, movies, music, and other digital entertainment. When you sign in to Xbox experiences—in apps or on a console—we also assign a unique identifier to your device. When your Xbox console is connected to the internet, for instance, and you sign in to the console, we identify which console and which version of the console's operating system you're using.

Xbox continues to provide new experiences in client apps that are connected to and backed by services such as the Xbox network and cloud gaming. When signed in to an Xbox experience, we collect required data to help keep these experiences reliable, up to date, secure, and performing as expected.

Data we collect about your use of Xbox services, games, apps, and consoles includes:

- ◆ When you sign in and sign out of Xbox, any purchases you make, and content you obtain.
- ◆ Which games you play and apps you use, your game progress, achievements, play time per game, and other play statistics.
- Performance data about Xbox consoles, Xbox Game Pass and other Xbox apps, the Xbox network, connected accessories, and your network connection, including any software or hardware errors.
- ◆ Content you add, upload, or share through the Xbox network, including text, pictures, and video you capture in games and apps.
- ◆ Social activity, including chat data and interactions with other gamers, and connections you make (friends you add and people who follow you) on the Xbox network.

If you use an Xbox console or Xbox app on another device capable of accessing the Xbox network, and that device includes a storage device (hard drive or memory unit), usage data will be stored on the storage device and sent to Microsoft the next time you sign in to Xbox, even if you've been playing offline.

Xbox console diagnostic data. Diagnostic data has two categories: required and optional. If you use an Xbox console, the console will send required data to Microsoft. Optional data is additional data that you choose to share with Microsoft.

- **Required.** The minimum data necessary to help keep Xbox safe, secure, up to date, and performing as expected.
- ◆ **Optional.** Optional data includes additional details about your console, its settings, its health, its use, and enhanced error reporting to help us detect, diagnose, and fix problems.

Learn more at [Manage settings for optional data sharing](#).

Game captures. Any player in a multiplayer game session can record video (game clips) and capture screenshots of their view of the game play. Other players' game clips and screenshots can capture your in-game character and gamertag during that session. If a player captures game clips and screenshots on a PC, the resulting game clips might also capture audio chat.

Captioning. During Xbox real-time ("party") chat, players may activate a voice-to-text feature that lets them view that chat as text. If a player activates this feature, all voice communication in the party is captioned for the player. Microsoft uses the resulting text data to provide captioning of chat for players who need it, as well as the other purposes described in this statement.

Data use. Microsoft uses the data we collect to improve gaming products and experiences—making them safer and more fun over time.

Data we collect also enables us to provide you with personalized, curated experiences. This includes connecting you to games, content, and services, as well as presenting you with offers, discounts, and recommendations.

Xbox data viewable by others. Your gamertag, game and play statistics, achievements, presence (whether you are currently signed in to Xbox), content you share, and other data about your activity on Xbox can be seen by:

- Other players signed in to Xbox.
- Customers of third-party services you've linked your profile to, or
- Other services associated with Xbox (including those of partner companies).

For example, your gamertag and scores that show on game leaderboards are considered public and cannot be hidden. For other data, you can adjust your privacy settings on consoles and at [Xbox.com](https://xbox.com) to limit or block what is shared with the public or with friends.

Learn more at [Xbox online safety and privacy settings](https://xbox.com).

Xbox data shared with third parties including game and apps publishers. When you use an Xbox online game or any network-connected app on your Xbox console, PC, or mobile device, the publisher of that game or app has access to data about your usage to help the publisher deliver, support, and improve its product. This data may include: your Xbox user identifier, gamertag, limited account info such as country and age range, data about your in-game communications, any Xbox enforcement activity, game-play sessions (for example, moves made in-game, types of vehicles used in-game), your presence on the Xbox network, the time you spend playing the game or app, rankings, statistics, gamer profiles, avatars, or gamerpics, friends lists, activity feeds for official clubs you belong to, official club memberships, and any content you create or submit in the game or app.

Third-party publishers and developers of games and apps have their own distinct and independent relationship with users and their collection and usage of personal data is subject to their specific privacy policies. You should carefully review their policies to determine how they use the data. For example, publishers may choose to disclose or display game data (such

as on leaderboards) through their own services. You may find their policies linked from game or app detail pages in the Microsoft Store.

Learn more at [Data Sharing with Games and Apps](#).

To stop sharing game or app data with a publisher, remove its games or app from all devices where you have installed them. Some publisher access to your data may be revoked at <https://microsoft.com/consent>.

Children and family. If you have kids who want to use the Xbox network, you can set up child and teen profiles for them once they have Microsoft accounts. Adult organizers in your Microsoft family group can change consent choices and online safety settings for child and teen profiles on [Xbox.com](#).

Learn more about Microsoft family groups at [Simplify your family's life](#).

Learn more about managing Xbox profiles, at [Xbox online safety and privacy settings](#).

For more information about Microsoft's collection of data from children, including Xbox, please see the [Collection of data from children](#) section of this privacy statement.

Safety. In order to help make the Xbox network a safe gaming environment and enforce the Community Standards for Xbox, we may collect and review voice, text, images, videos and in-game content (such as game clips you upload, conversations you have, and things you post in clubs and games).

Legacy.

- **Xbox 360.** This Xbox console collects limited required diagnostic data to keep your console functioning as expected while using a console connected to the Xbox network.
- **Kinect.** The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control gameplay. For example:
 - If you choose, the camera can be used to sign you in to the Xbox network automatically using facial recognition. This data stays on the console and is not shared with anyone, and you can choose to delete this data from your console at any time.
 - For game play, Kinect will map distances between your body's joints to create a stick figure representation of you that helps Kinect enable play.
 - The Kinect microphone can enable voice chat between players during play. The microphone also enables voice commands for control of the console, game, or app, or to enter search terms.
 - The Kinect sensor can also be used for audio and video communications through services such as Skype.

Learn more about Kinect at [Xbox Kinect and Privacy](#).

Microsoft Store

Microsoft Store is an online service, accessible via PC, the Xbox Console and the Xbox App, that allows you to browse, download, purchase, rate, and review applications and other digital content. It includes:

- Apps and content for Windows devices such as phones, PCs, and tablets.
- Games, subscriptions and other apps for Xbox consoles and other devices.
- Products and apps for Microsoft 365, SharePoint, Exchange, Access, and Project (2013 versions or later).

We collect data about how you access and use Microsoft Store; the products you've viewed, purchased, or installed; the preferences you set for viewing apps in Microsoft Store; and any ratings, reviews, or problem reports you submit. Your Microsoft account is associated with your ratings and reviews; and if you write a review, the name and picture from your Microsoft account will be published with your review.

Permission for Microsoft Store apps. Many apps you install from the Microsoft Store are designed to take advantage of specific hardware and software features of your device. An app's use of certain hardware and software features may give the app or its related service access to your data. For example, a photo editing app might access your device's camera to let you take a new photo or access photos or videos stored on your device for editing, and a restaurant guide might use your location to provide nearby recommendations. Information about the features that an app uses is provided on the app's product description page in Microsoft Store. Many of the features that Microsoft Store apps use can be turned on or off through your device's privacy settings. In Windows, in many cases, you can choose which apps can use a particular feature. Go to **Start > Settings > Privacy or Privacy & Security**, select the feature (for example, Calendar), and then select which app permissions are on or off. The lists of apps in Windows privacy settings that can use hardware and software features will not include "Classic Windows" applications, and these applications are not affected by these settings.

App updates. Unless you have turned off automatic app updates in the relevant Microsoft Store settings or have acquired an app provided and updated by the app developer, Microsoft Store will automatically check for, download, and install app updates to verify that you have the latest versions. Updated apps might use different Windows hardware and software features from the previous versions, which could give them access to different data on your device. You will be prompted for consent if an updated app accesses certain features, such as location. You can also review the hardware and software features an app uses by viewing its product description page in Microsoft Store.

Each app's use of your data collected through any of these features is subject to the app developer's privacy policies. If an app available through Microsoft Store collects and uses any of your personal data, the app developer is required to provide a privacy policy, and a link to the privacy policy is available on the app's product description page in Microsoft Store.

Sideloaded apps and developer mode. Developer features such as the "developer mode" setting are intended for development use only. If you enable developer features, your device may become unreliable or unusable, and expose you to security risks. Downloading or otherwise acquiring apps from sources other than Microsoft Store, also known as

"sideloading" apps, may make your device and personal data more vulnerable to attack or unexpected use by apps. Windows policies, notifications, permissions, and other features intended to help protect your privacy when apps access your data may not function as described in this statement for sideloaded apps or when developer features are enabled.

MSN

MSN services include websites and a suite of apps, including MSN News, Weather, Sports, and Money, and previous versions of the apps branded as Bing (together, "MSN Apps"). The MSN Apps are available on various platforms, including Windows, iOS, and Android. MSN services are also included within other Microsoft services, including the Microsoft Edge browser.

When you install MSN Apps, we collect data that tells us if the app was installed properly, the installation date, the app version, and other data about your device such as the operating system and browser. This data is collected on a regular basis to help us determine the number of MSN App users and identify performance issues associated with different app versions, operating systems, and browsers.

We also collect data about how you interact with MSN services, such as usage frequency and articles viewed, to provide you with relevant content. Some MSN services provide an enhanced experience when you sign in with your Microsoft account, including allowing you to customize your interests and favorites. You can manage personalization through MSN and Bing settings, as well as through settings in other Microsoft services that include MSN services. We also use the data we collect to provide you with advertisements that may be of interest to you. You can opt out of interest-based advertising through the advertising links within MSN services, or by visiting the Microsoft [opt-out page](#).

Previous versions of MSN Money allow you to access personal finance information from third-party financial institutions. MSN Money only displays this information and does not store it on our servers. Your sign-in credentials used to access your financial information from third parties are encrypted on your device and are not sent to Microsoft. These financial institutions, as well as any other third-party services you access through MSN services, are subject to their own terms and privacy policies.

Groove Music and Movies & TV

Groove Music lets you easily play your music collection and make playlists. Microsoft Movies & TV allows you to play your video collection and rent or buy movies and TV episodes. These services were formerly offered as Xbox Music and Video.

To help you discover content that may interest you, Microsoft will collect data about what content you play, the length of play, and the rating you give it.

To enrich your experience when playing content, Groove Music and Movies & TV will display related information about the content you play and the content in your music and video

libraries, such as the album title, cover art, song or video title, and other information, where available. To provide this information, Groove Music and Movies & TV send an information request to Microsoft containing standard device data, such as your device IP address, device software version, your regional and language settings, and an identifier for the content.

If you use Movies & TV to access content that has been protected with Microsoft Digital Rights Management (DRM), it may automatically request media usage rights from an online rights server and download and install DRM updates in order to let you play the content. See the DRM information in the [Silverlight](#) section of this privacy statement for more information.

Silverlight

Microsoft Silverlight helps you to access and enjoy rich content on the Web. Silverlight enables websites and services to store data on your device. Other Silverlight features involve connecting to Microsoft to obtain updates, or to Microsoft or third-party servers to play protected digital content.

Silverlight Configuration tool. You can make choices about these features in the Silverlight Configuration tool. To access the Silverlight Configuration tool, right click on content that is currently being displayed by Silverlight and select **Silverlight**. You can also run the Silverlight Configuration tool directly. In Windows, for example, you can access the tool by searching for "Microsoft Silverlight."

