Microsoft Procurement

Supplier Security & Privacy Assurance (SSPA) Program Guide

Version 11

April 2025

Table of Contents

SSPA Program Overview 3
SSPA Data Processing Profile 3
Scope 7
Personal Data by Data Type 7
Microsoft Confidential Data 10
Processing Location 11
Data Processing Role 11
Payment Card Processing 12
PCI Certification Requirement 12
Software as a Service (SaaS) 12
Use of Subcontractors 13
Website Hosting 13
Healthcare 14
Artificial Intelligence (AI) Systems 14
SSPA Process Overview 14
What is SSPA? 14
SSPA Process Diagram – New Supplier Enrollment 15
SSPA Process Diagram – Annual Supplier Renewal 15
Assurance Requirements 16
Self-Attestation to the DPR 16
Independent Assessment Requirement 17
Profiles requiring additional independent assurance: 18
Data Incidents 18

SSPA Program Overview

The Supplier Security and Privacy Assurance ("**SSPA**") Program is a partnership between Microsoft Procurement, Corporate External and Legal Affairs, Corporate Security, and the Office of Responsible AI to ensure privacy and security and responsible AI principles are followed by our suppliers. This corporate program is in place to deliver Microsoft's baseline data processing instructions to our suppliers globally, in the form of the Microsoft Supplier Data Protection Requirements ("DPR"), available on the SSPA page on Microsoft.com/Procurement.

Suppliers are enabled to make Data Processing Profile selections that align to the goods and/or services you are contracted to Perform. These selections trigger corresponding requirements to provide compliance assurances to Microsoft.

All enrolled suppliers will complete a self-attestation of compliance to the DPR annually. Your Data Processing Profile determines whether the full DPR is issued or if a subset of requirements applies. Suppliers that process what Microsoft considers higher risk data may also need to meet additional requirements, such as providing independent verification of compliance (see Independent Assessment). Note that suppliers may have to meet additional organizational level requirements that are decided and communicated independently of SSPA by the Microsoft group responsible for the engagement with supplier.

Important: Completed compliance activities determine an SSPA Status of Green (compliant) or Red (non-compliant) and Data Processing approvals (see below for Data Processing Profile). Microsoft purchasing tools validate the SSPA Status is Green (for each supplier in scope for SSPA) and requisite approvals prior to allowing an engagement to move forward.

SSPA Data Processing Profile

Microsoft suppliers have control over their SSPA Data Processing Profile. The approvals chosen in the Data Processing Profile help SSPA evaluate the risk level of your engagement(s) with Microsoft. SSPA compliance requirements vary based on the Data Processing Profile and its associated approvals, allowing suppliers to determine which engagements they want to be eligible for. It is important to carefully consider the selections and the compliance activity that must be completed to obtain approval.

Microsoft business groups will only be able to create engagements with suppliers where the data processing activity matches the approvals the supplier obtained.

Suppliers have the ability to update their Data Processing Profile at any point, if there are no open tasks. If any changes are made, the applicable compliance activity (tasks) will be issued and must be completed before new approvals will be reflected to your Data Processing Profile. The existing, completed approvals will apply until newly issued requirements are completed. If the new tasks are not completed within the 90-day time frame allowed, your SSPA Status will turn to Red (non-compliant), and the account is at risk of being deactivated from Microsoft Accounts Payable systems.

There are combinations that may elevate or reduce compliance requirements. The combinations are captured in the table below and this is what you can expect to execute from the Microsoft Supplier Compliance Portal upon completing your profile. You can always validate how your scenario fits into this framework by requesting an SSPA team review.

