Microsoft Compliance Report – Annex 10 – Windows PC (Operating System)

DMA.100160 – Microsoft; DMA.100026 – Microsoft – Operating Systems; DMA.100017 – Microsoft – Online Social Networking Services

SECTION 2

Information on compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925

2.1. For each core platform service in relation to which the Undertaking has been designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 and for each applicable obligation laid down in Articles 5 to 7 of Regulation (EU) 2022/1925,[1] please provide the following information:

1. For the Windows PC operating system ("**OS**") core platform service ("**CPS**"), Microsoft Corporation ("**Microsoft**") has been designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector – Digital Markets Act ("**DMA**").[2] The relevant versions of Windows are (i) Windows 11 and Windows 11 on ARM ("**Windows 11**") and (ii) Windows 10 and Windows 10 on ARM ("**Windows 10**") – Home, Pro, and Enterprise editions, collectively referred to as "**Windows**" unless a specific version is referenced. The Windows desktop-as-a-service offerings are Azure Virtual Desktop and Windows 365, both of which can run Windows 10 and Windows 11 in virtualized environments.

2. With respect to Windows features that to comply with the DMA behave differently in the European Economic Area ("**EEA**") than in other parts of the world, Microsoft determines the geographic nexus with the EEA based on the country or region the user (or system administrator) selects when setting up a device. This country or region is established during device setup and can be changed if the user (or system administrator) conducts a factory reset of the OS and goes through setup again. Country or region settings in Windows Settings are user preferences for things such as date/time format or to provide local content and are different from the country or region selected during device setup.

3. Windows PCs are identified as being in the EEA if the user selects any of the following countries or regions during device setup: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, French Guiana, Germany, Greece, Guadeloupe, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania,

---

[1] The information listed in Section 2 may be omitted for the obligations that are listed in response to Section 2.3 on condition that it can be established that a specific obligation laid down in Articles 5 to 7 of Regulation (EU) 2022/1925 cannot, by nature, apply to the Undertaking's relevant core platform service. If so, please explain why this is the case for the Undertaking.

[2] Commission Decision of 5 September 2023 designating Microsoft as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector, DMA.100017 Microsoft – online social networking services, DMA.100023 Microsoft – number-independent interpersonal communications services, DMA.100026 Microsoft – operating systems ("**Designation Decision**"), ¶44.

Luxembourg, Malta, Martinique, Mayotte, Netherlands, Norway, Poland, Portugal, Reunion, Romania, Slovakia, Slovenia, Spain, Sweden, and Switzerland.[3]

4. Microsoft provides the following information regarding Windows using the headings in the Commission's compliance report template under Article 11 of the DMA as a guide to structure the report.

[3] While Switzerland is not an EEA member, Microsoft identifies a Windows PC as in the EEA when it is set up in Switzerland as part of the single market.

Regarding Article 5(2)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

5. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 5(2) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data [4] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

6. Article 5(2) of the DMA provides:

"*The gatekeeper shall not do any of the following:*

(a) process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper;

(b) combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services;

(c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice-versa; and

(d) sign in end users to other services of the gatekeeper in order to combine personal data,

unless the end user has been presented with the specific choice and has given consent within the meaning of Article 4, point (11), and Article 7 of Regulation (EU) 2016/679. Where the consent given for the purposes of the first subparagraph has been refused or withdrawn by the end user, the gatekeeper shall not repeat its request for consent for the same purpose more than once within a period of one year.

[4] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

This paragraph is without prejudice to the possibility for the gatekeeper to rely on Article 6(1), points (c), (d) and (e) of Regulation (EU) 2016/679, where applicable."

7. As explained in further detail below, Windows complies with Article 5(2) of the DMA, which conditions certain use of personal data collected by Windows and user sign-in to combine personal data on Microsoft obtaining end-user consent.

8. In the following sections, Microsoft first provides an overview of how Windows collects and processes personal data (**Section A**). It then explains that:

- Article 5(2)(a) of the DMA does not apply to Windows because Windows does not provide online advertising services or process data collected from third-party applications for that purpose. And even if Article 5(2)(a) of the DMA did apply to Windows, Microsoft complies because the promotions presented in Windows do not use data collected from third-party applications running on Windows (**Section B**).

- Microsoft complies with Article 5(2)(b) of the DMA when combining personal data from Windows with personal data from other services (**Section C**).

- Article 5(2)(c) of the DMA imposes no additional obligations on Windows beyond those included under Article 5(2)(b) because Microsoft either collects end-user consent to cross-use personal data, in the same way as consent to combine personal data is provided, or does not cross-use personal data between Windows and services provided separately (**Section D**).

- Microsoft complies with Article 5(2)(d) of the DMA because Windows does not sign-in users to other Microsoft services in order to combine personal data without end-user consent (**Section E**).

A. Overview Of How Windows Collects And Processes Personal Data

9. Windows collects three categories of personal data: (**1**) Windows Diagnostic Data, (**2**) Account Data, and (**3**) Windows Required Service Data.

1. Windows Diagnostic Data

10. Windows collects Windows Diagnostic Data to diagnose and solve problems, to keep Windows up-to-date, secure, and operating properly, and to make product improvements.[5] Windows collects Diagnostic Data from users at two levels: required and optional.

11. **Required Diagnostic Data.** Windows collects required Diagnostic Data from all Windows PCs because this data is needed and used specifically to deliver Windows updates to individual PCs to keep them up-to-date and secure. Required Diagnostic Data includes device configuration data, data on both Microsoft applications and non-Microsoft applications (*i.e.*, third-party software from business users that runs on

[5] *See* Diagnostics, feedback, and privacy in Windows - Microsoft Support.

Windows) installed on the PC, and other similar data items. Microsoft publishes a complete description of this data.[6]

12. **Optional Diagnostic Data.** Microsoft collects additional Diagnostic Data at the optional level. Microsoft combines Windows optional Diagnostic Data with personal data from other services. The optional level of Windows Diagnostic Data includes all the required Diagnostic Data and additional data reflecting not only how the PC is configured, including the applications installed on the PC, but also how the end user uses their PC, including data related to their application usage (both Microsoft and non-Microsoft applications). Microsoft publicly documents the types of optional Diagnostic Data collected by Windows, with examples of data collected for each type.[7] Microsoft minimizes the volume of optional Diagnostic Data it collects from all devices by collecting some of the data from only a small percentage of devices (a sample). Except for personalized promotions and experiences ("**Tailored Experiences**"), described below, Windows does not use diagnostic data to personalize features.

13. **Diagnostic Data collected separately by applications in the EEA.** To comply with Article 6(3) of the DMA, Microsoft redesigned certain OS features to be applications rather than part of Windows in the EEA. Windows may continue to collect Diagnostic Data about these applications for purposes of ensuring these applications are working properly with Windows, as it does with all applications on Windows. And, in accordance with the consent to collect Windows optional Diagnostic Data (described below), Microsoft may also share this data with the respective applications. These new applications, like any first- or third-party application installed on Windows, may collect their own diagnostic data. Any such diagnostic data collected by these applications in the EEA is collected and stored separately from Windows Diagnostic Data.

14. For example, prior to the DMA compliance deadline, the Microsoft Edge browser was part of Windows, and Edge collected required and optional Diagnostic Data as part of Windows' required and optional Diagnostic Data. Because of the DMA qualifying Edge as an application in the EEA, Microsoft redesigned Edge as an uninstallable application on Windows. On PCs in the EEA, Edge now collects its own required and optional set of diagnostic data.

15. Microsoft processes Windows Diagnostic Data, sometimes together with data collected from other products, for several reasons.

16. First, the primary purpose is to monitor whether Windows, the applications that run on Windows, along with the hardware on which Windows runs, are secure, up-to-date, and operating as designed. Microsoft uses Diagnostic Data to diagnose problems so that software updates can be made to fix them for the entire ecosystem.

17. Second, Microsoft analyzes Windows Diagnostic Data, typically together with other data, to produce internal reports about how Windows and other products are used. These reports are used to inform business decisions and technical choices made by Microsoft. These reports comprise aggregated data.

---

6 *See* Windows Required diagnostic events and fields.

7 *See* Windows Optional diagnostic data.

18. Third, Microsoft uses Windows Diagnostic Data to test new features and capabilities in Windows using a practice commonly known as Randomized A/B Testing. Typically, Microsoft identifies a sample of devices that will test a new or revised feature (the "**treatment sample**") and a second sample of devices without the new or revised feature (the "**control sample**") against which the performance of the new or updated feature will be compared. The selection of the control and treatment samples proceeds via random selection of devices to ensure the two samples are statistically significantly similar to enable valid conclusions to be gleaned about the causal effect of the new or revised feature. Microsoft uses Diagnostic Data to measure and report on the results of each test. When Windows collects Diagnostic Data at the optional level, Microsoft may combine Diagnostic Data with personal data from other services during testing.