Silverlight application storage. Silverlight-based applications can store data files locally on your computer for a variety of purposes, including saving your custom settings, storing large files for graphically intensive features (such as games, maps, and images), and storing content that you create within certain applications. You can turn off or configure application storage in the Silverlight Configuration tool.

Silverlight updates. Silverlight will periodically check a Microsoft server for updates to provide you with the latest features and improvements. A small file containing information about the latest Silverlight version will be downloaded to your computer and compared to your currently installed version. If a newer version is available, it will be downloaded and installed on your computer. You can turn off or configure updates in the Silverlight Configuration tool.

Digital Rights Management. Silverlight uses Microsoft Digital Rights Management (DRM) technology to help protect the rights of content owners. If you access DRM-protected content (such as music or video) with Silverlight, it will request media usage rights from a rights server on the Internet. In order to provide a seamless playback experience, you will not be prompted before Silverlight sends the request to the rights server. When requesting media usage rights, Silverlight will provide the rights server with an ID for the DRM-protected content file and basic data about your device, including data about the DRM components on your device such as their revision and security levels, and a unique identifier for your device.

DRM updates. In some cases, accessing DRM-protected content will require an update to Silverlight or to the DRM components on your device. When you attempt to play content that requires a DRM update, Silverlight will send a request to a Microsoft server containing basic data about your device, including information about the DRM components on your computer such as their revision and security levels, troubleshooting data, and a unique identifier for your device. The Microsoft server uses this identifier to return a unique DRM update for your device, which will then be installed by Silverlight. You can turn off or configure DRM component updates on the **Playback** tab in the Silverlight Configuration tool.

Windows Mixed Reality

Windows Mixed Reality allows you to enable a virtual reality experience that immerses you in apps and games. Mixed Reality uses a compatible headset's camera, microphone, and infrared sensors to enable motions and voice to be used to control gameplay and to navigate apps and games.

Microsoft collects diagnostic data to solve problems and to keep Mixed Reality running on Windows up to date, secure, and operating properly. Diagnostic data also helps us improve Mixed Reality and related Microsoft products and services depending on the diagnostic data settings you've chosen for your device. [Learn more about Windows diagnostic data.](#)

Mixed Reality also processes and collects data specifically related to the Mixed Reality experiences, such as:

- Mixed Reality maps distances between your body's joints to create a stick figure representation of you. If you are connected to the Internet, we collect those numeric values to enable and improve your experience.
- Mixed Reality detects specific hand gestures intended to perform simple system interactions (such as menu navigation, pan/zoom, and scroll). This data is processed on your PC and is not stored.
- The headset's microphones enable voice commands to control games, apps, or to enter search terms. [Learn more about voice data collection.](#)
- Windows Mixed Reality can also be used for audio and video communications through services such as Skype.

- [Sitemap](#)
- [Contact Microsoft](#)
- [Privacy](#)
- [Manage cookies](#)
- [Terms of use](#)
- [Trademarks](#)
- [Safety & eco](#)
- [About our ads](#)
- © Microsoft 2022

Volume
Licensing

Service Level Agreement for Microsoft Online Services June 1, 2022

Table of Contents

TABLE OF CONTENTS	2	MICROSOFT AZURE SERVICES AND AZURE PLANS	18
INTRODUCTION	3	OTHER ONLINE SERVICES	18
GENERAL TERMS	4	MICROSOFT DEFENDER FOR IDENTITY	18
SERVICE SPECIFIC TERMS	6	BING MAPS ENTERPRISE PLATFORM.....	18
MICROSOFT DYNAMICS 365	6	BING MAPS MOBILE ASSET MANAGEMENT	19
DYNAMICS 365 BUSINESS CENTRAL	6	MICROSOFT CLOUD APP SECURITY	19
DYNAMICS 365 COMMERCE.....	6	MICROSOFT POWER AUTOMATE	20
DYNAMICS 365 CUSTOMER INSIGHTS.....	7	MICROSOFT INTUNE	20
DYNAMICS 365 CUSTOMER SERVICE ENTERPRISE; DYNAMICS 365 CUSTOMER SERVICE PROFESSIONAL; DYNAMICS 365 CUSTOMER SERVICE INSIGHTS;		MICROSOFT KAIZALA PRO.....	20
DYNAMICS 365 FIELD SERVICE; DYNAMICS 365 MARKETING	7	MICROSOFT POWER APPS	21
DYNAMICS 365 FRAUD PROTECTION	7	MICROSOFT SUSTAINABILITY MANAGER.....	22
DYNAMICS 365 GUIDES	8	MINECRAFT: EDUCATION EDITION	22
DYNAMICS 365 HUMAN RESOURCES	8	POWER BI EMBEDDED	22
DYNAMICS 365 INTELLIGENT ORDER MANAGEMENT	9	POWER BI PREMIUM.....	23
DYNAMICS 365 REMOTE ASSIST	9	POWER BI PRO	23
DYNAMICS 365 SALES ENTERPRISE; DYNAMICS 365 SALES PROFESSIONAL	9	TRANSLATOR API	24
DYNAMICS 365 SUPPLY CHAIN MANAGEMENT; DYNAMICS 365 FINANCE;		MICROSOFT DEFENDER FOR ENDPOINT	24
DYNAMICS 365 PROJECT OPERATIONS	10	UNIVERSAL PRINT	24
OFFICE 365 SERVICES	10	WINDOWS 365	25
DUET ENTERPRISE ONLINE	10	APPENDIX A – SERVICE LEVEL COMMITMENT FOR VIRUS DETECTION AND BLOCKING, SPAM EFFECTIVENESS, OR FALSE POSITIVE	26
EXCHANGE ONLINE.....	11	APPENDIX B - SERVICE LEVEL COMMITMENT FOR UPTIME AND EMAIL DELIVERY	27
EXCHANGE ONLINE ARCHIVING	11		
EXCHANGE ONLINE PROTECTION	12		
MICROSOFT MYANALYTICS	12		
MICROSOFT STREAM	12		
MICROSOFT TEAMS.....	13		
MICROSOFT 365 APPS FOR BUSINESS	13		
MICROSOFT 365 APPS FOR ENTERPRISE	13		
OFFICE 365 ADVANCED COMPLIANCE	14		
OFFICE ONLINE.....	14		
OFFICE 365 VIDEO.....	15		
ONEDRIVE FOR BUSINESS	15		
PROJECT	15		
SHAREPOINT ONLINE	16		
SKYPE FOR BUSINESS ONLINE	16		
MICROSOFT TEAMS – CALLING PLANS, PHONE SYSTEM AND AUDIO			
CONFERENCING	16		
MICROSOFT TEAMS – VOICE QUALITY	17		
WORKPLACE ANALYTICS	17		
YAMMER ENTERPRISE	18		

Introduction

About this Document

This Service Level Agreement for Microsoft Online Services (this “SLA”) is a part of your Microsoft volume licensing agreement (the “Agreement”). Capitalized terms used but not defined in this SLA will have the meaning assigned to them in the Agreement. This SLA applies to the Microsoft Online Services listed herein (a “Service” or the “Services”), but does not apply to separately branded services made available with or connected to the Services or to any on-premise software that is part of any Service.

If we do not achieve and maintain the Service Levels for each Service as described in this SLA, then you may be eligible for a credit towards a portion of your monthly service fees. We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, the version of this SLA that is current at the time of renewal will apply throughout your renewal term. We will provide at least 90 days’ notice for adverse material changes to this SLA. You can review the most current version of this SLA at any time by visiting <http://www.microsoftvolumelicensing.com/SLA>.

Prior Versions of this Document

This SLA provides information on Services currently available. Earlier versions of this document are available at <http://www.microsoftvolumelicensing.com>. To find the needed version, a customer may contact its reseller or Microsoft Account Manager.

Clarifications and Summary of Changes to this Document

Below are recent additions, deletions and other changes to this SLA. Also listed below, are clarifications of Microsoft policy in response to common customer questions.

Additions/Updates	Deletions
Microsoft Sustainability Manager	None

[Table of Contents / Definitions](#)[Table of Contents](#)[Introduction](#)[General Terms](#)[Service Specific Terms](#)[Appendices](#)

General Terms

Definitions

"Applicable Monthly Period" means, for a calendar month in which a Service Credit is owed, the number of days that you are a subscriber for a Service.

"Applicable Monthly Service Fees" means the total fees actually paid by you for a Service that are applied to the month in which a Service Credit is owed.

"Downtime" is defined for each Service in the Services Specific Terms below. Except for Microsoft Azure Services, Downtime does not include Scheduled Downtime. Downtime does not include unavailability of a Service due to limitations described below and in the Services Specific Terms.

"Error Code" means an indication that an operation has failed, such as an HTTP status code in the 5xx range.

"External Connectivity" is bi-directional network traffic over supported protocols such as HTTP and HTTPS that can be sent and received from a public IP address.

"Incident" means (i) any single event, or (ii) any set of events, that result in Downtime.

"Management Portal" means the web interface, provided by Microsoft, through which customers may manage the Service.

"Scheduled Downtime" means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish notice or notify you at least five (5) days prior to the commencement of such Downtime.

"Service Credit" is the percentage of the Applicable Monthly Service Fees credited to you following Microsoft's claim approval.

"Service Level" means the performance metric(s) set forth in this SLA that Microsoft agrees to meet in the delivery of the Services.

"Service Resource" means an individual resource available for use within a Service.

"Success Code" means an indication that an operation has succeeded, such as an HTTP status code in the 2xx range.

"Support Window" refers to the period of time during which a Service feature or compatibility with a separate product or service is supported.

"User Minutes" means the total number of minutes in a month, less all Scheduled Downtime, multiplied by the total number of users.

Terms

Claims

In order for Microsoft to consider a claim, you must submit the claim to customer support at Microsoft Corporation including all information necessary for Microsoft to validate the claim, including but not limited to: (i) a detailed description of the Incident; (ii) information regarding the time and duration of the Downtime; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the Incident at the time of occurrence.

For a claim related to Microsoft Azure, we must receive the claim within two months of the end of the billing month in which the Incident that is the subject of the claim occurred. For claims related to all other Services, we must receive the claim by the end of the calendar month following the month in which the Incident occurred. For example, if the Incident occurred on February 15th, we must receive the claim and all required information by March 31st.

We will evaluate all information reasonably available to us and make a good faith determination of whether a Service Credit is owed. We will use commercially reasonable efforts to process claims during the subsequent month and within forty-five (45) days of receipt. You must be in compliance with the Agreement in order to be eligible for a Service Credit. If we determine that a Service Credit is owed to you, we will apply the Service Credit to your Applicable Monthly Service Fees.

If you purchased more than one Service (not as a suite), then you may submit claims pursuant to the process described above as if each Service were covered by an individual SLA. For example, if you purchased both Exchange Online and SharePoint Online (not as part of a suite), and during the term of the subscription an Incident caused Downtime for both Services, then you could be eligible for two separate Service Credits (one for each Service), by submitting two claims under this SLA. In the event that more than one Service Level for a particular Service is not met because of the same Incident, you must choose only one Service Level under which to make a claim based on the Incident. Unless as otherwise provided in a specific SLA, only one Service Credit is permitted per Service for an Applicable Monthly Period.