SSPA Data Processing Profile Table

#	Profile	Requirements	Independent Assurance Options
1	**Scope**: Personal & Confidential **Processing Location:** At Microsoft or Customer **Processing Role:** Processor or Controller **Data Class:** Confidential or Highly Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A or YES **Website Hosting:** N/A or YES **Healthcare:** N/A or YES	Self-attestation to the DPR	
2	**Scope:** Confidential **Processing Location:** At Supplier **Processing Role:** N/A **Data Class:** Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation to the DPR	
3	**Scope:** Confidential **Processing Location:** At Supplier **Processing Role:** N/A **Data Class:** Highly Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR **and** Independent Assurance of compliance	Independent Assurance options: 1. Complete an Independent Assessment against the DPR, **or** 2. Submit ISO 27001
4	**Scope:** Personal& Confidential **Processing Location:** At Supplier **Processing Role:** Processor **Data Class:** Highly Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A	Self-attestation of compliance to the DPR **and** Independent Assurance of compliance	Independent Assurance options: 1. Complete an Independent Assessment against the DPR, **or**

	Healthcare: N/A		2. Independent Assessment against sections A-I of the DPR and ISO 27001, **or** 3. Submit ISO 27701 and ISO 27001
5	**Scope:** Personal & Confidential **Processing Location:** At Supplier **Processing Role:** Processor **Data Class:** Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR	
6	**Scope:** Personal & Confidential **Processing Location:** At Supplier **Processing Role:** Controller **Data Class:** Highly Confidential or Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A or YES **Website Hosting:** N/A **Healthcare:** N/A or YES	Self-attestation of compliance to the DPR	
7	**Scope:** Personal & Confidential **Processing Location:** Any **Processing Role:** Subprocessor (This role is determined by Microsoft – profile will read "Subprocessor Approval: Yes") **Data Class:** Highly Confidential or Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR **and** Independent Assurance of compliance	Independent Assurance options: 1. Complete an Independent Assessment against the DPR, **or** 2. Independent Assessment against sections A-I of the DPR and ISO 27001, **or** 3. Submit ISO 27701 and ISO 27001

8	**Scope:** Personal & Confidential **Processing Location:** At Supplier **Processing Role:** Processor **Data Class:** Highly Confidential or Confidential **Payment Cards:** N/A **Subcontractors:** YES or **SaaS:** YES or **Website Hosting:** YES or **Healthcare:** YES	Self-attestation of compliance to the DPR **and** Independent Assurance of compliance	Independent Assurance options: 1. Complete Independent Assessment against the DPR, **or** 2. Independent Assessment against sections A-I of the DPR and ISO 27001, **or** 3. Submit ISO 27701 and ISO 27001 **or** 4. HITRUST report (only for a covered entity or healthcare service provider in the US)
	Any of the profiles above and **Payment Cards**	Above requirements that apply **and** Payment Card Industry assurance	Submit PCI DSS Certification
	Any of the profiles above and **Software as a Service (SaaS)**	Above requirements that apply **and** submit your contractually required ISO 27001 certification covering the functional services.	Submit an ISO 27001 certification with functional coverage of the service(s) provided.
	Any of the profiles above and **Artificial Intelligence (AI) Systems**	Self-attestation of compliance to the DPR, including the AI branch **and** Independent Assurance of compliance	Independent Assurance options: 1. Complete Independent Assessment against the DPR including the AI branch, **or** 2. Independent Assessment against sections A-I, K of the DPR and ISO 27001 3. Independent Assessment against section

			K of the DPR and ISO 27701 and ISO 27001, **or** 4. Submit ISO 27701, ISO 27001, and ISO 42001* (*ISO 42001 required for service delivery that involves Sensitive Use AI Systems)

Scope

Confidential

Select this approval if the supplier's Performance will involve Processing of only Microsoft Confidential Data.

If you select this approval, you will not be eligible for Personal Data processing engagements.

Personal & Confidential

Select this approval if the supplier's Performance will involve Processing of Personal Data and Microsoft Confidential Data.

To help determine whether you (the supplier) Process Personal Data and/or Microsoft Confidential Data, see the list of examples in the tables below. Please note that these are examples and not an exhaustive list.

Note: A Microsoft business owner may ask for an enrollment outside of this list considering the confidential nature of the data processed.

Personal Data by Data Type

Examples include, but are not limited to:

Sensitive Data
Data related to children
Genetic, biometric, or health data
Racial or ethnic origin
Political, religious, or philosophical beliefs, opinions, and affiliations
Trade union membership
A natural person's sex life or sexual orientation
Immigration status (visa, work authorization, etc.)