19. **Tailored Experiences.** Windows provides users with Tailored Experiences on several surfaces in Windows and in the Microsoft Store. Tailored Experiences include suggestions on how to use and customize Windows, as well as recommendations and promotions for Microsoft and third-party products and services, features, applications, and hardware to improve the customer's experience on Windows.[8] The surfaces in Windows where Tailored Experiences using Diagnostic Data can appear each have their own setting that allows the user to control whether promotions do appear. There are user controls for each.

20. Most promotions are for Microsoft's own products and services. Microsoft alone selects the third-party products included in promotions, which are available from the Microsoft Store and intended to enhance the Windows experience. Sometimes, Microsoft enters into agreements with third parties to include their products in promotions on Windows. For example, Microsoft might agree to promote a third-party application if the third party agrees to develop a version of a popular application for Windows. Importantly, Microsoft does not operate any online advertising service allowing third parties to provide advertising content presented through Tailored Experiences.

2. Account Data

21. Account Data is data associated with the user's Microsoft account. There are three types of Account Data that Microsoft stores with the user's account: (i) Basic Account Data, (ii) Account Sync Data, and (iii) User content data. Account Data is used by Windows and other Microsoft products and services. Further, non-Microsoft applications can access Account Data with user consent.

22. **Basic Account Data.** Basic Account Data is the data that is required to create an account and naturally connected to the account. This includes personal information about the user, such as their name, age, location, language, payment information, as provided by the user to Microsoft when creating the account, and active subscriptions and entitlements to Microsoft products and services the user later acquires. When a user signs-in to Windows, Windows retrieves the Basic Account Data and caches it locally on the PC.

[8] *See* Diagnostics, feedback, and privacy in Windows – Tailored Experiences.

23. Basic Account Data is not Windows personal data. Rather, it is data that is intrinsically part of the account and used by any service that permits the user to sign-in using their account.

24. **Account Sync Data.** Windows synchronizes data between the user's Microsoft account and the local PC if the end user provides consent.

25. When the user consents, Windows will keep device data stored locally synchronized with the user's Account Data. If the user refuses or withdraws consent, Windows will not synchronize the data and changes to the device data stored locally will not be reflected in the user's Account Data and *vice versa*.

26. The Account Sync Data consent allows Windows to synchronize data with other Microsoft products. Windows typically accomplishes this by storing Account Sync Data on the Microsoft Graph, which is a cloud storage location.[9] The Microsoft Graph provides application programming interfaces ("**APIs**") that allow Microsoft and non-Microsoft applications (if the user has also consented to giving access to the non-Microsoft application), to access the user's data. Most Account Sync Data stored by Windows is used only by Windows, such as the user's Windows settings, which are synchronized between the user's Windows PCs. Some Account Sync Data is shared between Windows and other products and services, such as the user's custom dictionary, which stores the words the user has added for spell checking.

27. **User Content Data.** With consent, Windows stores User Content Data associated with the user's account. For example, Windows stores user activity data collected pursuant to separate consent associated with the user's account. Windows also allows users to store user content, such as photos and documents, with the user's account in OneDrive.

3. Windows Required Service Data

28. Windows collects and processes personal data called Required Service Data, which is the data necessary to deliver the cloud-service-backed features of Windows. Some cloud services are essential to the functioning of the product, such as licensing (online activation) and authentication (enables signing into Windows). Some cloud services are optional, such as the Windows "Find My Device" service (helps users locate their Windows PC if it is lost or stolen). To illustrate this concept, the Session Context described below for Tailored Experiences is Required Service Data sent to the cloud service that provides the content for Tailored Experiences. Sending the Session Context is necessary for the Tailored Experiences feature to operate.

29. Microsoft processes Required Service Data for two purposes: to deliver features using the associated cloud service, and in aggregated or de-identified form to improve the cloud service. The primary purpose is to deliver the cloud-service-backed feature of Windows. Windows must send Required Service Data to the associated cloud service so that the feature can function. As part of delivering the cloud service, Microsoft may process the Required Service Data to ensure that the service is available, secure, and performing as expected. Second, in some cases, Microsoft de-identifies or aggregates Required Service Data and processes the resulting data to improve the cloud service's

[9] *See* Microsoft Graph overview.

quality. This resulting data is no longer personal data because it is not linked or linkable to an individual user.

B. Compliance With Article 5(2)(a) Of The DMA

30. Article 5(2)(a) of the DMA does not apply to Windows because data collected by Windows is not used to provide "online advertising services" as contemplated by Article 5(2)(a). Microsoft does not provide online advertising services in Windows. It does not sell advertising to business users for display in Windows. Data collected by Windows is also not used by Microsoft's online advertising services. Thus, Article 5(2)(a) of the DMA does not require any changes to Windows' data practices.

31. As explained above, Windows provides Tailored Experiences, which are personalized promotions and recommendations in Windows and the Microsoft Store. Tailored Experiences are not covered by Article 5(2)(a) because they are not an online advertising service. Even if Tailored Experiences were considered an online advertising service (*quod non*), Microsoft would comply with Article 5(2)(a) because, on PCs in the EEA and as a result of the DMA, Microsoft will not process any third-party application data collected by Windows to inform Tailored Experiences.

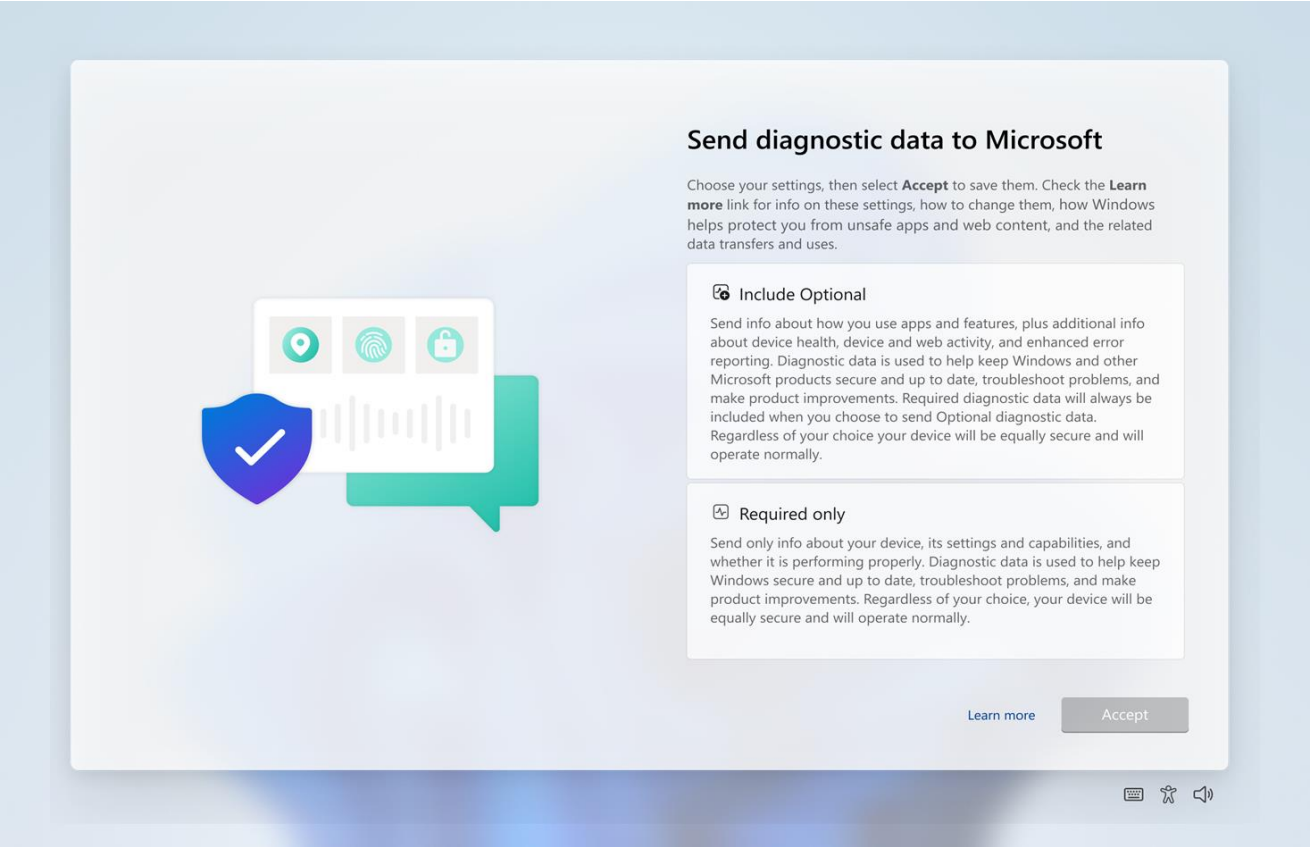
C. Compliance With Article 5(2)(b) Of The DMA

32. Except to provide security services, as explained below, Microsoft does not combine personal data from Windows with personal data from other services without end-user consent.