Service Credits

Service Credits are your sole and exclusive remedy for any performance or availability issues for any Service under the Agreement and this SLA. You may not unilaterally offset your Applicable Monthly Service Fees for any performance or availability issues.

Service Credits apply only to fees paid for the particular Service, Service Resource, or Service tier for which a Service Level has not been met. In cases where Service Levels apply to individual Service Resources or to separate Service tiers, Service Credits apply only to fees paid for the affected

Service Resource or Service tier, as applicable. The Service Credits awarded in any billing month for a particular Service or Service Resource will not, under any circumstance, exceed your monthly service fees for that Service or Service Resource, as applicable, in the billing month. If you purchased Services as part of a suite or other single offer, the Applicable Monthly Service Fees and Service Credit for each Service will be pro-rated.

If you purchased a Service from a reseller, you will receive a service credit directly from your reseller and the reseller will receive a Service Credit directly from us. The Service Credit will be based on the estimated retail price for the applicable Service, as determined by us in our reasonable discretion.

Limitations

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centers, including at your site or between your site and our data center);
2. That result from the use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;
3. That results from failures in a single Microsoft Datacenter location, when your network connectivity is explicitly dependent on that location in a non-geo-resilient manner;
4. Caused by your use of a Service after we advised you to modify your use of the Service, if you did not modify your use as advised;
5. During or with respect to preview, pre-release, beta or trial versions of a Service, feature or software (as determined by us) or to purchases made using Microsoft subscription credits;
6. That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;
7. That result from your failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or your use of the Service in a manner inconsistent with the features and functionality of the Service (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;
8. That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);
9. That result from your attempts to perform operations that exceed prescribed quotas or that resulted from our throttling of suspected abusive behavior;
10. Due to your use of Service features that are outside of associated Support Windows; or
11. For licenses reserved, but not paid for, at the time of the Incident.

Services purchased through Open, Open Value, and Open Value Subscription volume licensing agreements, and Services in an Office 365 Small Business Premium suite purchased in the form of a product key are not eligible for Service Credits based on service fees. For these Services, any Service Credit that you may be eligible for will be credited in the form of service time (i.e., days) as opposed to service fees, and any references to “Applicable Monthly Service Fees” is deleted and replaced by “Applicable Monthly Period.”

[Table of Contents / Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Service Specific Terms

Microsoft Dynamics 365

Dynamics 365 Business Central

Downtime: Any period of time when end users are unable to login to their instance.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Dynamics 365 Commerce

Additional Definitions:

“Active Tenant” means a tenant with an active high availability production topology in the Management Portal that (A) has been deployed to a Partner Application Service; and (B) has an active database that users can log into.

“Partner Application Service” means a partner application built on top of and combined with the Platform that (A) is used for processing your organization’s actual business transactions; and (B) has reserve compute and storage resources equal to or greater than one of the Scale Units your partner selected for the applicable partner application.

“Maximum Available Minutes” means the total accumulated minutes during a billing month in which an Active Tenant was deployed in a Partner Application Service using an active high availability production topology.

“Platform” means the Service’s client forms, SQL server reports, batched operations, and API endpoints, or the Service’s retail APIs that are used for commerce or retail purposes only.

“Scale Unit” means the increments by which compute and storage resources are added to or removed from a Partner Application Service.

“Service Infrastructure” means the authentication, computing, and storage resources that Microsoft provides in connection with the Service.

Downtime: Any period of time when end users are unable to access their Active Tenant, due to a failure in the unexpired Platform or the Service Infrastructure as Microsoft determines from automated health monitoring and system logs. Downtime does not include Scheduled Downtime, the unavailability of Service add-on features, the inability to access the Service due to your modifications of the Service, or periods where the Scale Unit capacity is exceeded.

Monthly Uptime Percentage: The Monthly Uptime Percentage for a given Active Tenant in a calendar month is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%

[Table of Contents](#)

→

[Introduction](#)

→

[General Terms](#)

→

[Service Specific Terms](#)

→

[Appendices](#)

Monthly Uptime Percentage	Service Credit
< 95%	100%

[Table of Contents](#) / [Definitions](#)

Dynamics 365 Customer Insights

Downtime: Any period of time when end users are unable to login to their environment. Downtime does not include Scheduled Downtime, the unavailability of Service add-on features, or the inability to access the Service due to your modifications of the Service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#) / [Definitions](#)

Dynamics 365 Customer Service Enterprise; Dynamics 365 Customer Service Professional; Dynamics 365 Customer Service Insights; Dynamics 365 Field Service; Dynamics 365 Marketing

Downtime: Any period of time when end users are unable to read or write any Service data for which they have appropriate permission but this does not include non-availability of Service add-on features.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#) / [Definitions](#)

Dynamics 365 Fraud Protection

Downtime: Any period of time when end users are unable to read or write any Service data for which they have appropriate permission but this does not include non-availability of Service add-on features.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{\#Minutes in month} - \text{\#Minutes DFP service is unavailable}}{\text{\#Minutes in month}} \times 100$$

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

where, in a given minute interval, the service is said to be available if there is a successful watchdog ping test of the service through its external DNS.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Dynamics 365 Guides

Additional Definitions:

Downtime: Any period of time when end user is unable to read or write any Service data for which they have appropriate permission. Any period of time when end users are unable to initiate or participate in calls.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

* Downtime does not include Scheduled Downtime.

Service Credit:

Monthly Uptime Percentage	Service Credit
<99.5%	25%
<99%	50%

[Table of Contents / Definitions](#)

Dynamics 365 Human Resources

Additional Definitions:

“Active Tenant” means a tenant with an active high availability production topology in the Management Portal that has an active database that users can log into.

Downtime: Any period of time when end users are unable to read or write any Service data for which they have appropriate permission. Downtime does not include Scheduled Downtime.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.5%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)
[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

Dynamics 365 Intelligent Order Management

Downtime: Any period of time when end user are unable to read or write any Service data for which they have appropriate permission but this does not include any non-availability of Service add-on features. Downtime does not include Scheduled Downtime.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Dynamics 365 Remote Assist

Additional Definitions:

Downtime: Any period of time when end users are unable to conduct instant messaging conversations, or initiate or participate in calls.*

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

*Instant messaging conversations available only in some platforms

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%

[Table of Contents / Definitions](#)

Dynamics 365 Sales Enterprise; Dynamics 365 Sales Professional

Downtime: Any period of time when end users are unable to read or write any Service data for which they have appropriate permission but this does not include non-availability of Service add-on features.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Dynamics 365 Supply Chain Management; Dynamics 365 Finance; Dynamics 365 Project Operations

Additional Definitions:

“Active Tenant” means a tenant with an active high availability production topology in the Management Portal that (A) has been deployed to a Partner Application Service; and (B) has an active database that users can log into.

“Partner Application Service” means a partner application built on top of and combined with the Platform that (A) is used for processing your organization’s actual business transactions; and (B) has reserve compute and storage resources equal to or greater than one of the Scale Units your partner selected for the applicable partner application.

“Maximum Available Minutes” means the total accumulated minutes during a billing month in which an Active Tenant was deployed in a Partner Application Service using an active high availability production topology.

“Platform” means the Service’s client forms, SQL server reports, batched operations, and API endpoints, or the Service’s retail APIs that are used for commerce or retail purposes only.

“Scale Unit” means the increments by which compute and storage resources are added to or removed from a Partner Application Service.

“Service Infrastructure” means the authentication, computing, and storage resources that Microsoft provides in connection with the Service.

Downtime: Any period of time when end users are unable to login to their Active Tenant, due to a failure in the unexpired Platform or the Service Infrastructure as Microsoft determines from automated health monitoring and system logs. Downtime does not include Scheduled Downtime, the unavailability of Service add-on features, the inability to access the Service due to your modifications of the Service, or periods where the Scale Unit capacity is exceeded.

Monthly Uptime Percentage: The Monthly Uptime Percentage for a given Active Tenant in a calendar month is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Office 365 Services

Duet Enterprise Online

Downtime: Any period of time when users are unable to read or write any portion of a SharePoint Online site collection for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply when the inability to read or write any portion of a SharePoint Online site is caused by any failure of third party software, equipment, or services that are not controlled by Microsoft, or Microsoft software that is not being run by Microsoft itself as part of the Service.

Additional Terms: You will be eligible for a Service Credit for Duet Enterprise Online only when you are eligible for a Service Credit for the SharePoint Online Plan 2 User SLs that you have purchased as a prerequisite for your Duet Enterprise Online User SLs.

[Table of Contents / Definitions](#)

Exchange Online

Downtime: Any period of time when users are unable to send or receive email with Outlook Web Access. There is no Scheduled Downtime for this service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Additional Terms: See Appendix 1 – Service Level Commitment for Virus Detection and Blocking, Spam Effectiveness, or False Positive.

[Table of Contents / Definitions](#)

Exchange Online Archiving

Downtime: Any period of time when users are unable to access the email messages stored in their archive. There is no Scheduled Downtime for this service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to the Enterprise CAL suite purchased through Open Value and Open Value Subscription volume licensing agreements.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

[Table of Contents](#) / [Definitions](#)

Exchange Online Protection

Downtime: Any period of time when the network is not able to receive and process email messages. There is no Scheduled Downtime for this service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to the Enterprise CAL suite purchased through Open Value and Open Value Subscription volume licensing agreements.

Additional Terms: See (i) Appendix 1 – Service Level Commitment for Virus Detection and Blocking, Spam Effectiveness, or False Positive and (ii) Appendix 2 – Service Level Commitment for Uptime and Email Delivery.

[Table of Contents](#) / [Definitions](#)

Microsoft MyAnalytics

Downtime: Any period of time when users are unable to access the MyAnalytics dashboard.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#) / [Definitions](#)

Microsoft Stream

Downtime: Any period of time when users are unable to upload, playback, delete video or edit video metadata when they have appropriate permissions and content is valid excluding unsupported scenarios¹.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

[Table of Contents](#)[Introduction](#)[General Terms](#)[Service Specific Terms](#)[Appendices](#)

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Level Commitment:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: No SLA is provided for any free of charge tier of Microsoft Stream.

¹Unsupported Scenarios could include playback on unsupported devices / OS, client side network issues, and user errors.

[Table of Contents / Definitions](#)

Microsoft Teams

Downtime: Any period of time when end users are unable to see presence status, conduct instant messaging conversations, or initiate online meetings.¹

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

¹Online meeting functionality applicable only to users licensed for the Skype for Business Online Plan 2 Service.