Government identifiers (passport, driver's license, visa, social security numbers, national identity numbers)
Precise user location data (within 300 meters)
Personal bank account numbers
Credit card number and expiration date; **or** security/access code or password/credentials allowing access to an account
End-user Pseudonymized Information (EUPI) (Identifiers created by Microsoft to identify users of Microsoft products and services) • Globally Unique Identifier (GUID) • Passport User ID or Unique Identifier (PUID) • Hashed End-User Identifiable Information (EUII) • Session IDs • Device IDs • Diagnostic data • Log data • Customer data associated with a support case
Customer Content Data
Documents, photos, videos, music, etc.
Reviews and/or ratings entered in a product or service
Survey responses
Browsing history, interests, and favorites
Inking, typing and speech utterance (voice/audio and/or chat/bot)
Credential data (passwords, password hints, username, biometric data used for identification)
Customer data associated with a support case
Captured and Generated Data
Imprecise location data
IP address
Device preferences and personalization
Service usage for websites, webpage click tracking

Social media data, social graph relationships
Activity data from connected devices such as fitness monitors
Contact data such as name, address, phone number, email address, date of birth, dependent and emergency contacts
Fraud and risk assessment, background check
Insurance, pension, benefit detail
Candidate resumes, interview notes/feedback
Metadata and telemetry
Account Data
Payment instrument data
Credit card number and expiration date
Bank routing information
Bank account number
Credit requests or line of credit
Tax documents and identifiers
Investment or expense data
Corporate cards
Online Customer Data
Microsoft online enterprise customer (Azure tenant, M365 tenant, etc.)
Microsoft consumer customer (Xbox Live, OneDrive Consumer)
Microsoft enterprise customer (on premises customer)
Support data (customer originates a ticket)
Account data (billing data, e-commerce)
Survey/event registration/training
Protected Health Information
National identification numbers (including tribal numbers and health information identification numbers)
Demographic data used in a Protected Health Information (PHI) context: • Birth date

• Gender • Ethnicity • Biometric data • Full face photographs • Address (full or partial) • Contact information • Emergency contact data
Sensitive Use (AI Systems)
Consequential impact on legal position or life opportunities including: • Criminal justice system risk assessment and scoring systems • Higher education admission system • Credit scoring and application systems
Risk of physical or psychological injury including: • Medical diagnostic or treatment systems • Mental health and wellbeing systems • Equipment control and predictive maintenance systems
Threat to human rights including: • Synthetic media systems that could generate disinformation or political propaganda in order to influence elections • Alert system based on religious, political or social expressions • Social credit-scoring

Microsoft Confidential Data

Examples include, but are not limited to:

Highly Confidential
Information concerning or related to the development, testing, or manufacturing of Microsoft Products or components of Microsoft Products *Microsoft software, online services, or hardware sold commercially in any channel is considered "**Microsoft Product**"* **Note:** For Gaming product development, the Microsoft business owner can indicate whether the work product should have a Data Classification of Highly Confidential or Confidential.
Microsoft device pre-release marketing information
Unannounced Microsoft corporate financial data subject to SEC rules

Confidential
Microsoft product license keys on behalf of Microsoft for distribution via any method
Information concerning or related to the development or testing of Microsoft internal Line of Business (LOB) applications
Microsoft pre-release marketing materials for Microsoft software and services such as Office, SQL, Azure, etc.
Written, design, electronic, or print documentation for any Microsoft services or products, such as devices (process or procedure guides, configuration data, etc.)

Important: A Microsoft business owner may require participation for data not included in this list.

Processing Location

At Microsoft or Customer

Select this approval if all of supplier's Performance involves supplier's Processing of data within the Microsoft network environment where staff use @microsoft.com access credentials or within the environment of a Microsoft customer.

Do not select this option under these circumstances:

- Supplier manages a Microsoft designated offshore facility (OF).
- Supplier provides resources to Microsoft, and they work on and off the Microsoft network at times. The processing location for working off-network is considered "at supplier."

At Supplier

If the condition "At Microsoft or Customer" (as described above) does not apply, select this option.

Data Processing Role

Controller

Select this approval if all aspects of Performance by supplier meet the Controller data processing role definition (see DPR).