33. **Windows Diagnostic Data.** Windows collects required Diagnostic Data from all Windows PCs and uses that data without consent to deliver Windows updates to individual PCs to keep them up-to-date and secure.

34. Windows collects Diagnostic Data at the optional level only with separate consent from the user. The consent request existed prior to the DMA. Windows requests consent, as shown in **Figure 1**, to collect this data during the device setup experience and after adding a new user to a PC. The consent makes clear that Microsoft uses the data in combination with data from other products to maintain and improve Windows and other Microsoft products.

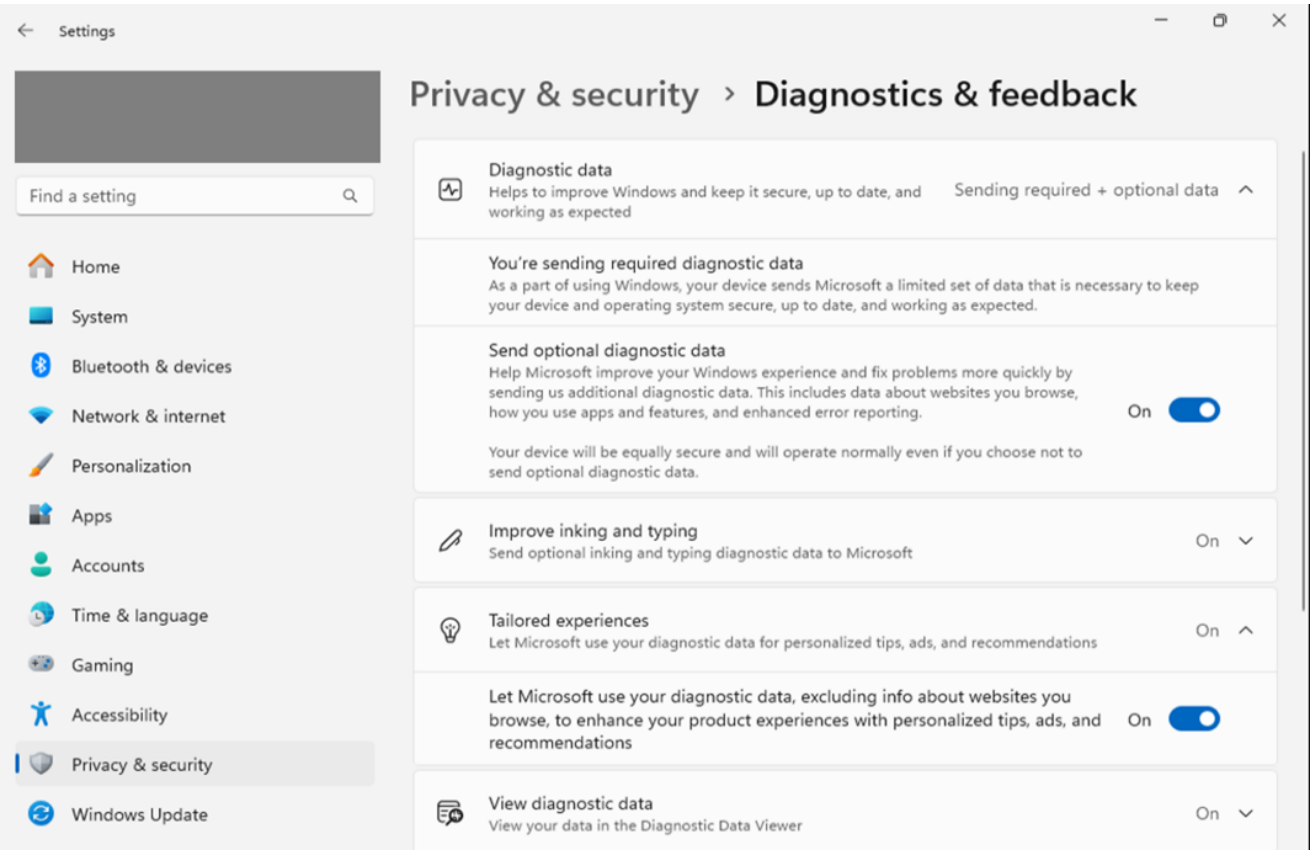
Figure 1. Windows Consent To Collect Optional Diagnostic Data In The Device Setup Experience



Source: Microsoft

35. Users can configure this Diagnostic Data collection control at any time through Windows settings, as shown in **Figure 2**.

Figure 2. Windows Optional Diagnostic Data Control In Settings



Source: Microsoft

36. IT administrators can manage this setting as part of configuring the device for work or school accounts.

37. For each user on the PC, in the EEA, if the user refuses or later withdraws consent Windows will not ask again for consent to collect Diagnostic Data at the optional level.[10] Users can provide or withdraw consent at any time in Windows settings.

38. This consent permits Microsoft to use Windows Diagnostic Data to "*help keep Windows and other Microsoft products secure and up-to-date, troubleshoot problems, and make product improvements*" (emphasis added, *see* **Figure 1**). This language makes it clear that Windows Diagnostic Data will be cross-used with, or combined with data from, those other Microsoft products for these purposes.

39. Except for the Tailored Experiences described in this report, Windows does not behave differently whether the end user consents to Microsoft's collection of optional Diagnostic Data or not.

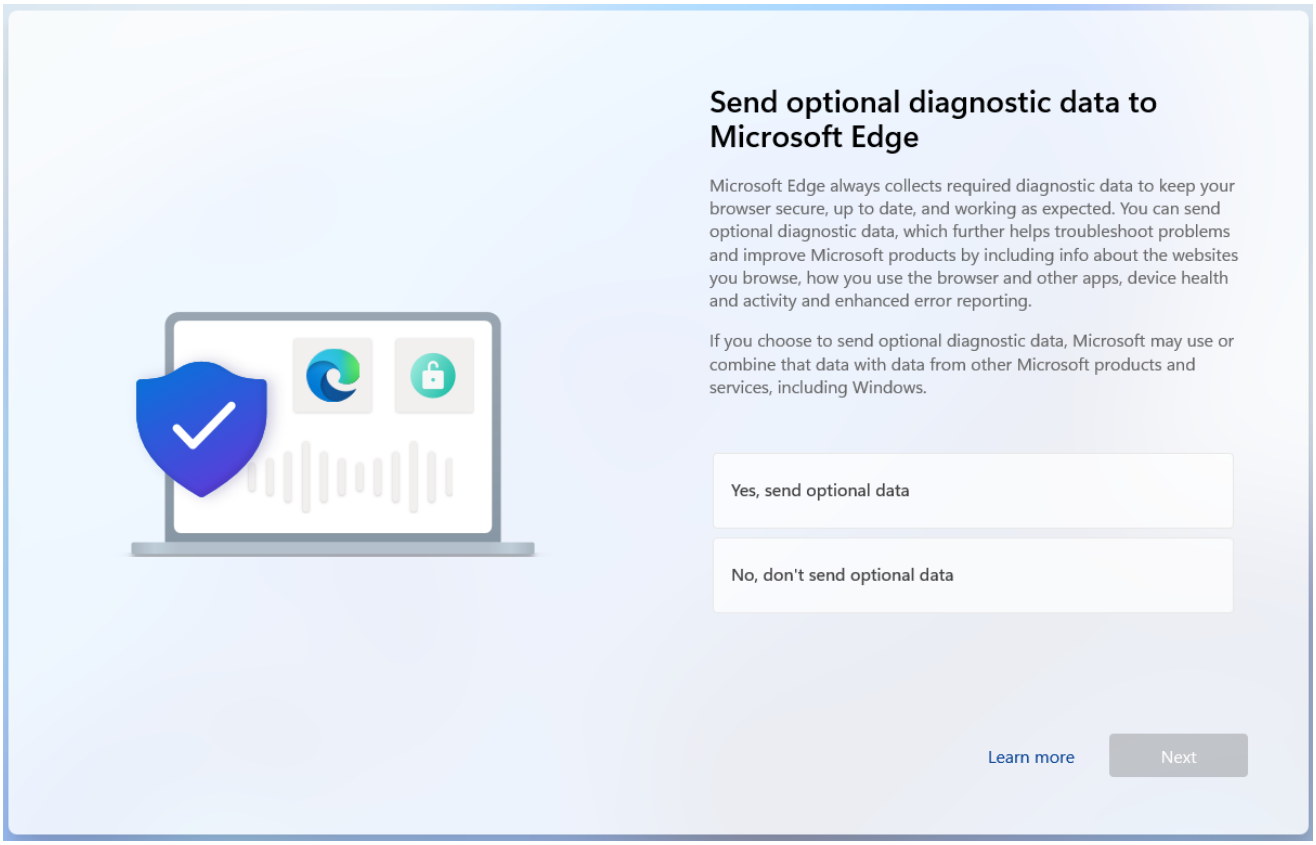
40. **Diagnostic Data collected separately by applications in the EEA.** As discussed above, to comply with Article 6(3) of the DMA, Microsoft redesigned certain OS features to be applications rather than part of Windows in the EEA. These new

[10] If Microsoft were to change this practice and repeat this request for consent to users on PCs in the EEA, it would ensure that it did not do so "*more than once within a period of a year*" as required by Article 5(2) of the DMA.

applications, like any first- or third-party application that is installed on Windows, may collect diagnostic data of their own. Any such diagnostic data collected by these applications in the EEA is collected and stored separately from Windows Diagnostic Data.