[Table of Contents / Definitions](#)

Microsoft 365 Apps for business

Downtime: Any period of time when Office applications are put into reduced functionality mode due to an issue with Office 365 activation.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Microsoft 365 Apps for enterprise

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Downtime: Any period of time when Office applications are put into reduced functionality mode due to an issue with Office 365 activation.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Office 365 Advanced Compliance

Downtime: Any period of time when Customer Lockbox component of Office 365 Advanced Compliance is put into reduced functionality mode due to an issue with Office 365.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Office Online

Downtime: Any period of time when users are unable to use the Web Applications to view and edit any Office document stored on a SharePoint Online site for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Office 365 Video

Downtime: Any period of time when users are unable to upload, view or edit videos in the video portal when they have appropriate permissions and valid content.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Level Commitment:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#) / [Definitions](#)

OneDrive for Business

Downtime: Any period of time when users are unable to view or edit files stored on their personal OneDrive for Business storage.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#) / [Definitions](#)

Project

Downtime: Any period of time when users are unable to read or write any portion of a SharePoint Online site collection with Project Web App for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#)

→

[Introduction](#)

→

[General Terms](#)

→

[Service Specific Terms](#)

→

[Appendices](#)

[Table of Contents / Definitions](#)

SharePoint Online

Downtime: Any period of time when users are unable to read or write any portion of a SharePoint Online site collection for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Skype for Business Online

Downtime: Any period of time when end users are unable to see presence status, conduct instant messaging conversations, or initiate online meetings.¹

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

¹Online meeting functionality applicable only to Skype for Business Online Plan 2 Service.

[Table of Contents / Definitions](#)

Microsoft Teams – Calling Plans, Phone System and Audio Conferencing

Downtime: Any period of time when end users are unable to initiate a PSTN call or unable to dial into conference audio via the PSTN, or process calls with Call Queues or Auto Attendant.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula for each of the services:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

Where Downtime is measured in user-minutes; that is, for each month Downtime is the sum of the length (in minutes) of each incident that occurs during that month multiplied by the number of users impacted by that incident. Credit will be paid only against the actual service(s) that are impacted.

[Table of Contents](#)[Introduction](#)[General Terms](#)[Service Specific Terms](#)[Appendices](#)

This SLA does not apply to outages caused by any failure of third-party software, equipment, or services that are not controlled by Microsoft, or Microsoft software that is not being run by Microsoft itself as part of the Service.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Microsoft Teams – Voice Quality

This SLA applies to any eligible call placed by any voice service user within the subscription (enabled for making any type of call VOIP or PSTN).

Additional Definitions:

“Eligible Call” is a Microsoft Teams placed call (within a subscription) that meets both conditions below:

- The call was placed from a Microsoft Teams Certified IP Desk phones on wired Ethernet
- Packet Loss, Jitter and Latency issues on the call were due to networks managed by Microsoft.

“Total Calls” is the total number of Eligible Calls

“Poor Quality Calls” is the total number of Eligible Calls that are classified as poor based on numerous factors that could impact call quality in the networks managed by Microsoft. While the current Poor Call classifier is built primarily on network parameters like RTT (Roundtrip Time), Packet Loss Rate, Jitter and Packet Loss-Delay Concealment Factors, it is dynamic and continually updated based on new learnings from analysis using millions of Skype, Skype for Business, and Microsoft Teams calls and evolution of Devices, Algorithms and end user ratings.

Monthly Good Call Rate: The Monthly Good Call Rate is calculated using the following formula:

$$\frac{\text{Total Calls} - \text{Poor Quality Calls}}{\text{Total Calls}} \times 100$$

Service Credit:

Monthly Good Call Rate	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Workplace Analytics

Downtime: Any period of time when users are unable to access the Workplace Analytics website.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Yammer Enterprise

Downtime: Any period of time greater than ten minutes when more than five percent of end users are unable to post or read messages on any portion of the Yammer network for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#) / [Definitions](#)

Microsoft Azure Services and Azure Plans

For Service Specific Terms for Azure Services and Azure Plans, refer to <http://azure.microsoft.com/support/legal/sla/>.

Other Online Services

Microsoft Defender for Identity

Additional Definitions:

"Downtime" is Any period of time when the admin is unable to access the Microsoft Defender for Identity portal.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents](#) / [Definitions](#)

Bing Maps Enterprise Platform

Downtime: Any period of time when the Service is not available as measured in Microsoft's data centers, provided that you access the Service using the methods of access, authentication and tracking methods documented in the Bing Maps Platform SDKs.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

where Downtime is measured as the total number of minutes during the month when the aspects of the Service set forth above are unavailable.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to Bing Maps Enterprise Platform purchased through Open Value and Open Value Subscription volume licensing agreements.

Service Credits will not apply if: (i) you fail to implement any Services updates within the time specified in the Bing Maps Platform API's Terms of Use; and (ii) you do not provide Microsoft with at least ninety (90) days' advance notice of any known significant usage volume increase, with significant usage volume increase defined as 50% or more of the previous month's usage.

[Table of Contents / Definitions](#)

Bing Maps Mobile Asset Management

Downtime: Any period of time when the Service is not available as measured in Microsoft's data centers, provided that you access the Service using the methods of access, authentication and tracking methods documented in the Bing Maps Platform SDKs.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured as the total number of minutes during the month when the aspects of the Service set forth above are unavailable.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to Bing Maps Enterprise Platform purchased through Open Value and Open Value Subscription volume licensing agreements.

Service Credits will not apply if: (i) you fail to implement any Services updates within the time specified in the Bing Maps Platform API's Terms of Use; and (ii) you do not provide Microsoft with at least ninety (90) days' advance notice of any known significant usage volume increase, with significant usage volume increase defined as 50% or more of the previous month's usage.

[Table of Contents / Definitions](#)

Microsoft Cloud App Security

Downtime: Any period of time when the Customer's IT administrator or users authorized by Customer are unable to log on with proper credentials. Scheduled Downtime will not exceed 10 hours per calendar year.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: This Service Level does not apply to any: (i) On-premises software licensed as part of the Service subscription, or (ii) Internet-based services (excluding Microsoft Cloud App Security) that provide updates via API (application programming interface) to any services licensed as part of the Service subscription.

[Table of Contents / Definitions](#)

Microsoft Power Automate

Downtime: Any period of time when users' flows have no connectivity to Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: No SLA is provided for any free of charge tier of Microsoft Power Automate.

[Table of Contents / Definitions](#)

Microsoft Intune

Downtime: Any period of time when the Customer's IT administrator or users authorized by Customer are unable to log on with proper credentials. Scheduled Downtime will not exceed 10 hours per calendar year.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This Service Level does not apply to any: (i) On-premises software licensed as part of the Service subscription, or (ii) Internet-based services (excluding Microsoft Intune Service) that provide updates to any on-premise software licensed as part of the Service subscription.

[Table of Contents / Definitions](#)

Microsoft Kaizala Pro

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Downtime: Any period of time when end users are unable to read or post message in organizations groups for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Microsoft Power Apps

Downtime: Any period of time when users are unable to read or write any portion of data in Microsoft Power Apps to which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: No SLA is provided for any free of charge tier of Microsoft Power Apps.

[Table of Contents / Definitions](#)

Microsoft Power Virtual Agents

Additional Definitions:

“Total Message Requests” is the total number of requests made by an end user to Power Virtual Agents during a billing month.

“Failed Message Requests” are the total number of requests within Total Message Requests that Power Virtual Agents is unable to send a response message to due to a system error within Power Virtual Agents.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Message Requests} - \text{Failed Message Requests}}{\text{Total Message Requests}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%

[Table of Contents / Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Microsoft Sustainability Manager

Downtime: Any period of time when end users are unable to log into their environment. Downtime does not include Scheduled Downtime, the unavailability of Service add-on features, or the inability to access the Service due to your modifications of the Service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.5%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Minecraft: Education Edition

Downtime: Any period of time when users are unable to access Minecraft: Education Edition.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Power BI Embedded

Deployment Minutes: The total number of minutes for which a given embedded capacity has been active during a billing month.

Maximum Available Minutes: The sum of all Deployment Minutes for a specific embedded capacity provisioned by a customer in a given Microsoft Azure subscription during a billing month.

Downtime Minutes: The total accumulated Deployment Minutes during which an embedded capacity is unable to be utilized in all applicable Power BI features listed below:

View: View Power BI Dashboards, Reports, and Apps in the service.

Dataset Refresh: Schedule or manually trigger refresh operation and expect those operations to complete within expected timeframes considering all conditions that might impact refresh speeds (e.g., size of dataset).

Access Power BI Portal: Access and use the Power BI Portal within expected timeframes considering network conditions and limitations local to the customer environment or external to Microsoft.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

$$\frac{\text{Maximum Available Minutes} - \text{Downtime Minutes}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Power BI Premium

Capacity: Means a named capacity provisioned by an admin through the Power BI Premium capacity admin portal. A Capacity is a grouping of one or more nodes.

Maximum Available Minutes: The sum of all minutes that a given Capacity has been instantiated during a billing month for a given tenant.

Downtime Minutes: The total accumulated minutes in a billing month for a given Capacity, after its creation, or before it is deprovisioned when the Capacity is unable to be utilized in all applicable Power BI features listed below:

View: View Power BI Dashboards, Reports, and Apps in the service.

Dataset Refresh: Schedule or manually trigger refresh operation and expect those operations to complete within expected timeframes considering all conditions that might impact refresh speeds (e.g., size of dataset).

Access Power BI Portal: Access and use the Power BI Portal within expected timeframes considering network conditions and limitations local to the customer environment or external to Microsoft.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime Minutes}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Power BI Pro

Downtime Minutes: The total accumulated minutes in a billing month during which all Power BI features listed below are unavailable:

View: View Power BI Dashboards, Reports, and Apps in the service.

Dataset Refresh: Schedule or manually trigger refresh operation and expect those operations to complete within expected timeframes considering all conditions that might impact refresh speeds (e.g., size of dataset).

Access Power BI Portal: Access and use the Power BI Portal within expected timeframes considering network conditions and limitations local to the customer environment or external to Microsoft.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime Minutes}}{\text{Total number of minutes in a month}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)
[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

Translator API

Downtime: Any period of time when users are not able to perform translations.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured as the total number of minutes during the month when the aspects of the Service set forth above are unavailable.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Microsoft Defender for Endpoint

Additional Definitions:

“Maximum Available Minutes” is the total accumulated minutes during a billing month for Microsoft Defender for Endpoint portal. Maximum Available Minutes is measured from when the Tenant has been created resultant from successful completion of the on-boarding process.

“Tenant” represents Microsoft Defender for Endpoint customer specific cloud environment.

Downtime: The total accumulated minutes that are part of Maximum Available Minutes in which the Customer unable to access any portion of a Microsoft Defender for Endpoint portal site collections for which they have appropriate permissions and customer has a valid, active, license.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: This SLA does not apply to any trial/preview version Tenants.

[Table of Contents / Definitions](#)

Universal Print

Downtime: Any period of time when unavailability of the Universal Print Service results in the inability for users to discover printers or submit print jobs, or the inability for administrators to register or configure printers, manage access control, or monitor Universal Print status and usage.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident..

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to any trial/preview version Tenants.

[Table of Contents / Definitions](#)

Windows 365

Cloud PC: the specific instance of Windows 365 licensed to a user.

Downtime: measured in minutes, the period in which all connection attempts by a specific user to a specific Cloud PC were unsuccessful, excluding any of the following types of failures:

1. Failures resulting from the Cloud PC being in an inoperable state unrelated to the underlying Azure infrastructure (e.g. damaged or corrupt operating system, operating system configuration, or misconfiguration); and
2. Failure resulting from an application or other software installed on the Cloud PC.

Individual Downtime: means Downtime for a given user for each month.

Individual Minutes: means the User Minutes for a given user for each month.