If you select this approval, you will not be eligible for Personal Data processing with the 'Processor' role designation. If supplier is both a Processor and a Controller to Microsoft, do not select 'Controller,' select Processor.

Processor

This is the most common processing role when suppliers Process data on behalf of Microsoft. Please review the definition of Processor in the DPR.

Subprocessor

Suppliers cannot self-identify as a Subprocessor at Microsoft because it requires pre-approval by internal Privacy teams. Please review the definition of Subprocessor in the DPR. Subprocessors will have additional contract and compliance requirements, including a Data Protection Addendum and an Independent Assessment (see below). Suppliers that are on a published Microsoft Subprocessor list will also be asked to provide independent verification of compliance.

Payment Card Processing

Select this approval if any part of the data Processed by supplier includes data to support credit card or other payment card processing on behalf of Microsoft.

This approval allows a supplier to engage in payment card processing engagements.

PCI Certification Requirement

The Payment Card Industry Data Security Standard (PCI DSS) is a framework for developing robust payment card data security that includes prevention, detection, and appropriate reaction to security incidents. The framework was developed by the PCI Security Standards Council, a self-regulatory industry organization. The purpose of the PCI DSS requirements is to identify technology and process vulnerabilities that pose risks to the security of cardholder data that is processed.

Microsoft is required to comply with these standards. If a supplier handles payment card information on Microsoft's behalf, we require evidence of adherence to these standards. Consult the PCI Security standards council to understand the requirements set by the PCI organization.

Depending on the volume of transactions processed, a supplier will either be required to have a Qualified Security Assessor certify compliance or can complete a self-assessment questionnaire form.

Payment card brands set the thresholds for assessment type, typically:

- Level 1: Provide a 3rd Party Assessor PCI AOC certificate
- Level 2 or 3: Provide a PCI DSS Self-Assessment Questionnaire (SAQ) signed by the supplier's officer.

Submit the certification that applies and meets PCI requirements. Suppliers who process or store Microsoft customer payment data must possess a current PCI Tier 1 certification as a service provider.

Software as a Service (SaaS)

Software as a Service (SaaS) allows users to connect to and use cloud-based applications over the Internet. For SSPA compliance purposes, view SaaS broadly to also include platform as a service

(PaaS), and infrastructure as a service (IaaS). (To learn more about SaaS please see this explanation.)

Microsoft defines **Software as a Service (SaaS)** as software based on common code used in a one-to-many model on a pay-for-use basis or as a subscription based on use metrics. The cloud service provider develops and maintains cloud-based software, provides automatic software updates, and makes software available to its customers via the internet on a one-to-many, pay-as-you-go basis. This method of software delivery and licensing allows software to be accessed online via a subscription rather than bought and installed on each individual computer.

Note: Most SaaS suppliers will need to add the Subcontractor approval in the Microsoft Supplier Compliance Portal if the Personal Data or Microsoft Confidential data is hosted on a 3rd party platform or cloud infrastructure provider.

Suppliers that meet the SaaS definition included on the Data Processing Profile will be required to provide a valid ISO 27001 certification. Please do not submit a datacenter certification. We expect the ISO 27001 certification that applies to the software service(s) noted in your contract with Microsoft.

Use of Subcontractors

Select this approval if supplier uses Subcontractors to Perform. "**Subcontractor**" means a third-party to whom supplier delegates its obligations in connection with the contract covering their Performance, including a supplier affiliate not contracting directly with Microsoft.

This also includes Freelancers (see DPR).

Microsoft considers the use of subcontractors a high-risk factor. Suppliers using subcontractors who will Process Personal and or Microsoft Confidential Data must disclose those subcontractors. Additionally, the supplier must also disclose the countries where that personal data will be processed by each subcontractor.

Website Hosting

Select this profile option if supplier hosts websites, provides website portals, online services, and/or mobile applications on Microsoft's behalf.

A website hosting service is an online service that creates and/or maintains websites on behalf of Microsoft, i.e., supplier provides all materials and services required for them to create and maintain a site and makes it accessible on the internet. The "web hosting service provider" or "web host" is the supplier who provides the tools and services needed for the website or webpage to be viewed on the Internet, such as, Cookies or web beacons for advertising.