41. For example, Edge collects optional diagnostic data pursuant to an end-user consent that is separate from the Windows Diagnostic Data consent and provided in **Figure 3** below. Even though Edge collects its own diagnostic data, Windows Diagnostic Data may still include some information about websites to which the user browses, and so, for example, the consent in **Figure 1** will still mention web activity. For example, when a browser like Edge crashes, the crash report collected by Windows will note the website in case that site might have had something to do with the crash.

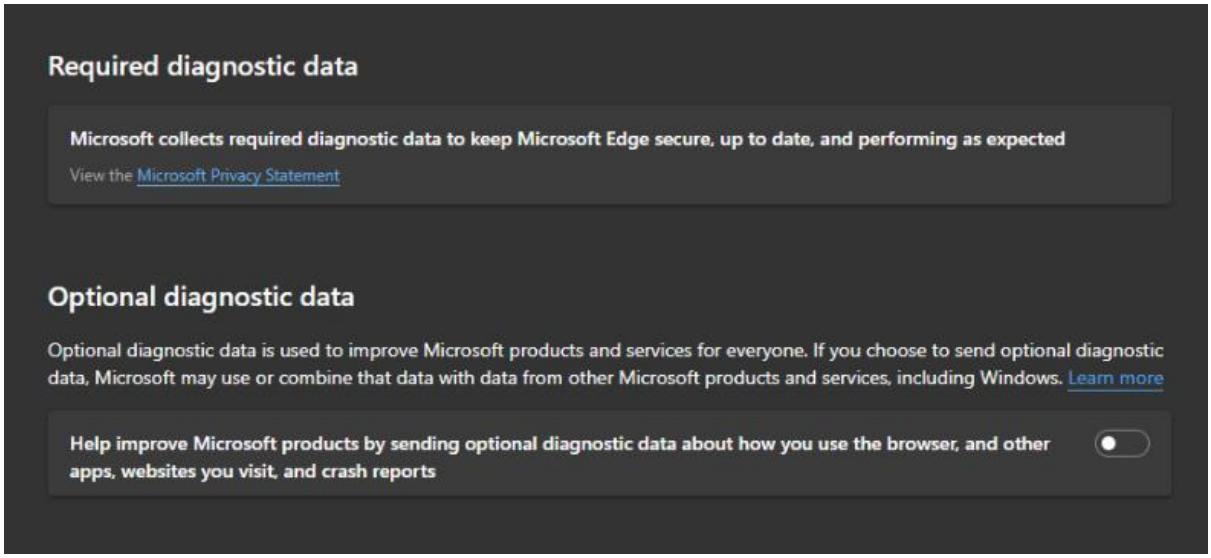
Figure 3. Microsoft Edge Consent To Collect Optional Diagnostic Data



Source: Microsoft

42. Users can configure this Edge diagnostic data collection at any time through Edge controls (*see* **Figure 4**).

Figure 4. Microsoft Edge Diagnostic Data Controls In Edge Settings



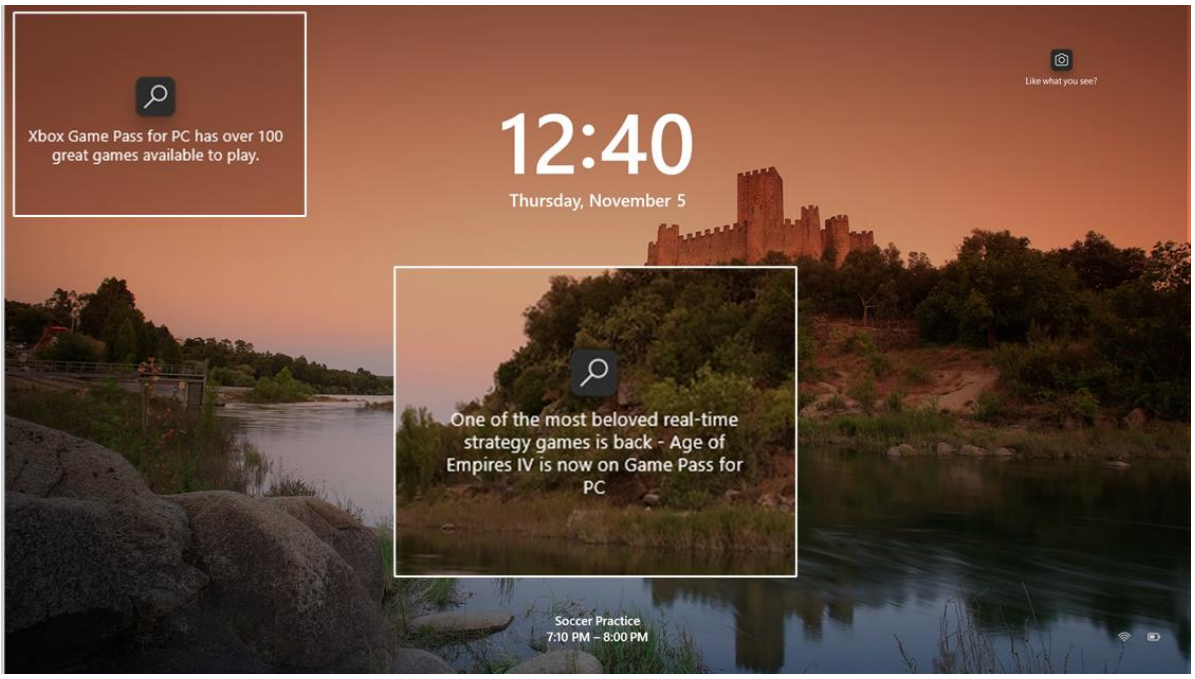
Source: Microsoft

43. **Tailored Experiences.** Prior to the DMA compliance deadline, with end-user consent, Windows performed processing that combined Windows Diagnostic Data with personal data from other Microsoft products and services to deliver Tailored Experiences.

44. In particular, Microsoft processed Diagnostic Data from Windows together with personal data from other Microsoft products and services to sort users into groups of similar characteristics and interests called "audience segments," which can be used to determine the promotions most likely to be of interest to the user. For example, Microsoft could offer Tailored Experiences related to games to users who appear to be interested in video games.

45. In the following example, illustrated in **Figure 5**, Tailored Experiences on the Lockscreen Spotlight shows a promotion for Xbox Game Pass.

Figure 5. Tailored Experiences On The Lockscreen Spotlight (Promotional Areas Zoomed In For Readability)



Source: Microsoft

46. Windows was therefore only using Diagnostic Data to show Tailored Experiences if the user provided consent to use data for this purpose through the "tailored experiences" consent. Because that existing consent did not include specific consent to combine personal data, for compliance with Article 5(2)(b) of the DMA, Microsoft has stopped the use of Diagnostic Data together with personal data from other Microsoft products and services on PCs in the EEA. In the future, Microsoft plans to revise the consent experience to obtain the required consent to combine data under Article 5(2)(b) of the DMA and at that point would resume some data combinations to deliver Tailored Experiences.

47. Windows relies on a cloud service to provide the content that Tailored Experiences displays in Windows. When Windows calls the cloud service to request a Tailored Experience, it passes contextual data to the service called the "Session Context." Because Microsoft has stopped using Diagnostic Data for Tailored Experiences on PCs in the EEA, the cloud service will return a contextual promotion selected using only the Session Context without using Diagnostic Data, just as if the user had declined the "tailored experiences" consent.

48. The Session Context contains information from the device used to show appropriate promotions for the user regardless of whether the user agreed to the "tailored experiences" consent. For example, the Session Context is used to make sure content is in the correct language and appropriate depending on whether the user is an adult or a child. The cloud service uses the Session Context when selecting an individual promotion for Tailored Experiences, which it returns to Windows to be displayed. For example, the cloud service may use the age of the PC to avoid showing promotions for new PCs to a user who already has a new PC. After returning the content to Windows, the Session Context is discarded and not stored or combined.