Individual Uptime Percentage: Individual Uptime Percentage is calculated as:

$$\frac{\text{Individual Minutes} - \text{Individual Downtime}}{\text{Individual Minutes}} \times 100$$

Per-User Credit: For a month in which the Regional Uptime Percentage is less than 99.9%, a Per-User Credit shall be calculated as a percentage of the per user portion of the Applicable Monthly Service Fees for each user for whom the Individual Uptime Percentage was less than 99.9% according to the following table (provided, however, that any Individual Uptime Percentage that is lower than the Regional Uptime Percentage shall be deemed to be equal to the Regional Uptime Percentage):

Individual Uptime Percentage	Per User Credit
< 99.9%	10%
< 99%	25%
< 95%	100%

Region: means the regions detailed at: <https://aka.ms/DSLARegionLink>.

Regional Downtime: means the sum of all your Downtime in a Region for each month.

Regional Minutes: means the User Minutes in a Region for each month.

Regional Uptime Percentage: is calculated using the following formula:

$$\frac{\text{Regional Minutes} - \text{Regional Downtime}}{\text{Regional Minutes}} \times 100$$

Service Credit: for Windows 365, Service Credits are not a percentage of the Applicable Monthly Service Fee, but shall be the sum of all Per-User Credits.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Appendix A – Service Level Commitment for Virus Detection and Blocking, Spam Effectiveness, or False Positive

With respect to Exchange Online and EOP licensed as a standalone Service or via ECAL suite, or Exchange Enterprise CAL with Services, you may be eligible for Service Credits if we do not meet the Service Level described below for: (1) Virus Detection and Blocking, (2) Spam Effectiveness, or (3) False Positive. If any one of these individual Service Levels is not met, you may submit a claim for a Service Credit. If one Incident causes us to fail more than one SLA metric for Exchange Online or EOP, you may only make one Service Credit claim for that incident per Service.

1. Virus Detection and Blocking Service Level

- a. "Virus Detection and Blocking" is defined as the detection and blocking of Viruses by the filters to prevent infection. "Viruses" is broadly defined as known malware, which includes viruses, worms, and Trojan horses.
- b. A Virus is considered known when widely used commercial virus scanning engines can detect the virus and the detection capability is available throughout the EOP network.
- c. Must result from a non-purposeful infection.
- d. The Virus must have been scanned by the EOP virus filter.
- e. If EOP delivers an email that is infected with a known virus to you, EOP will notify you and work with you to identify and remove it. If this results in the prevention of an infection, you won't be eligible for a Service Credit under the Virus Detection and Blocking Service Level.
- f. The Virus Detection and Blocking Service Level shall not apply to:
 - i. Forms of email abuse not classified as malware, such as spam, phishing and other scams, adware, and forms of spyware, which due to its targeted nature or limited use is not known to the anti-virus community and thus not tracked by anti-virus products as a virus.
 - ii. Corrupt, defective, truncated, or inactive viruses contained in NDRs, notifications, or bounced emails.
- g. The Service Credit available for the Virus Detection and Blocking Service is: 25% Service Credit of Applicable Monthly Service Fee if an infection occurs in a calendar month, with a maximum of one claim allowed per calendar month.

2. Spam Effectiveness Service Level

- a. "Spam Effectiveness" is defined as the percentage of inbound spam detected by the filtering system, measured on a daily basis.
- b. Spam effectiveness estimates exclude false negatives to invalid mailboxes.
- c. The spam message must be processed by our service and not be corrupt, malformed, or truncated.
- d. The Spam Effectiveness Service Level does not apply to email containing a majority of non-English content.
- e. You acknowledge that classification of spam is subjective and accept that we will make a good faith estimation of the spam capture rate based on evidence timely supplied by you.
- f. The Service Credit available for the Spam Effectiveness Service is:

% of Calendar Month that Spam Effectiveness is below 99%	Service Credit
>25%	25%
> 50%	50%
100%	100%

3. False Positive Service Level

- a. "False Positive" is defined as the ratio of legitimate business email incorrectly identified as spam by the filtering system to all email processed by the service in a calendar month.
- b. Complete, original messages, including all headers, must be reported to the abuse team.
- c. Applies to email sent to valid mailboxes only.
- d. You acknowledge that classification of false positives is subjective and understand that we will make a good faith estimation of the false positive ratio based on evidence timely supplied by you.
- e. This False Positive Service Level shall not apply to:
 - i. bulk, personal, or pornographic email
 - ii. email containing a majority of non-English content
 - iii. email blocked by a policy rule, reputation filtering, or SMTP connection filtering
 - iv. email delivered to the junk folder
- f. The Service Credit available for the False Positive Service is:

False Positive Ratio in a Calendar Month	Service Credit
> 1:250,000	25%
> 1:10,000	50%
> 1:100	100%

Appendix B - Service Level Commitment for Uptime and Email Delivery

With respect to EOP licensed as a standalone Service, ECAL suite, or Exchange Enterprise CAL with Services, you may be eligible for Service Credits if we do not meet the Service Level described below for (1) Uptime and (2) Email Delivery.

1. **Monthly Uptime Percentage:**

If the Monthly Uptime Percentage for EOP falls below 99.999% for any given month, you may be eligible for the following Service Credit:

Monthly Uptime Percentage	Service Credit
<99.999%	25%
<99.0%	50%
<98.0%	100%

2. **Email Delivery Service Level:**

- a. "Email Delivery Time" is defined as the average of email delivery times, measured in minutes over a calendar month, where email delivery is defined as the elapsed time from when a business email enters the EOP network to when the first delivery attempt is made.
- b. Email Delivery Time is measured and recorded every 5 minutes, then sorted by elapsed time. The fastest 95% of measurements are used to create the average for the calendar month.
- c. We use simulated or test emails to measure delivery time.
- d. The Email Delivery Service Level applies only to legitimate business email (non-bulk email) delivered to valid email accounts.
- e. This Email Delivery Service Level does not apply to:
 1. Delivery of email to quarantine or archive
 2. Email in deferral queues
 3. Denial of service attacks (DoS)
 4. Email loops
- f. The Service Credit available for the Email Delivery Service is:

Average Email Delivery Time (as defined above)	Service Credit
> 1	25%
> 4	50%
> 10	100%

[Table of Contents / Definitions](#)

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

Microsoft Online Services Data Protection Addendum Last updated December 9, 2020

Published in English on December 9, 2020. Translations will be published by Microsoft when available. These commitments are binding on Microsoft as of December 9, 2020.

Table of Contents

INTRODUCTION	3	Notice and Controls on use of Subprocessors	10
Applicable DPA Terms and Updates	3	Educational Institutions	11
Electronic Notices	3	CJIS Customer Agreement	11
Prior Versions	3	HIPAA Business Associate	11
DEFINITIONS	4	California Consumer Privacy Act (CCPA)	11
GENERAL TERMS	6	Biometric Data	11
Compliance with Laws	6	How to Contact Microsoft	12
DATA PROTECTION TERMS	6	APPENDIX A – SECURITY MEASURES	13
Scope	6	ATTACHMENT 1 – NOTICES	16
Nature of Data Processing; Ownership	6	PROFESSIONAL SERVICES	16
Disclosure of Processed Data	7	California Consumer Privacy Act (CCPA)	19
Processing of Personal Data; GDPR	7	Biometric Data	19
Data Security	8	ATTACHMENT 2 – THE STANDARD CONTRACTUAL CLAUSES (PROCESSORS)	20
Security Incident Notification	9	ATTACHMENT 3 – EUROPEAN UNION GENERAL DATA PROTECTION REGULATION TERMS	27
Data Transfers and Location	10		
Data Retention and Deletion	10		
Processor Confidentiality Commitment	10		

Introduction

The parties agree that this Microsoft Online Services Data Protection Addendum (“DPA”) sets forth their obligations with respect to the processing and security of Customer Data and Personal Data in connection with the Online Services. The DPA is incorporated by reference into the Online Services Terms (or successor location in the Use Rights). The parties also agree that, unless a separate Professional Services agreement exists, this DPA governs the processing and security of Professional Services Data. Separate terms, including different privacy and security terms, govern Customer’s use of Non-Microsoft Products.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in Customer’s volume licensing, the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Personal Data, or Professional Services Data as defined herein. For clarity, consistent with Clause 10 of the Standard Contractual Clauses in [Attachment 2](#), the Standard Contractual Clauses prevail over any other term of the DPA Terms.

Microsoft makes the commitments in this DPA to all customers with volume license agreements. These commitments are binding on Microsoft with regard to Customer regardless of (1) the Use Rights that is otherwise applicable to any given Online Services subscription, or (2) any other agreement that references the OST.

Applicable DPA Terms and Updates

Limits on Updates

When Customer renews or purchases a new subscription to an Online Service, the then-current DPA Terms will apply and will not change during Customer’s subscription for that Online Service.

New Features, Supplements, or Related Software

Notwithstanding the foregoing limits on updates, when Microsoft introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), Microsoft may provide terms or make updates to the DPA that apply to Customer’s use of those new features, supplements or related software. If those terms include any material adverse changes to the DPA Terms, Microsoft will provide Customer a choice to use the new features, supplements, or related software, without loss of existing functionality of an generally available Online Service. If Customer does not use the new features, supplements, or related software, the corresponding new terms will not apply.

Government Regulation and Requirements

Notwithstanding the foregoing limits on updates, Microsoft may modify or terminate an Online Service in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects Microsoft to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for Microsoft to continue operating the Online Service without modification, and/or (3) causes Microsoft to believe the DPA Terms or the Online Service may conflict with any such requirement or obligation.

Electronic Notices

Microsoft may provide Customer with information and notices about Online Services electronically, including via email, through the portal for the Online Service, or through a web site that Microsoft identifies. Notice is given as of the date it is made available by Microsoft.

Prior Versions

The DPA Terms provide terms for Online Services that are currently available. For earlier versions of the DPA Terms, Customer may refer to <https://aka.ms/licensingdocs> or contact its reseller or Microsoft Account Manager.

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – Specific Terms](#)



[Attachments](#)

Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in the volume license agreement. The following defined terms are used in this DPA:

“Customer Data” means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data.

“Data Protection Requirements” means the GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

“Diagnostic Data” means data collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service. Diagnostic Data may also be referred to as telemetry. Diagnostic Data does not include Customer Data, Service Generated Data, or Professional Services Data.

“DPA Terms” means the terms in the DPA and any Online Service-specific terms in the Use Rights that specifically supplement or modify the privacy and security terms in the DPA for a specific Online Service (or feature of an Online Service). In the event of any conflict or inconsistency between the DPA and such Online Service-specific terms, the Online Service-specific terms shall prevail as to the applicable Online Service (or feature of that Online Service).

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Local EU/EEA Data Protection Laws” means any subordinate legislation and regulation implementing the GDPR.

“GDPR Terms” means the terms in [Attachment 3](#), under which Microsoft makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

“Personal Data” means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Professional Services Data” means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from an Online Service) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services. Professional Services Data includes Support Data.

“Service Generated Data” means data generated or derived by Microsoft through the operation of an Online Service. Service Generated Data does not include Customer Data, Diagnostic Data, or Professional Services Data.