Healthcare

Select this profile option if the supplier is required to process Protected Health Information.

"**Protected Health Information**" or "**PHI**" means Microsoft Personal Data that is protected by the United States Health Information Portability and Accountability Act (HIPAA).

Artificial Intelligence (AI) Systems

Select this profile option if supplier will provide services to Microsoft involving AI Systems including using tools, systems, or platforms with AI Technology to train and build intelligent systems to create entirely new content such as images, sounds, videos, insights, analysis, and/or text. This only applies to publishers of AI Systems (own, manage, control, etc.). If your engagements with Microsoft are only in the utilization of Microsoft Copilot or a third-party AI that you do not publish and is not a subcontractor (see DPR for definition), then you can say "no" to this question on your profile.

The SSPA AI Systems Approval will include documentation on the Processing of Personal and/or Microsoft Confidential Data, impacts to people, organizations and society, and acceptance of appropriate supplier certifications. The supplier will complete the Responsible AI branch of the Microsoft Supplier Data Protection Requirements with required signed agreements and/or Microsoft internal reviews completed before purchasing can proceed. All suppliers providing AI Systems will be required to provide Independent Assurance options. The ISO 42001 can be offered to validate compliance against Section K of the DPR and is **required** for any AI sensitive cases. For suppliers getting an Independent Assessment against Section K of the DPR, the Independent Assessment must be performed by a preferred assessor (list available here).

This approval will only be granted upon the Independent Assessment being accepted by SSPA.

SSPA Process Overview

What is SSPA?

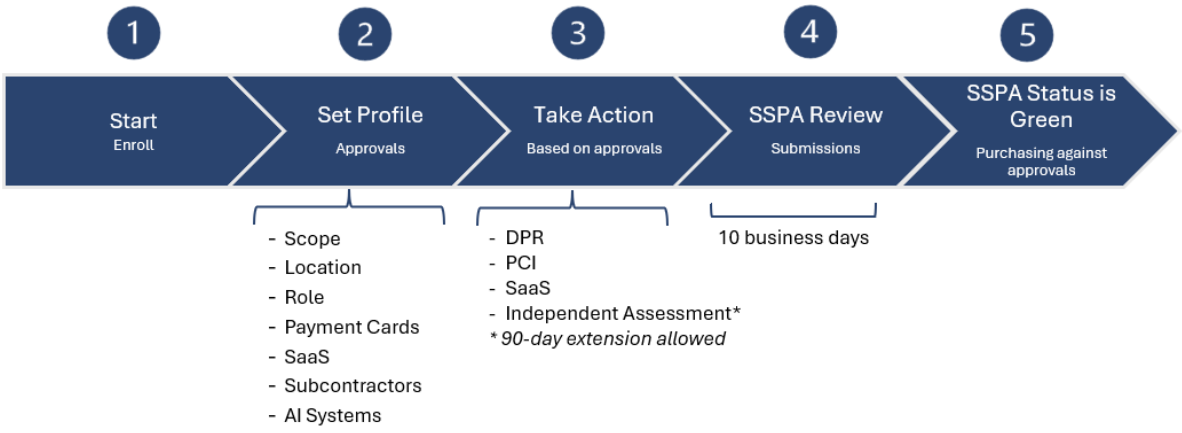
At Microsoft, we believe privacy is a fundamental right. In our mission to empower every individual and organization on the planet to achieve more, we strive to earn and maintain the trust of our customers every day.

Strong privacy and security practices are critical to our mission, essential to customer trust, and in several jurisdictions required by law. The standards captured in Microsoft's privacy and security policies reflect our values as a company and these extend to our suppliers (such as your company) that Process Microsoft data on our behalf.