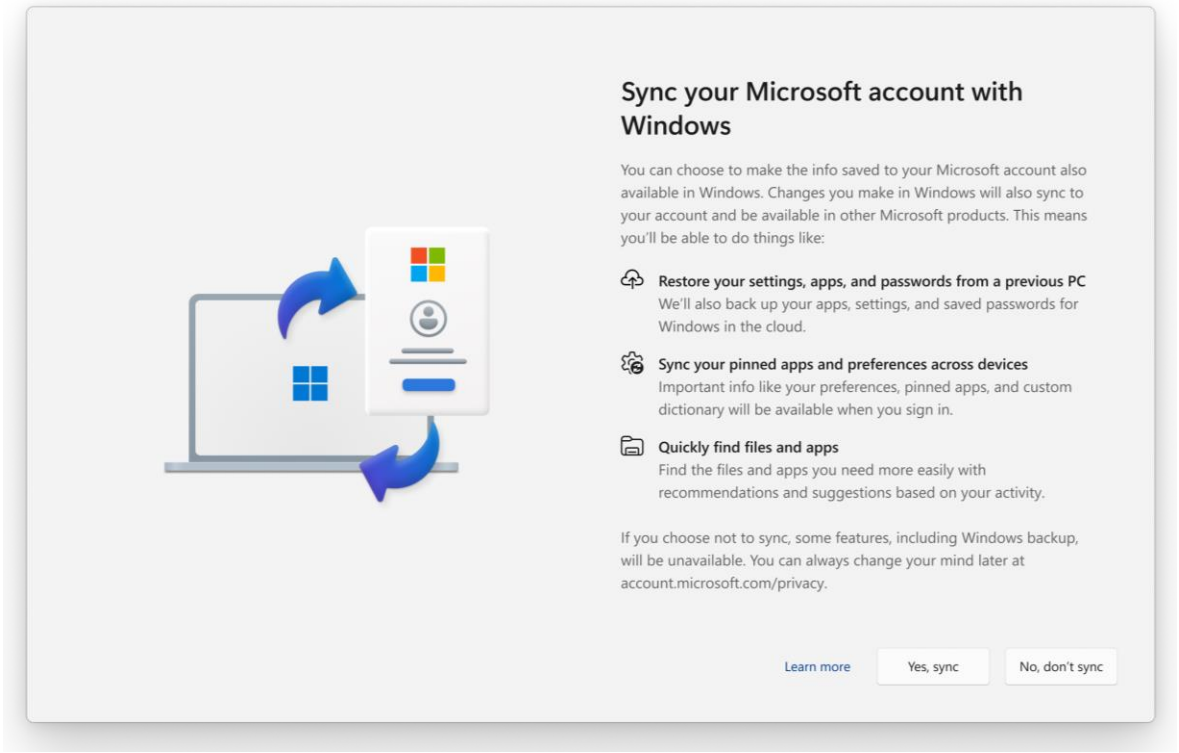
49. The cloud service maintains an inventory of available promotions for different campaigns. Microsoft designs some campaigns to only be delivered to users who agree to the "tailored experiences" consent because they are targeted using Diagnostic Data, but these campaigns will not be delivered to PCs in the EEA. Other campaigns do not rely on processing Diagnostic Data but instead the cloud service matches campaigns based on device information provided in the Session Context. For example, a campaign might show promotions offering the user a deal for a new PC on devices that are more than four years old, but this does not depend on processing Diagnostic Data. Lastly, the cloud service always maintains an inventory of "untargeted campaigns" with promotions that do not depend on data from either Windows or other services. These campaigns often promote general awareness of Microsoft products and technology that are not targeted at particular users.

50. **Other Microsoft Products and Services.** Prior to the DMA compliance deadline, Microsoft combined Windows Diagnostic Data collected at the required level with data collected by other products if users provided consent in those other products. Again, to the extent the consent in other Microsoft products does not include specific consent to combine personal data from those products with diagnostic data collected at the required level from Windows, Microsoft has stopped these data combinations in the EEA and will not resume them until those products revise the consents to cover such combinations.

51. **Account Data.** For Account Sync Data, as a result of the DMA, Microsoft obtains consent to store personal data from Windows in the user's account, which may be accessed by other applications, and to retrieve personal data provided by other products and services. Prior to the DMA, this synchronization was performed automatically without consent on PCs in the EEA.

52. Windows now requests this consent during the device setup experience as shown in **Figure 6**, which was implemented for PCs in the EEA.

Figure 6. Windows Consent To Sync Account Data With Windows

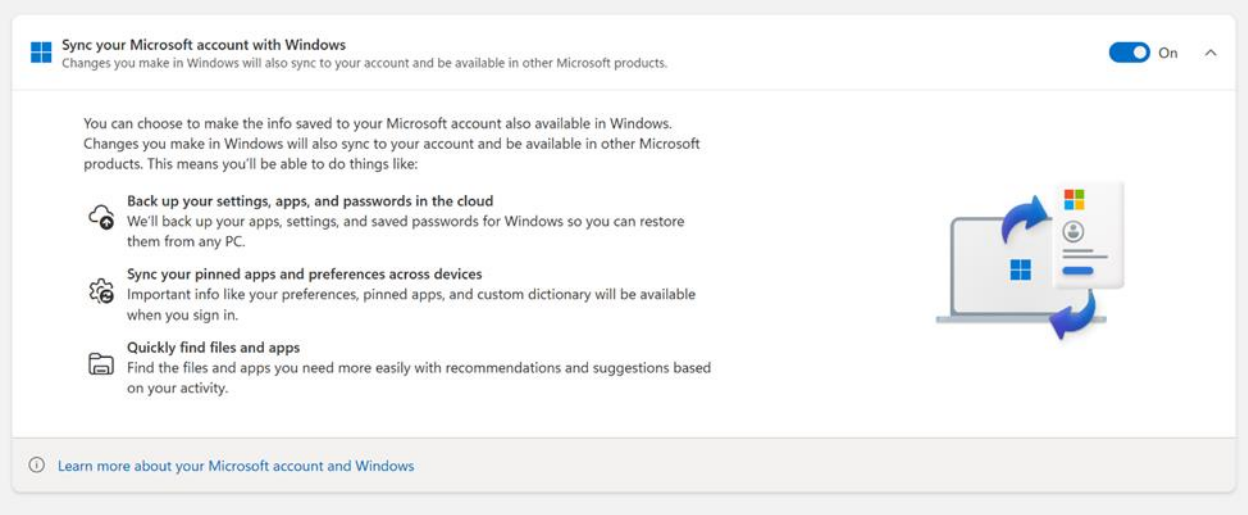


Source: Microsoft

53. Once stored and made available on the Microsoft Graph, Account Data is available to first- and third-party applications, which can cross-use or combine the data with other personal data. To the extent Microsoft combines personal data in the user's account from Windows with personal data from other services, the consent in **Figure 6** covers this combination.

54. Users can control the consent to sync account data with Windows by accessing the setting available on the account.microsoft.com website, as illustrated in **Figure 7**. If the user does not consent, or later withdraws consent, Windows will not ask the user for consent more than once within one year.

Figure 7. Setting To Control Consent To Sync Account Data With Windows



Source: Microsoft

55. **Windows Required Service Data.** Microsoft does not combine personal data provided in Required Service Data with personal data from other services. As described above, Windows sends Required Service Data to Microsoft to provide cloud-enabled features. The Required Service Data is typically discarded after providing the service. Some services process Required Service Data and update the user's Account Data using the results. Microsoft will not combine this updated Account Data with personal data from other products and services unless the service seeks separate consent to do so before it writes the Account Data. Some services de-identify the Required Service Data and store the results, and this data may be used to improve the service. After the data is de-identified, it is no longer personal data, and any subsequent combination with data from other sources is not a combination with personal data from Windows under Article 5(2)(b) of the DMA.

56. **Information on IT Administrators.** IT Administrators can control settings for work and school accounts. When users authenticate to Windows using a "work or school account," Windows makes it possible for the IT administrator who provided that account to configure settings on the device. These settings include some of the controls governing how personal data is collected and used by Windows.[11] For example, IT Administrators can enable the Windows Diagnostic Data processor configuration, which makes the customer the controller of diagnostic data collected from devices configured with this setting.[12] When IT administrators manage settings as part of configuring the device, the IT administrator provides (or declines) consent on behalf of the end user for certain processing of the user's personal data and Windows may not seek additional consent directly from the end user. Microsoft may process Diagnostic Data on behalf of the customer including combining Diagnostic Data with personal data in other products and services. The customer as the controller requests this processing and, consequently, Article 5(2) of the DMA does not apply here because the customer, and not Microsoft, is controlling the processing.

---

11 *See, e.g.*, Windows Privacy Compliance Guide.

12 *See* Configure Windows diagnostic data in your organization.

57. **Cybersecurity Protection.** Windows comes with security features, such as the Microsoft Defender Antivirus[13] and Microsoft Defender SmartScreen[14] (the "**Defender Security Services**") to protect users against cyberattacks. The Defender Security Services provide security protection to Windows users.