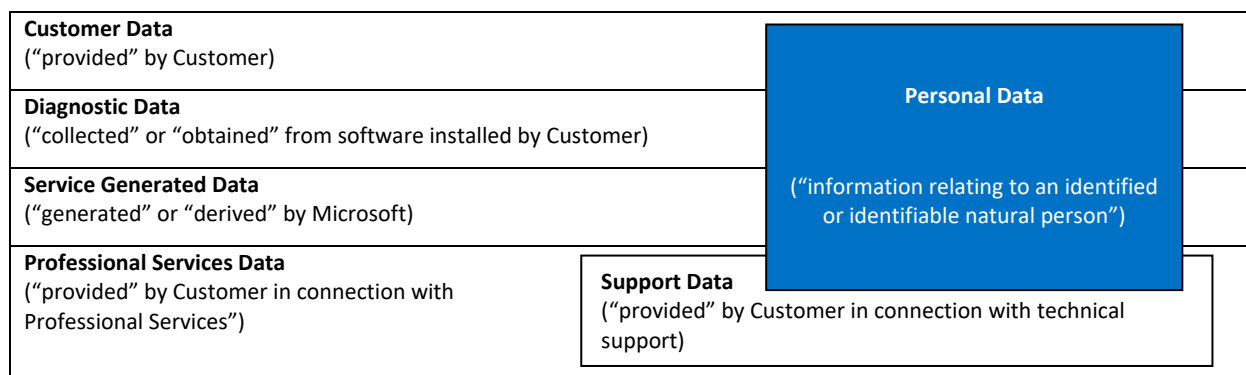
“Standard Contractual Clauses” means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010. The Standard Contractual Clauses are in [Attachment 2](#).

“Subprocessor” means other processors used by Microsoft to process Customer Data and Personal Data, as described in Article 28 of the GDPR.

“Support Data” means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by or on behalf of Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain technical support for Online Services covered under this agreement. Support Data is a subset of Professional Services Data.

Lower case terms used but not defined in this DPA, such as “personal data breach”, “processing”, “controller”, “processor”, “profiling”, “personal data”, and “data subject” will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies. The terms “data importer” and “data exporter” have the meanings given in the Standard Contractual Clauses.

For clarity, and as detailed above, data defined as Customer Data, Diagnostic Data, Service Generated Data, and Professional Services Data may contain Personal Data. For illustrative purposes, please see the chart inserted below:



Above is a visual representation of the data types defined in the DPA. All Personal Data is processed as a part of one of the other data types (all of which also include non-personal data). Support Data is a sub-set of Professional Services Data. The DPA Terms focus on Customer Data and Personal Data (with Professional Services Data, including Support Data and any Personal Data in Professional Services Data and Support Data, covered in Attachment 1).

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Data Protection Terms](#)



[Attachments](#)

General Terms

Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law and Data Protection Requirements. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Microsoft does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all Federal laws and regulations of the United States applicable to its use of Online Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Protection Addendum, Attachment 2 - Standard Contractual Clauses, Attachment 3 – European Union General Data Protection Regulation Terms (GDPR), EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States. Customer is responsible for determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Online Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of an Online Service, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Data Protection Terms

This section of the DPA includes the following subsections:

- Scope
- Nature of Data Processing; Ownership
- Disclosure of Processed Data
- Processing of Personal Data; GDPR
- Data Security
- Security Incident Notification
- Data Transfers and Location
- Data Retention and Deletion
- Processor Confidentiality Commitment
- Notice and Controls on Use of Subprocessors
- Educational Institutions
- CJIS Customer Agreement
- HIPAA Business Associate
- California Consumer Privacy Act (CCPA) Terms
- Biometric Data
- How to Contact Microsoft
- Appendix A – Security Measures

Scope

The DPA Terms apply to all Online Services except any Online Services specifically identified as excluded in Attachment 1 to the OST (or successor location in the Use Rights), which are governed by the privacy and security terms in the applicable Online Service specific terms.

Previews may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise noted, Customer should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements. The following terms in this DPA do not apply to Previews: Processing of Personal Data; GDPR, Data Security, and HIPAA Business Associate.

[Attachment 1](#) to the DPA includes the privacy and security terms for Professional Services Data, including any Personal Data therein, in connection with the provision of Professional Services. Therefore, unless expressly made applicable in [Attachment 1](#), the terms in this DPA do not apply to the provision of Professional Services.

Nature of Data Processing; Ownership

Microsoft will use and otherwise process Customer Data and Personal Data only in accordance with Customer's documented instructions and as described and subject to the limitations provided below (a) to provide Customer the Online Services, and (b) for Microsoft's legitimate business operations incident to delivery of the Online Services to Customer. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Processing to Provide Customer the Online Services

For purposes of this DPA, "to provide" an Online Service consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, and security).

When providing Online Services, Microsoft will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.

Processing for Microsoft's Legitimate Business Operations

For purposes of this DPA, "Microsoft's legitimate business operations" consist of the following, each as incident to delivery of the Online Services to Customer: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Processed Data outlined below).

When processing for Microsoft's legitimate business operations, Microsoft will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section.

Disclosure of Processed Data

Microsoft will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Personal Data; and (c) any other data processed by Microsoft in connection with the Online Service that is Customer's confidential information under the volume license agreement. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under the volume license agreement.

Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.

Processing of Personal Data; GDPR

All Personal Data processed by Microsoft in connection with the Online Services is obtained as either Customer Data, Diagnostic Data, or Service Generated Data. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data. Pseudonymized identifiers may be included in Diagnostic Data or Service Generated Data and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in [Attachment 3](#) govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in the Online Service Specific terms or this DPA. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its volume licensing agreement (including the DPA Terms and any applicable updates), along with the product documentation and Customer's use and configuration of features in the Online Services, are Customer's complete documented instructions to Microsoft for the processing of Personal Data. Information on use and configuration of the Online Services can be found at <https://docs.microsoft.com/en-us/> or a successor location. Any additional or alternate instructions must be agreed to according to the process for amending Customer's volume licensing agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Microsoft that Customer's instructions, including appointment of Microsoft as a processor or subprocessor, have been authorized by the relevant controller.

To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR for Microsoft's legitimate business operations incident to delivery of the Online Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use. Microsoft is accepting the added responsibilities of a data "controller" under GDPR for processing in connection with its legitimate business operations to: (a) act consistent with regulatory requirements, to the extent required under GDPR; and (b) provide increased transparency to Customers and confirm Microsoft's accountability for such processing. Microsoft employs safeguards to protect Customer Data and Personal

Data in processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR. With respect to processing of Personal Data under this paragraph, Microsoft makes the commitments set forth in Appendix 3 to Attachment 2 – The Standard Contractual Clauses (Processors) of the DPA; for those purposes, (i) any Microsoft disclosure of Personal Data, as described in Appendix 3, that has been transferred in connection with Microsoft’s legitimate business operations is deemed a “Relevant Disclosure” and (ii) the commitments in that Appendix 3 apply to such Personal Data.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled “Nature of Data Processing; Ownership” above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Online Service pursuant to Customer’s volume licensing agreement and for Microsoft’s legitimate business operations incident to delivery of the Online Service to Customer (as further described in the section of this DPA entitled “Nature of Data Processing; Ownership” above).
- **Categories of Data.** The types of Personal Data processed by Microsoft when providing the Online Service include: (i) Personal Data that Customer elects to include in Customer Data; and (ii) those expressly identified in Article 4 of the GDPR that may be contained in Diagnostic Data or Service Generated Data. The types of Personal Data that Customer elects to include in Customer Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in [Appendix 1 to Attachment 2](#) – The Standard Contractual Clauses (Processors) of the DPA.
- **Data Subjects.** The categories of data subjects are Customer’s representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in [Appendix 1 to Attachment 2](#) – The Standard Contractual Clauses (Processors) of the DPA.

Data Subject Rights; Assistance with Requests

Microsoft will make available to Customer, in a manner consistent with the functionality of the Online Service and Microsoft’s role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Microsoft receives a request from Customer’s data subject to exercise one or more of its rights under the GDPR in connection with an Online Service for which Microsoft is a data processor or subprocessor, Microsoft will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Online Service. Microsoft shall comply with reasonable requests by Customer to assist with Customer’s response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires Microsoft to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Microsoft and keep it accurate and up-to-date. Microsoft may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with descriptions of the security controls in place for the Online Service and other information reasonably requested by Customer regarding Microsoft security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. Each Core Online Service also complies with the control standards and frameworks shown in the table in Attachment 1 to the OST (or successor location in the Use Rights) and implements and maintains the security measures set forth in Appendix A for the protection of Customer Data.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate ISO 27001, ISO 27002, ISO 27018 or the standards or frameworks in the table in Attachment 1 to the OST (or successor location in the Use Rights), unless it is no longer used in the industry and it is replaced with a successor (if any).

Data Encryption

Customer Data (including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default.

Microsoft also encrypts Customer Data stored at rest in Online Services. In the case of Online Services on which Customer or a third-party acting on Customer's behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties.

Data Access

Microsoft employs least privilege access mechanisms to control access to Customer Data (including any Personal Data therein). For Core Online Services, Microsoft maintains Access Control mechanisms described in the table entitled "Security Measures" in Appendix 1 – Notices, and there is no standing access by Microsoft personnel to Customer Data. Role-based access controls are employed to ensure that access to Customer Data required for service operations is for an appropriate purpose, for a limited time, and approved with management oversight.

Customer Responsibilities

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for an Online Service meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Microsoft provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer's virtual machine or application).

Auditing Compliance

Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at <https://servicetrust.microsoft.com/> or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor. If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

To the extent Customer's audit requirements under the Standard Contractual Clauses or Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, Microsoft will promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and Microsoft will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Microsoft to unreasonably delay performance of the audit. To the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data and Personal Data by Microsoft, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Microsoft, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Microsoft's other customers or to Microsoft systems or facilities not involved in the Online Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Microsoft expends for any such audit, in addition to the rates for services performed by Microsoft. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material non-compliance.

If the Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Requirements. Microsoft Corporation is an intended third-party beneficiary of this section.

Security Incident Notification

If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Microsoft's notification of or response to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

Data Transfers and Location

Data Transfers

Customer Data and Personal Data that Microsoft processes on Customer's behalf may not be transferred to, or stored and processed in a geographic location except in accordance with the DPA Terms and the safeguards provided below in this section. Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data and Personal Data to provide the Online Services, except as described elsewhere in the DPA Terms.

All transfers of Customer Data and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Online Services shall be governed by the Standard Contractual Clauses in [Attachment 2](#).

Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail, although Microsoft does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18. Microsoft agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

Location of Customer Data at Rest

For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as set forth in Attachment 1 to the OST (or successor location in the Use Rights).

Microsoft does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

Data Retention and Deletion

At all times during the term of Customer's subscription, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service.

Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data within an additional 90 days, unless Microsoft is permitted or required by applicable law, or authorized under this DPA, to retain such data.

The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data or Personal Data as described in this section.

Processor Confidentiality Commitment

Microsoft will ensure that its personnel engaged in the processing of Customer Data and Personal Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Customer Data and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors

Microsoft may hire Subprocessors to provide certain limited or ancillary services on its behalf. Customer consents to this engagement and to Microsoft Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Microsoft of the processing of Customer Data and Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Microsoft is responsible for its Subprocessors' compliance with Microsoft's obligations in this DPA. Microsoft makes available information about Subprocessors on a Microsoft website. When engaging any Subprocessor, Microsoft will ensure via a written contract that the Subprocessor may access and use Customer Data or Personal Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Customer Data or Personal Data for any other purpose. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 6 months in advance of providing that Subprocessor with access to Customer Data. Additionally, Microsoft will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 30 days in advance of providing that Subprocessor with access to Personal Data other than that which is contained in Customer Data. If Microsoft engages a new Subprocessor for a new Online Service, Microsoft will give Customer notice prior to availability of that Online Service.