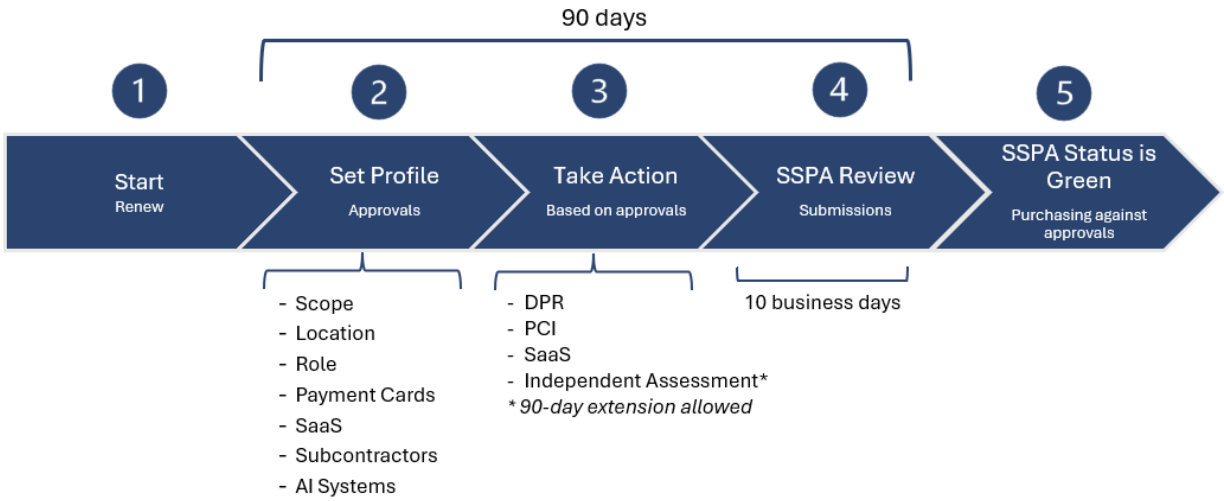
Key SSPA terms are defined in the DPR. To learn more about the program, visit the SSPA site and engage our global team by writing to SSPAHelp@microsoft.com.

The DPR is an annual requirement. Compliance activities determine an SSPA Status of Green (compliant) or Red (non-compliant). Microsoft purchasing tools validate the SSPA Status is Green (for each supplier in scope for SSPA) and that the supplier has requisite approvals prior to allowing an engagement to move forward.

SSPA Process Diagram – New Supplier Enrollment



SSPA Process Diagram – Annual Supplier Renewal



Assurance Requirements

The approvals selected in your Data Processing Profile inform the risk level across your Microsoft's engagement(s). SSPA compliance requirements differ based on the Data Processing Profile and associated approvals.

Self-Attestation to the DPR

All suppliers enrolled in SSPA must complete a self-attestation of compliance to the DPR within 90 days of receiving the request. This request will be provided on an annual basis but may be more frequent if the Data Processing Profile is updated mid-year. Supplier accounts will change to an SSPA Status of Red (non-compliant) if the 90-day period is exceeded. New in-scope purchase orders cannot be processed until the SSPA Status turns to Green (compliant).

Newly enrolled suppliers must complete issued requirements to secure a SSPA Status of Green (compliant) before engagements can begin.

Important: The SSPA team is not authorized to provide extensions for this task.

Suppliers are expected to respond to all applicable DPR requirements issued per the Data Processing Profile. It is expected that, within the issued requirements, a few may not apply to the goods or services the supplier provides to Microsoft. These can be marked as 'does not apply' with a detailed comment for SSPA reviewers to validate.

DPR submissions are reviewed by the SSPA team for any selections of 'does not apply,' 'local legal conflict' or 'contractual conflict' against issued requirements. The SSPA team may ask for clarification of one or more selections. Local legal and contract conflicts are only accepted if supporting references are provided and the conflict is clear.

Authorized representatives that will complete the self-attestation should ensure they have sufficient information from subject matter experts to reply to each requirement with confidence. In addition, by adding their name to a SSPA form they are certifying that they have read and understand the DPR. A separate security contact is required to sign off on Section J of the DPR specifically and may be called upon to assist should a security incident occur involving your company. Suppliers can add other contacts to the online tool to assist with completing the requirements.

The Authorized Representative (see DPR for definition), is to:

1. Determine which requirements apply.
2. Post a response to each applicable requirement.
3. Sign and submit the attestation in the Microsoft Supplier Compliance Portal.