58. The Defender Security Services work by obtaining data signals about potentially malicious files and creating signatures or other mechanisms to detect that file before it is able to infect another machine and/or to mitigate the malicious file's impact after the fact. For example, a file on Windows PC A might install and then engage in malicious activity on the PC in a way that is observed by Microsoft Defender. That information is sent into the Microsoft Defender Security Services to determine if the file is truly malicious and to create mitigations for the file, such as creating signatures to identify that file on other computers and potentially prevent it from running. This analysis work is done as part of Microsoft's overall Defender Security Services. Those learnings from PC A could then be applied to PC B to prevent PC B from getting infected in the first place.

59. Similarly, Microsoft could detect threats based on signals from other Microsoft services. For example, it might detect through the Outlook service that a file is being sent from a particular domain. It can then use that domain information to infer that other files from that similar domain may also be malicious and provide better protection to Windows PC users who receive messages from that domain or who might use the browser to navigate to the website associated with that domain. It could, for example, enable future emails from such a domain to be blocked. The Defender Security Services can also use the outputs of this personal data processing to identify Windows PCs and Windows accounts that have been used to conduct abuse, track those devices and accounts, alert impacted users, and prevent further abuse. Microsoft provides security for other Microsoft products and services and offers various security products to customers that rely upon this shared malicious software detection capabilities.[15]

60. Processing data from Windows and other sources is therefore critical to protecting all Windows users. It enables Microsoft to identify and mitigate security risks for users faster and more efficiently than if data from Windows and any other product and service had to remain in a silo. The data is used solely for the purpose of providing security to Windows devices and other Microsoft products and services. It is not used for any non-security Microsoft product or service, and it is not used for any user or device tracking, profiling, or targeted advertising.

61. Furthermore, to help deter cybercrime throughout the technology sector, Microsoft assists other security solutions in protecting users on any platform from the same threats. Windows provides open APIs that provide equal access to third-party security providers to access data points collected from Windows by the Defender Security Services. Microsoft also offers the Microsoft Virus Initiative through which it shares

---

[13] Microsoft Defender Antivirus is an antimalware solution that protects Windows devices from viruses, Trojans, ransomware, and other types of malware.

[14] Microsoft SmartScreen protects Windows devices by checking the applications and files the user is downloading or seeking to run against a list of known safe or unsafe items as well as of items that might be unknown with little reputation, and warns of potentially unsafe files.

[15] *See* https://www.microsoft.com/en-us/security.

information with other security providers about security threats.[16] The Microsoft Digital Crimes Unit ("**DCU**") uses this information to investigate cybercrime targeting Microsoft services and customers. This information allows the DCU to understand the techniques, tactics, and procedures utilized by cybercriminals to harm people. The evidence and insights obtained by the DCU through accessing this information also enables criminal referrals to law enforcement agencies worldwide, which helps governments fight cybercrime, bring legal proceedings against cybercriminals, and protect their citizens.[17] And Microsoft creates threat briefs and other reports to share with the broader industry.[18]

62. For all of its cybersecurity-related work, Microsoft collects data from Windows and certain applications installed on Windows and combines it with data from other sources. The consent obligation in Article 5(2)(b) of the DMA does not apply to combining personal data exclusively for the purposes of Microsoft's cybersecurity work, including for Microsoft's Defender Security Services. As the Commission has made clear, improving cybersecurity is essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information.[19] Because of the critical importance of maintaining and improving cybersecurity, the EU is adopting reinforced obligations on, *e.g.*, OS providers.[20] Consistent with EU cybersecurity goals, Article 5(2) of the DMA refers to Article 6(1)(c) of the GDPR[21] according to which processing of personal data is lawful if it is "*necessary for compliance with a legal obligation to which the controller is subject*."

D. Compliance With Article 5(2)(c) Of The DMA

63. Windows either has consent to cross-use data through the same mechanisms used to obtain consent to combine personal data described above, or in circumstances where there is no combination of personal data, Windows only cross-uses data in services that are provided together with or in support of the associated Windows feature and not separately.

64. **Windows Diagnostic Data.** Microsoft cross-uses Windows Diagnostic Data in other services provided by Microsoft. To the extent such cross-use is in other services

16 *See* Microsoft Virus Initiative.

17 *See* Digital Crimes Unit: Leading the fight against cybercrime.

18 *See* Threat briefs.

19 *See* The EU's Cybersecurity Strategy for the Digital Decade, p.4.

20 *See* Proposal for a Regulation Of The European Parliament And Of The Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 and Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products.

21 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 ("**GDPR**")), OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

provided separately, rather than together with Windows, Microsoft only does so with consent as described above.

65. **Account Data.** As described above, Microsoft obtains consent to store personal data from Windows in the user's account, which may result in the cross-use of Account Data in other services provided by Microsoft. To the extent Microsoft cross-uses Account Data from Windows in other services provided by Microsoft separately, the consent in **Figure 6** covers this cross-use for PCs in the EEA.

66. **Windows Required Service Data.** Article 5(2)(c) of the DMA does not apply to any cross-use of Required Service Data in other services provided by Microsoft because those services are not provided separately. Instead, any such services are always provided together with and in support of the Windows features they enable.

67. As described above, some features of Windows are powered by cloud services. Windows sends Required Service Data to the service to provide the cloud-enabled features. To the extent any of these services are "other services" provided by Microsoft under Article 5(2) of the DMA, and not part of Windows, the services are always provided together with and in support of the associated features in Windows.

68. Consequently, to the extent Windows cross-uses Required Serviced Data in other services, consent is not required.

E. Compliance With Article 5(2)(d) Of The DMA

69. Article 5(2)(d) of the DMA provides that Windows may not sign-in end users to other Microsoft services in order to combine personal data unless the user has provided consent.

70. End users are required to sign-in to Windows, but to comply with the DMA on PCs in the EEA, Windows no longer combines personal data from Windows with personal data from any other Microsoft product or service as a result of that authentication unless the user provides opt-in consent.

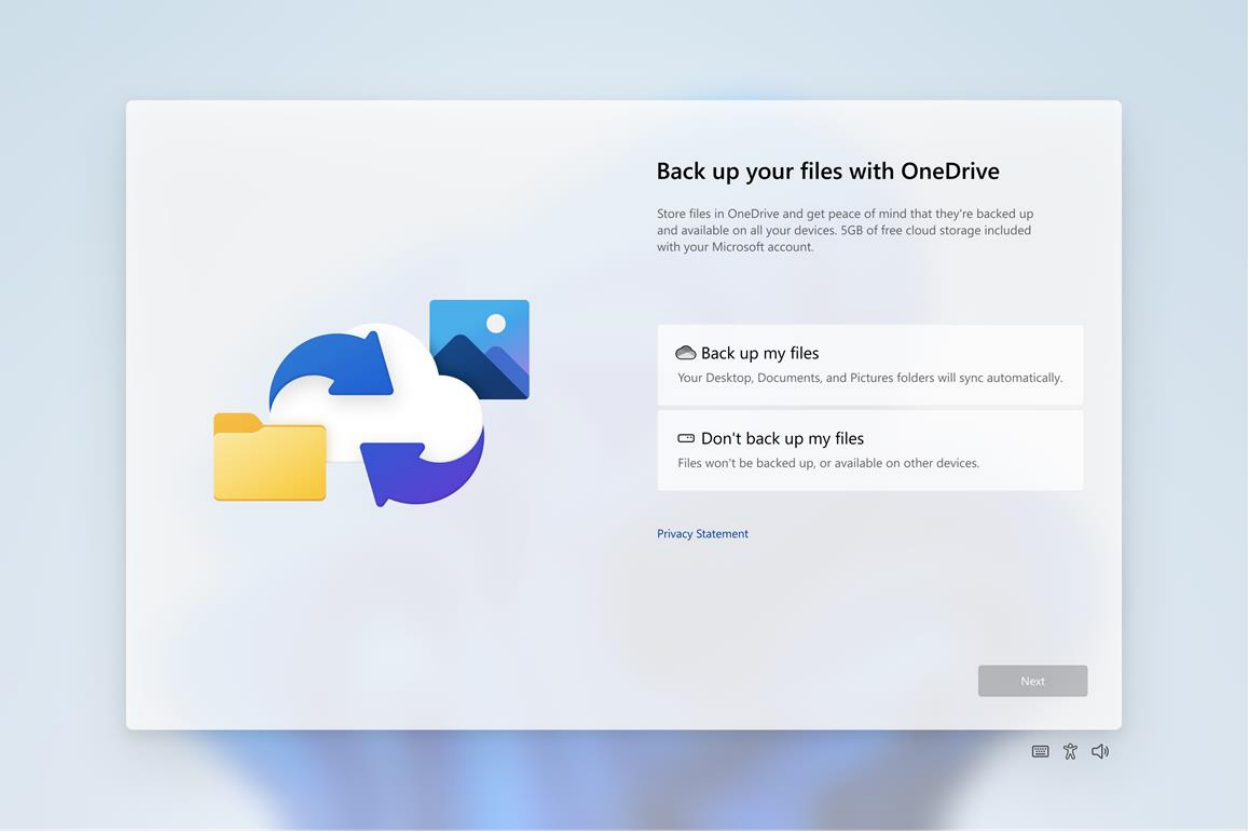
71. Prior to the DMA compliance deadline, users were also automatically signed-in to other Microsoft products and services that they accessed using the same account used to sign-in to Windows. Going forward, as a result of the DMA, users on PCs in the EEA who sign-in to Windows using a personal Microsoft account or a work or school account will no longer be automatically signed-in to Microsoft applications and services running on Windows. The only exception to this pertains to the OneDrive cloud storage application.