If Customer does not approve of a new Subprocessor, then Customer may terminate any subscription for the affected Online Service without penalty by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Microsoft to re-evaluate any such new Subprocessor based on the applicable concerns. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for any subscriptions for the terminated Online Service from subsequent invoices to Customer or its reseller.

Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Microsoft acknowledges that for the purposes of the DPA, Microsoft is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that Microsoft may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Microsoft to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Microsoft's possession as may be required under applicable law.

CJIS Customer Agreement

Microsoft provides certain government cloud services ("Covered Services") in accordance with the FBI Criminal Justice Information Services ("CJIS") Security Policy ("CJIS Policy"). The CJIS Policy governs the use and transmission of criminal justice information. All Microsoft CJIS Covered Services shall be governed by the terms and conditions in the CJIS Customer Agreement located here: <http://aka.ms/CJISCustomerAgreement>.

HIPAA Business Associate

If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data as those terms are defined in 45 CFR § 160.103, execution of Customer's volume licensing agreement includes execution of the HIPAA Business Associate Agreement ("BAA"), the full text of which identifies the Online Services to which it applies and is available at <http://aka.ms/BAA>. Customer may opt out of the BAA by sending the following information to Microsoft in a written notice (under the terms of the Customer's volume licensing agreement):

- the full legal name of the Customer and any Affiliate that is opting out; and
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the opt out applies.

California Consumer Privacy Act (CCPA)

If Microsoft is processing Personal Data within the scope of the CCPA, Microsoft makes the following additional commitments to Customer. Microsoft will process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any "sale" exemption. In no event will Microsoft sell any such data. These CCPA terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the DPA Terms, Use Rights, or other agreement between Microsoft and Customer.

Biometric Data

If Customer uses an Online Service to process Biometric Data, Customer is responsible for: (i) providing notice to data subjects, including with respect to retention periods and destruction; (ii) obtaining consent from data subjects; and (iii) deleting the Biometric Data, all as appropriate and required under applicable Data Protection Requirements. Microsoft will process that Biometric Data following Customer's documented instructions (as described in the "Processor and Controller Roles and Responsibilities" section above) and protect that Biometric Data in accordance with the data security and protection terms under this DPA. For purposes of this section, "Biometric Data" will have the meaning set forth in Article 4 of the GDPR and, if applicable, equivalent terms in other Data Protection Requirements.

How to Contact Microsoft

If Customer believes that Microsoft is not adhering to its privacy or security commitments, Customer may contact customer support or use Microsoft's Privacy web form, located at <http://go.microsoft.com/?linkid=9846224>. Microsoft's mailing address is:

Microsoft Enterprise Service Privacy

Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. The privacy representative of Microsoft Ireland Operations Limited can be reached at the following address:

Microsoft Ireland Operations, Ltd.

Attn: Data Protection
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Data Protection Terms](#)



[Attachments](#)

Appendix A – Security Measures

Microsoft has implemented and will maintain for Customer Data in the Core Online Services the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms), are Microsoft's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	<p>Security Ownership. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.</p> <p>Security Roles and Responsibilities. Microsoft personnel with access to Customer Data are subject to confidentiality obligations.</p> <p>Risk Management Program. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service.</p> <p>Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.</p>
Asset Management	<p>Asset Inventory. Microsoft maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access.</p> <p>Asset Handling</p> <ul style="list-style-type: none"> - Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities.
Human Resources Security	<p>Security Training. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.</p>
Physical and Environmental Security	<p>Physical Access to Facilities. Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.</p> <p>Physical Access to Components. Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain.</p> <p>Protection from Disruptions. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.</p> <p>Component Disposal. Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.</p>
Communications and Operations Management	<p>Operational Policy. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.</p> <p>Data Recovery Procedures</p> <ul style="list-style-type: none"> - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered. - Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - Microsoft has specific procedures in place governing access to copies of Customer Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months. - Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. <p>Malicious Software. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.</p> <p>Data Beyond Boundaries</p>

Domain	Practices
	<ul style="list-style-type: none"> - Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - Microsoft restricts access to Customer Data in media leaving its facilities. <p>Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.</p>
Access Control	<p>Access Policy. Microsoft maintains a record of security privileges of individuals having access to Customer Data.</p> <p>Access Authorization</p> <ul style="list-style-type: none"> - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. <p>Least Privilege</p> <ul style="list-style-type: none"> - Technical support personnel are only permitted to have access to Customer Data when needed. - Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function. <p>Integrity and Confidentiality</p> <ul style="list-style-type: none"> - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force. <p>Authentication</p> <ul style="list-style-type: none"> - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. <p>Network Design. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.</p>
Information Security Incident Management	<p>Incident Response Process</p> <ul style="list-style-type: none"> - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the “Security Incident Notification” section above) will be made without undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. <p>Service Monitoring. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.</p>

Domain	Practices
Business Continuity Management	<ul style="list-style-type: none">- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data are located.- Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

[Table of Contents](#) / [General Terms](#)[Table of Contents](#)[Introduction](#)[General Terms](#)[Data Protection Terms](#)[Attachments](#)

Attachment 1 – Notices

Professional Services

Professional Services are provided subject to the “Professional Services Terms” below. If, however, Professional Services are provided pursuant to a separate agreement, then the terms of that separate agreement will apply to those Professional Services.

The Professional Services to which this Notice applies are not Online Services, and the rest of the Use Rights and DPA do not apply unless expressly made applicable by the Professional Services Terms below.

Processing of Professional Services Data; Ownership

Microsoft will use and otherwise process Professional Services Data only in accordance with Customer’s documented instructions and as described and subject to the limitations provided below (a) to provide Customer the Professional Services, and (b) for Microsoft’s legitimate business operations incident to delivery of the Professional Services to Customer. As between the parties, Customer retains all right, title and interest in and to Professional Services Data. Microsoft acquires no rights in Professional Services Data, other than the rights Customer grants to Microsoft to provide the Professional Services to Customer. This paragraph does not affect Microsoft’s rights in software or services Microsoft licenses to Customer.

Processing to Provide Customer the Professional Services

For purposes of this DPA, “to provide” Professional Services consists of:

- Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services;
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents); and
- Ongoing improvement (maintaining the Professional Services, including installing the latest updates, and making improvements to the reliability, efficacy, quality, and security).

When providing Professional Services, Microsoft will not use or otherwise process Professional Services Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer’s documented instructions.

Processing for Microsoft’s Legitimate Business Operations

For purposes of this DPA, “Microsoft’s legitimate business operations” consist of: (1) billing and account management; (2) compensation (e.g., calculating employee commissions); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting or compliance with legal obligations (subject to the limitations on disclosure outlined below), each incident to the delivery of the Professional Services to Customer.

When processing for Microsoft’s legitimate business operations, Microsoft will not use or otherwise process Professional Services Data for: (a) user profiling, or (b) advertising or similar commercial purposes or (c) any other purpose, other than purposes set out in this section.

Disclosure of Professional Services Data

The “Disclosure of Processed Data” provision of the Data Protection Terms section of the DPA applies to Customer’s Professional Services engagement with respect to Professional Services Data.

Processing of Personal Data; GDPR

Personal Data provided to Microsoft by, or on behalf of, Customer through an engagement with Microsoft to obtain Professional Services is also Professional Services Data.

To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in [Attachment 3](#) govern that processing and the parties also agree to the following terms in this sub-section (“Processing of Personal Data; GDPR”):

Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data included in Professional Services Data and Microsoft is the processor, except (a) when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in these Professional Services Terms. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its volume licensing agreement (including the DPA Terms and any applicable updates), along with any statement of services agreed between the parties, are Customer’s complete and final documented instructions to Microsoft for the processing of Personal Data contained within Professional Services Data. Any additional or alternate instructions must be

agreed to according to the process for amending Customer's volume licensing agreement or statements of services. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Microsoft that Customer's instructions, including appointment of Microsoft as a processor or subprocessor, have been authorized by the relevant controller.

To the extent Microsoft uses or otherwise processes Professional Services Data subject to the GDPR for Microsoft's legitimate business operations incident to delivery of the Professional Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use. Microsoft is accepting the added responsibilities of a data "controller" under GDPR for processing in connection with its legitimate business operations to: (a) act consistent with regulatory requirements, to the extent required under GDPR; and (b) provide increased transparency to Customers and confirm Microsoft's accountability for such processing. Microsoft employs safeguards to protect Professional Service Data in processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR. With respect to processing of Personal Data under this paragraph, Microsoft makes the commitments set forth in Appendix 3 to Attachment 2 – The Standard Contractual Clauses (Processors) of the DPA; for those purposes, (i) any Microsoft disclosure of Personal Data, as described in Appendix 3, that has been transferred in connection with Microsoft's legitimate business operations is deemed a "Relevant Disclosure" and (ii) the commitments in that Appendix 3 apply to such Personal Data.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of these Professional Services Terms entitled "Processing of Professional Services Data; Ownership" above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and these Professional Services Terms.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide Professional Services pursuant to Customer's volume licensing agreement and any statement of services, and for Microsoft's legitimate business operations incident to delivery of the Professional Services to Customer (as further described in the section of these Professional Services Terms entitled "Processing of Professional Services Data; Ownership" above).
- **Categories of Data.** The types of Personal Data processed by Microsoft in connection with the provision of Professional Services include (i) Personal Data that Customer elects to include in Professional Services Data; and (ii) those expressly identified in Article 4 of the GDPR. The types of Personal Data that Customer elects to include in Professional Services Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in [Appendix 1 to Attachment 2](#) – The Standard Contractual Clauses (Processors) of the DPA.
- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in [Appendix 1 to Attachment 2](#) – The Standard Contractual Clauses (Processors) of the DPA.

Data Subject Rights; Assistance with Requests

For Professional Services Data that Customer stores in an Online Service, Microsoft will abide by the obligations set forth in the "Data Subject Rights; Assistance with Requests" provision of the Data Protection Terms section of the DPA. For other Professional Services Data, Microsoft will delete or return all copies of Professional Services Data in accordance with the "Data Deletion or Return" section below.

Records of Processing Activities

To the extent the GDPR requires Microsoft to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Microsoft and keep it accurate and up-to-date. Microsoft may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Professional Services Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

Customer Responsibilities

The "Customer Responsibilities" provision of the Data Protection Terms section of the DPA applies to Customer's Professional Services engagement with respect to Professional Services Data. In addition, with respect to Customer's Professional Services engagement, Customer agrees not to provide any Professional Services Data, other than Support Data, to Microsoft which would be subject to regulations under the

Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) or the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191) (HIPAA).

Security Incident Notification

The “Security Incident Notification” provision of the Data Protection Terms section of the DPA applies to Customer’s Professional Services engagement with respect to Professional Services Data.