Important: SSPA may ask for collaborating evidence of compliance for a particular Data Protection Requirement to support compliant attestations. Additionally, Suppliers may be selected to provide evidence as described in the Microsoft Supplier Data Protection Requirements outside of the annual compliance cycle. This will only apply to companies that do not receive the Independent Assessment task.

Independent Assessment Requirement

Please see the Requirements by Approvals in the SSPA Data Processing Profile Table to see the data processing approvals that trigger this requirement.

Suppliers have the option to change approvals by updating their Data Processing Profile. However, if the supplier has a Data Processing Role of "Subprocessor," the supplier cannot change this approval and will be required to have an Independent Assessment conducted annually.

To secure the approvals that require independent verification of compliance, suppliers will need to select an independent assessor to validate compliance against the DPR. The assessor is to prepare an advisory letter (Letter of Attestation) to provide compliance assurances to Microsoft. This letter must be unqualified and all non-compliant issues must be resolved and remediated before the confirmation letter is submitted to the Microsoft Supplier Compliance Portal for SSPA team review. **All assessors must use the approved advisory letter template, which is attached to the "Preferred Assessors" PDF available here.**

The **SSPA Data Processing Profile Table** includes acceptable certification alternatives if you elect not to use an independent assessor to verify compliance to the DPR (when applicable, such as for SaaS suppliers, website hosting suppliers or suppliers with Subcontractors). The ISO 27701 (privacy), ISO 27001 (security), and ISO 42001 for AI Systems (DPR Section K) are relied on as providing close mapping to the DPR. A SOC 2 report with security trust criteria may be accepted for DPR Section J (security) where no qualifications are noted.

Where Supplier is a covered entity under HIPAA or healthcare service provider in the United States, we will accept a HITRUST report for privacy and security coverage.

If circumstances beyond standard triggers warrant additional due diligence, SSPA may require an independent assessment regardless of the Data Processing Profile. Examples include: a request from division privacy or security; validation of data incident remediation; an SSPA team out of cycle review; or requirement for automated data subject rights execution.

Guidance on how to approach this requirement:

1. The engagement must be performed by an assessor with sufficient technical training and subject knowledge to adequately assess compliance.
2. Assessors must be affiliated with the International Federation of Accountants (IFAC) or the American Institute of Certified Public Accountants (AICPA); a certified ISO auditor qualified for ISO 27001, ISO 27701, and ISO 42001 where applicable; or must possess certifications from other relevant privacy and security organizations, such as the International Association of Privacy Professionals (IAPP) or the Information Systems Audit and Control Association (ISACA).
3. The assessor must use the most current DPR which includes the evidence required to support each requirement. **Suppliers will need to provide their most recently approved DPR attestation responses to the assessor.**

4. The scope of the engagement is limited to all in-scope data processing activity executed against the supplier account number which received the request. If the supplier elects to more than one supplier account at one time, the **letter of attestation must include the list of supplier accounts included in the assessment.**
5. The letter submitted to SSPA must not include any statements where the supplier cannot meet the Data Protection Requirements as written. These issues must be corrected before the letter is submitted.

SSPA has made a list of preferred assessors available. These companies are familiar with conducting SSPA assessments. Suppliers are expected to pay for this assessment; the costs will vary depending on the scale and scope of the data processing.

Profiles requiring additional independent assurance:

Software as a Service (SaaS)

Suppliers that meet the SaaS definition included on the Data Processing Profile may be required to provide a valid ISO 27001 certification if this is required in the Microsoft Cloud Services Agreement. Please do not submit a datacenter certification. We expect the ISO 27001 certification that applies to the software service(s) noted in your contract with Microsoft.

SSPA reviewers will validate that your submission meets the contract obligation.

AI Systems

If the service delivery includes Sensitive Use, an ISO 42001 certification will be required. Additionally, the ISO 42001 may be submitted for section K of the Independent Assessment task.

Data Incidents

If a supplier becomes aware of a privacy or security data incident, suppliers must inform Microsoft as detailed and defined in the DPR.

Report a data incident using SupplierWeb or email SuppIR@microsoft.com.

Be sure to include:

- Data incident date
- Supplier name
- Supplier number
- Microsoft contact(s) notified
- Associated PO, if applicable/available
- Summary of the data incident.