72. Windows does automatically sign-in users to OneDrive, but signing-in to OneDrive does not result in Microsoft combining any personal data. OneDrive is a Microsoft file storage application, which the user can access through the Windows file system interface, and when Windows signs-in the user to OneDrive it merely makes the OneDrive file storage an option for the user in the Windows file system. Any files stored in OneDrive are stored by the user for the exclusive benefit of the user (and not Microsoft). When a user chooses to store files in OneDrive, it does not cause a Microsoft data combination under Article 5(2)(d) of the DMA. A user's files are only stored in OneDrive pursuant to that user's direction and consent.

73. Users may choose to store files in OneDrive by giving Windows a command to do so, for example, by the user taking action to save an individual file to OneDrive or by moving a file (such as via "drag-and-drop") from some other storage location to OneDrive.

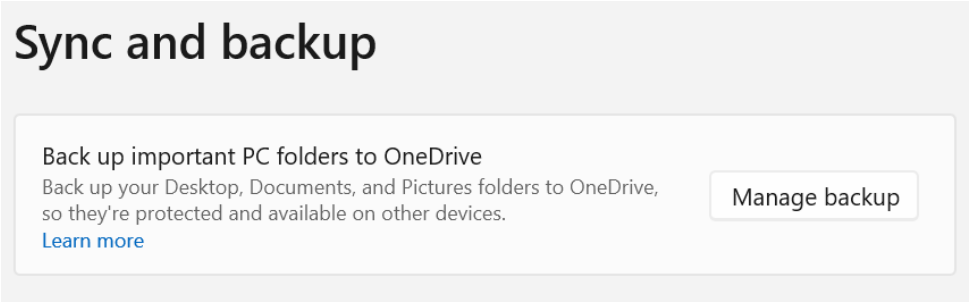
74. Microsoft provides users with the option to back up automatically to OneDrive certain key folders in the Windows file system. Windows requests consent to automatically back up these folders to OneDrive on PCs in the EEA during the device setup experience, as shown in **Figure 8**. The user can control which folders OneDrive backs up through controls in OneDrive settings, as illustrated in **Figures 9-10**.

Figure 8. Windows Consent To Back Up Files With OneDrive



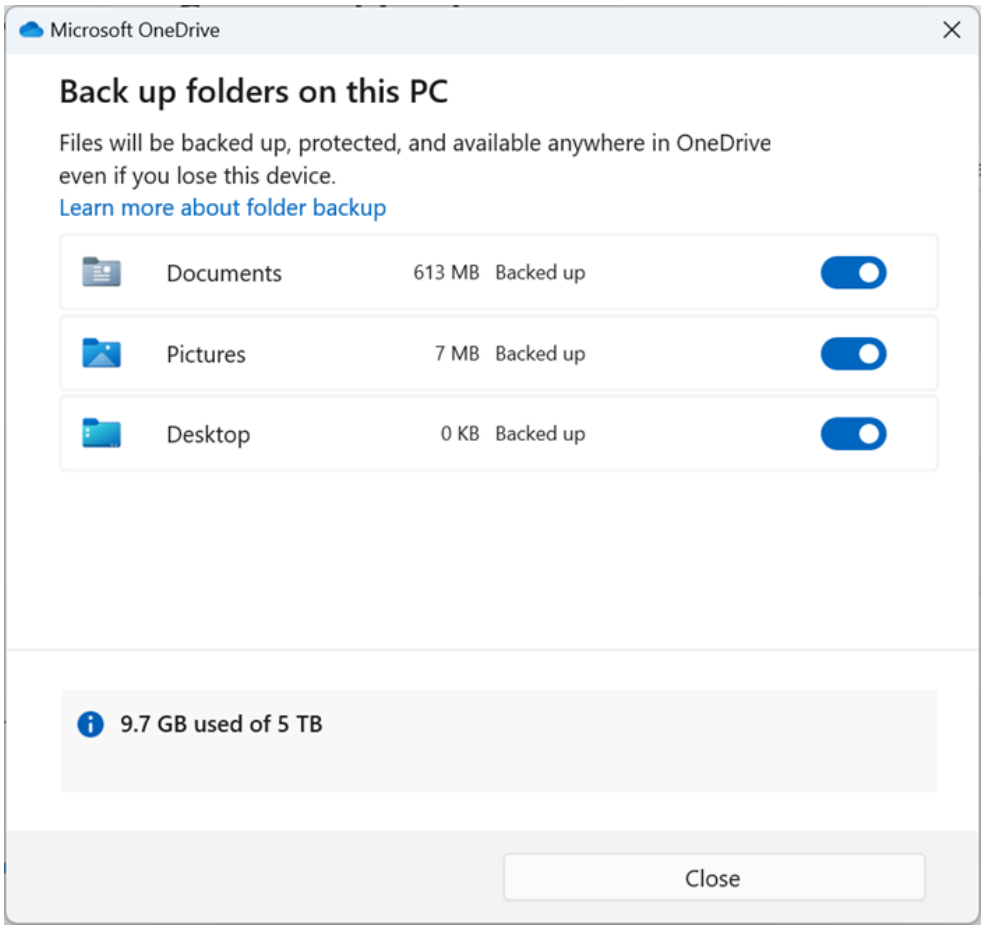
Source: Microsoft

Figure 9. Sync And Backup Settings In OneDrive



Source: Microsoft

Figure 10. OneDrive Settings To Select Which Important Folders OneDrive Will Back Up



Source: Microsoft

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[22]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

75. Microsoft refers to **Section 2.1.2 (i)** above for the measures that were introduced on PCs in the EEA to comply with the DMA.

b) when the measure was implemented;

76. Most of the practices above existed prior to the DMA compliance deadline. Where Microsoft made changes described above for Windows running on PCs in the EEA, they were implemented in the months prior to the DMA compliance deadline.

[22] For example, this may be particularly relevant to illustrate changes impacting user journeys.

c) the scope of the measure in terms of the products/services/devices covered;

77. The practices described in **Section 2.1.2 (i)** above apply to the Windows PC OS installed directly on PCs as well as Microsoft's "desktop as a service" offerings (Azure Virtual Desktop and Windows 365) where the software runs in the cloud.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

78. The practices above that existed prior to the DMA compliance deadline are generally available worldwide. As described in **Section 2.1.2 (i)** above, Microsoft made certain changes to its practices to comply with the DMA that apply only to Windows running on PCs in the EEA.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

79. Microsoft refers to **Section 2.1.2 (i)** above.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[23] consent forms,[24] warning messages, system updates, functionalities available, or customer journey to access functionalities[25]);

80. Microsoft refers to **Section 2.1.2 (i)** above.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned

---

23 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

24 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

25 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

(e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

81. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

82. None.

i) any consultation[26] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high-level description of the topic of the consultation with those users/parties;

83. Microsoft conducted a series of video interviews through a third-party vendor with French and German consumer customers to get feedback on potential designs for the Windows Account Sync consent request illustrated in **Figure 6**. The goal of this user research was to assess user comprehension and ensure that users would understand the privacy implications of the consent in context. Microsoft used the results of this research as one of the inputs into the final design of the consent request.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

84. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

85. None.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

86. None.

[26] This information should include a description of the methodology for the consultation.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

87. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

88. None.

o) any type of market analysis or testing (in particular A/B testing[27]), business user surveys or consumer surveys or end user consent rates,[28] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[29]

89. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[30]

90. As noted above for point **2.1.2 (ii) (i)**, Microsoft performed user research related to the Windows Account Sync consent request illustrated in **Figure 6**, but this research was focused on whether users understood the consent and did not evaluate expected or actual impact of the consent request.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of

---

27 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

28 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

29 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

30 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

91. Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

r) any relevant data[31] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

92. As outlined in **Section 2.1.2 (ii) (q)** above, Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

93. Microsoft remains open to discussing any indicators and ways to monitor those indicators that would assist the Commission in its assessment of whether a particular measure is effective in achieving the objectives of the DMA, including metrics that track the choices made by users under mechanisms required by the DMA such as consent rates, installing and setting applications as the default, use of data portability mechanisms or others.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently

[31] Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

audited, data access policies, data retention policies and measures to enable secure data access).