Data Transfers

Professional Services Data that Microsoft processes on Customer’s behalf may not be transferred to, or stored and processed in a geographic location except in accordance with the Professional Services Terms and the safeguards provided below in this section. Taking into account such safeguards, Customer appoints Microsoft to transfer Professional Services Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Professional Services Data to provide the Professional Services, except as described elsewhere in the Professional Services Terms.

All transfers of Professional Services Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Professional Services shall be governed by the Standard Contractual Clauses in Attachment 2.

Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail, although Microsoft does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18. Microsoft agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

Data Deletion or Return

Microsoft will delete or return all copies of Professional Services Data after the business purposes for which the Professional Services Data was collected or transferred have been fulfilled or earlier upon Customer’s request, unless Microsoft is permitted or required by applicable law, or authorized under this DPA, to retain such data.

Processor Confidentiality Commitment

Microsoft will ensure that its personnel engaged in the processing of Professional Services Data (i) will process such data only on instructions from Customer or as described in these Professional Services Terms, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Professional Services Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors

Microsoft may hire Subprocessors to provide certain limited or ancillary services on its behalf. Customer consents to this engagement and to Microsoft Affiliates as Subprocessors. The above authorizations will constitute Customer’s prior written consent to the subcontracting by Microsoft of the processing of Professional Services Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Microsoft is responsible for its Subprocessors of Professional Services Data compliance with Microsoft’s obligations in [Attachment 1](#) of the DPA. Microsoft will ensure via a written contract that the Subprocessor may access and use Professional Services Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Professional Services Data for any other purpose. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by these Professional Services Terms. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

With respect to Professional Services Data other than Support Data, a list of Microsoft’s Subprocessors is available upon request. If such list is requested, at least 30 days before authorizing any new Subprocessor to access Personal Data, Microsoft will update the list and provide Customer with a mechanism to obtain notice of that update.

If Customer does not approve of a new Subprocessor, then Customer may terminate the affected Professional Services engagement by providing, before the end of the notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Microsoft to re-evaluate any such new Subprocessor based on the applicable concerns.

With respect to Support Data, Microsoft’s use of Subprocessors in connection with the provision of technical support for Online Services is governed by the same restrictions and procedures that govern its use of Subprocessors in connection with the Online Services set forth in the “Notice and Controls on use of Subprocessors” provision in the DPA.

Additional Terms for Support Data

Security of Support Data

Microsoft will implement and maintain appropriate technical and organizational measures to protect Support Data. Those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018

Educational Institutions

Microsoft's acknowledgements and agreements and Customer's responsibilities to obtain parental consent and convey notification set out in the "Educational Institutions" provision in the Data Protection Terms section of the DPA also apply with respect to Support Data.

California Consumer Privacy Act (CCPA)

If Microsoft is processing Personal Data within the scope of the CCPA, Microsoft makes the following additional commitments to Customer. Microsoft will process Professional Services Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any "sale" exemption. In no event will Microsoft sell any such data. These CCPA terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the DPA Terms, Use Rights, or other agreement between Microsoft and Customer.

Biometric Data

If Customer uses a Professional Service to process Biometric Data, Customer is responsible for: (i) providing notice to data subjects, including with respect to retention periods and destruction; (ii) obtaining consent from data subjects; and (iii) deleting the Biometric Data, all as appropriate and required under applicable Data Protection Requirements. Microsoft will process that Biometric Data following Customer's documented instructions (as described in the "Processor and Controller Roles and Responsibilities" section above) and protect that Biometric Data in accordance with the data security and protection terms under this DPA. For purposes of this section, "Biometric Data" will have the meaning set forth in Article 4 of the GDPR and, if applicable, equivalent terms in other Data Protection Requirements.

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Data Protection Terms](#)



[Attachments](#)

Attachment 2 – The Standard Contractual Clauses (Processors)

Execution of the volume licensing agreement by Customer includes execution of this Attachment 2, which is countersigned by Microsoft Corporation.

In countries where regulatory approval is required for use of the Standard Contractual Clauses, the Standard Contractual Clauses cannot be relied upon under European Commission 2010/87/EU (of February 2010) to legitimize export of data from the country, unless Customer has the required regulatory approval.

Beginning May 25, 2018 and thereafter, references to various Articles from the Directive 95/46/EC in the Standard Contractual Clauses below will be treated as references to the relevant and appropriate Articles in the GDPR.

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and Microsoft Corporation (as data importer, whose signature appears below), each a “party,” together “the parties,” have agreed on the following Contractual Clauses (the “Clauses” or “Standard Contractual Clauses”) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law.

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

Data exporter: Customer is the data exporter. The data exporter is a user of Online Services or Professional Services as defined in the DPA and OST.

Data importer: The data importer is MICROSOFT CORPORATION, a global producer of software and services.

Data subjects: Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. Microsoft acknowledges that, depending on Customer's use of the Online Service or Professional Services, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of data: The personal data transferred that is included in e-mail, documents and other data in an electronic form in the context of the Online Services or Professional Services. Microsoft acknowledges that, depending on Customer's use of the Online Service or Professional Services, Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified in Article 4 of the GDPR.

Processing operations: The personal data transferred will be subject to the following basic processing activities:

a. Duration and Object of Data Processing. The duration of data processing shall be for the term designated under the applicable volume licensing agreement between data exporter and the Microsoft entity to which these Standard Contractual Clauses are annexed ("Microsoft"). The objective of the data processing is the performance of Online Services and Professional Services.

b. Scope and Purpose of Data Processing. The scope and purpose of processing personal data is described in the "Processing of Personal Data; GDPR" section of the DPA. The data importer operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities in accordance with the "Security Practices and Policies" section of the DPA.

c. Customer Data and Personal Data Access. For the term designated under the applicable volume licensing agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data and personal data, or (2) make such corrections, deletions, or blockages on its behalf.

d. Data Exporter's Instructions. For Online Services and Professional Services, data importer will only act upon data exporter's instructions as conveyed by Microsoft.

e. Customer Data and Personal Data Deletion or Return. Upon expiration or termination of data exporter's use of Online Services or Professional Services, it may extract Customer Data and personal data and data importer will delete Customer Data and personal data, each in accordance with the DPA Terms applicable to the agreement.

Subcontractors: In accordance with the DPA, the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data and personal data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data and personal data for any other purpose.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. Personnel. Data importer's personnel will not process Customer Data or personal data without authorization. Personnel are obligated to maintain the confidentiality of any such Customer Data and personal data and this obligation continues even after their engagement ends.

2. Data Privacy Contact. The data privacy officer of the data importer can be reached at the following address:

Microsoft Corporation
Attn: Chief Privacy Officer
1 Microsoft Way
Redmond, WA 98052 USA

3. Technical and Organization Measures. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data and personal data, as defined in the Security Practices and Policies section of the DPA, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in the Security Practices and Policies section of the DPA are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Appendix 3 to the Standard Contractual Clauses

Additional Safeguards Addendum

By this Additional Safeguards Addendum to Standard Contractual Clauses (this "Addendum"), Microsoft Corporation ("Microsoft") provides additional safeguards to Customer and additional redress to the data subjects to whom Customer's personal data relates.

This Addendum supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses.

1. Challenges to Orders. In addition to Clause 5(d)(i) of the Standard Contractual Clauses, in the event Microsoft receives an order from any third party for compelled disclosure of any personal data that has been transferred under the Standard Contractual Clauses, Microsoft shall:

- a. use every reasonable effort to redirect the third party to request data directly from Customer;
- b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and
- c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable Member State law.

For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2. Indemnification of Data Subjects. Subject to Sections 3 and 4, Microsoft shall indemnify a data subject for any material or non-material damage to the data subject caused by Microsoft's disclosure of personal data of the data subject that has been transferred under the Standard Contractual Clauses in response to an order from a non-EU/EEA government body or law enforcement agency (a "Relevant Disclosure"). Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under this Section 2 to the extent the data subject has already received compensation for the same damage, whether from Microsoft or otherwise.

3. Conditions of Indemnification. Indemnification under Section 2 is conditional upon the data subject establishing, to Microsoft's reasonable satisfaction, that:

- a. Microsoft engaged in a Relevant Disclosure;
- b. the Relevant Disclosure was the basis of an official proceeding by the non-EU/EEA government body or law enforcement agency against the data subject; and

- c. the Relevant Disclosure directly caused the data subject to suffer material or non-material damage.

The data subject bears the burden of proof with respect to conditions a. through c.

Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under Section 2 if Microsoft establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

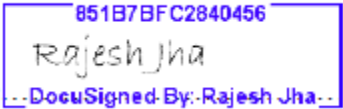
4. Scope of Damages. Indemnification under Section 2 is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Microsoft's infringement of the GDPR.

5. Exercise of Rights. Rights granted to data subjects under this Addendum may be enforced by the data subject against Microsoft irrespective of any restriction in Clauses 3 or 6 of the Standard Contractual Clauses. The data subject may only bring a claim under this Addendum on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Addendum are personal to the data subject and may not be assigned.

6. Notice of Change. In addition to Clause 5(b) of the Standard Contractual Clauses, Microsoft agrees and warrants that it has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the data exporter and its obligations under this Addendum or the Standard Contractual Clauses and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum or the Standard Contractual Clauses, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract.

7. Termination. This Addendum shall automatically terminate if the European Commission, a competent Member State supervisory authority, or an EU or competent Member State court approves a different lawful transfer mechanism that would be applicable to the data transfers covered by the Standard Contractual Clauses (and if such mechanism applies only to some of the data transfers, this Addendum will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Addendum.

Signing the Standard Contractual Clauses, Appendix 1, Appendix 2 and Appendix 3 on behalf of the data importer:

Signature  851B7BFC2840456
DocuSigned By: Rajesh Jha

Rajesh Jha, Executive Vice President

Microsoft Corporation

One Microsoft Way, Redmond WA, USA 98052

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Data Protection Terms](#)



[Attachments](#)

Attachment 3 – European Union General Data Protection Regulation Terms

Microsoft makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon Microsoft with regard to Customer regardless of (1) the version of the OST and DPA that is otherwise applicable to any given Online Services subscription or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Microsoft on behalf of Customer. These GDPR Terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the Use Rights or other agreement between Microsoft and Customer. These GDPR Terms do not apply where Microsoft is a controller of Personal Data.

Relevant GDPR Obligations: Articles 28, 32, and 33

1. Microsoft shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, Microsoft shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))
2. Processing by Microsoft shall be governed by these GDPR Terms under European Union (hereafter “Union”) or Member State law and are binding on Microsoft with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer’s licensing agreement, including these GDPR Terms. In particular, Microsoft shall:
 - (a) process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Microsoft is subject; in such a case, Microsoft shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - (b) ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - (c) take all measures required pursuant to Article 32 of the GDPR;
 - (d) respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;
 - (e) taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III of the GDPR;
 - (f) assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Microsoft;
 - (g) at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;
 - (h) make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Microsoft shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

3. Where Microsoft engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Microsoft shall remain fully liable to the Customer for the performance of that other processor’s obligations. (Article 28(4))

4. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and Microsoft shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymisation and encryption of Personal Data;

- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))

5. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Article 32(2))

6. Customer and Microsoft shall take steps to ensure that any natural person acting under the authority of Customer or Microsoft who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4))

7. Microsoft shall notify Customer without undue delay after becoming aware of a Personal Data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Microsoft.

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Data Protection Terms](#)



[Attachments](#)