94. None.

Regarding Article 5(3)

95. Microsoft refers to **Section 2.3** below.

Regarding Article 5(4)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

96. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 5(4) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[32] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

97. Article 5(4) of the DMA provides: "[t]*he gatekeeper shall allow business users, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels, and to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the gatekeeper*."

98. When a user launches an application on Windows, Windows is designed such that the application – not the Windows OS – controls its own commercial experiences. The application, therefore, may choose to communicate and promote offers to users through the experience in that application or by directing the user to the internet or elsewhere. Similarly, the application may conclude contracts with its users through the experiences in the application or by directing the user to the internet or elsewhere. This was true before the DMA was adopted, is the same wherever Windows is available, and no change was necessary to comply with the DMA. This design alone is sufficient to comply with Article 5(4) of the DMA.

[32] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[33]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

99. None.

b) when the measure was implemented;

100. None.

c) the scope of the measure in terms of the products/services/devices covered;

101. None.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

102. None.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

103. None.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[34] consent forms,[35] warning messages, system updates, functionalities available, or customer journey to access functionalities[36]);

104. None.

---

33 For example, this may be particularly relevant to illustrate changes impacting user journeys.

34 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

35 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

36 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

105. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

106. None.

i) any consultation[37] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high- level description of the topic of the consultation with those users/parties;

107. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

108. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

109. None.

[37] This information should include a description of the methodology for the consultation.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

110. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

111. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

112. None.

o) any type of market analysis or testing (in particular A/B testing[38]), business user surveys or consumer surveys or end user consent rates,[39] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[40]

113. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[41]

114. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of

---

38 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

39 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

40 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

41 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

115. None.

r) any relevant data[42] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

116. None.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

117. None.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

118. None.

[42] Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

Regarding Article 5(5)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

119. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 5(5) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[43] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

120. Article 5(5) of the DMA provides: "[t]*he gatekeeper shall allow end users to access and use, through* its *core platform services, content, subscriptions, features or other items, by using the software application of a business user, including where those end users acquired such items from the relevant business user without using the core platform services of the gatekeeper*."

121. When a user launches an application on Windows, Windows is designed such that the application – not the Windows OS – controls its own the commercial experiences. Therefore, nothing prevents the application from allowing users to access and use content, subscriptions, features, or other items in the application experience. And the application may do so even when the user did not acquire those items through Windows. This was true before the DMA was adopted, is the same wherever Windows is available, and no change was necessary to comply with the DMA. This design alone is sufficient to comply with Article 5(5) of the DMA.

[43] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[44]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

122. None.

b) when the measure was implemented;

123. None.

c) the scope of the measure in terms of the products/services/devices covered;

124. None.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

125. None.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

126. None.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[45] consent forms,[46] warning messages, system updates, functionalities available, or customer journey to access functionalities[47]);

127. None.

---

44 For example, this may be particularly relevant to illustrate changes impacting user journeys.

45 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

46 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

47 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

128. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

129. None.

i) any consultation[48] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high- level description of the topic of the consultation with those users/parties;

130. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

131. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

132. None.

[48] This information should include a description of the methodology for the consultation.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

133. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

134. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

135. None.

o) any type of market analysis or testing (in particular A/B testing[49]), business user surveys or consumer surveys or end user consent rates,[50] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[51]

136. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[52]

137. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of

---

49 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

50 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

51 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

52 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

138. None.

r) any relevant data[53] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

139. None.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

140. None.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

141. None.

[53] Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

Regarding Article 5(6)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

142. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 5(6) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[54] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

143. Article 5(6) of the DMA provides: "[t]*he gatekeeper shall not directly or indirectly prevent or restrict business users or end users from raising any issue of non-compliance with the relevant Union or national law by the gatekeeper with any relevant public authority, including national courts, related to any practice of the gatekeeper. This is without prejudice to the right of business users and gatekeepers to lay down in their agreements the terms of use of lawful complaints-handling mechanisms*."

144. Microsoft has created a centralized webpage to provide information regarding, and receive feedback about, Microsoft's compliance with the DMA.[55] To comply with Article 5(6) of the DMA, Microsoft has clearly stated, on this webpage, that any business user or end user may raise any issue of non-compliance with any appropriate EU authority. This statement also makes clear that nothing in any Microsoft agreement limits anyone from raising such a concern, and provides a way for anyone to receive additional guidance if they have a concern that any Microsoft confidentiality agreement constrains their ability to raise any issue with any EU authority. The following is the statement on Microsoft's DMA Compliance webpage:

> "*Microsoft customers, users, partners, employees and contractors may raise any concern they have with Microsoft legal compliance, including compliance with the European Digital Markets Act, with Microsoft through the "Feedback" section of this web site. They may also raise any such concerns with an appropriate EU authority. Nothing in any Microsoft agreement limits any customer, user, or partner from raising such a concern with an appropriate EU authority. If you have any*

[54] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

[55] *See* https://www.microsoft.com/en-us/legal/compliance/dmacompliance.

question about your ability to raise a concern, please contact DMAFeedback@microsoft.com."

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[56]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

145. Microsoft refers to **Section 2.1.2 (i)** above.

b) when the measure was implemented;

146. This measure is implemented by the compliance deadline.

c) the scope of the measure in terms of the products/services/devices covered;

147. This measure applies to the entirety of Windows.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

148. This measure applies throughout the entirety of the EEA.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

149. None.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[57] consent forms,[58] warning messages, system

[56] For example, this may be particularly relevant to illustrate changes impacting user journeys.

[57] For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

[58] This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

updates, functionalities available, or customer journey to access functionalities[59]);

150. None.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

151. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

152. None.

i) any consultation[60] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high- level description of the topic of the consultation with those users/parties;

153. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

154. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing

---

59 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

60 This information should include a description of the methodology for the consultation.

open standards and/or state of the art implementations and the reasons for not choosing them;

155. None.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

156. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

157. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

158. None.

o) any type of market analysis or testing (in particular A/B testing[61]), business user surveys or consumer surveys or end user consent rates,[62] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[63]

159. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or

---

61 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

62 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

63 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[64]

160. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

161. Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

r) any relevant data[65] **which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;**

162. As outlined in **Section 2.1.2 (ii) (q)** above, Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

163. Microsoft remains open to discussing any indicators and ways to monitor those indicators that would assist the Commission in its assessment of whether a particular measure is effective in achieving the objectives of the DMA, including metrics that

64 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

65 Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

track the choices made by users under mechanisms required by the DMA such as consent rates, installing and setting applications as the default, use of data portability mechanisms or others.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

164. None.

Regarding Article 5(7)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

165. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 5(7) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[66] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

166. Article 5(7) of the DMA provides: "[t]*he gatekeeper shall not require end users to use, or business users to use, to offer, or to interoperate with, an identification service, a web browser engine or a payment service, or technical services that support the provision of payment services, such as payment systems for in-app purchases, of that gatekeeper in the context of services provided by the business users using that gatekeeper's core platform services*."

167. When a user launches an application on Windows, Windows is designed such that the application – not the Windows OS – controls its own commercial experiences. The application, therefore, may be designed to use any identification service, web browser engine, or payment service it chooses. Windows has no requirement that applications running on Windows use the Microsoft version of these services. This was true before the DMA was adopted, is the same wherever Windows is available, and no change was necessary to comply with the DMA. This design alone is sufficient to comply with Article 5(7) of the DMA.

[66] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[67]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

168. None.

b) when the measure was implemented;

169. None.

c) the scope of the measure in terms of the products/services/devices covered;

170. None.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

171. None.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

172. None.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[68] consent forms,[69] warning messages, system updates, functionalities available, or customer journey to access functionalities[70]);

173. None.

---

67 For example, this may be particularly relevant to illustrate changes impacting user journeys.

68 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

69 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

70 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

174. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

175. None.

i) any consultation[71] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high- level description of the topic of the consultation with those users/parties;

176. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

177. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

178. None.

[71] This information should include a description of the methodology for the consultation.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

179. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

180. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

181. None.

o) any type of market analysis or testing (in particular A/B testing[72]), business user surveys or consumer surveys or end user consent rates,[73] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[74]

182. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[75]

183. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of

---

72 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

73 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

74 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

75 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

184. None.

r) any relevant data[76] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

185. None.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

186. None.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

187. None.

[76] Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

Regarding Article 5(8)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

188. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 5(8) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[77] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

189. Article 5(8) of the DMA provides: "[t]*he gatekeeper shall not require business users or end users to subscribe to, or register with, any further core platform services listed in the designation decision pursuant to Article 3(9) or which meet the thresholds in Article 3(2), point (b), as a condition for being able to use, access, sign up for or registering with any of that gatekeeper's core platform services listed pursuant to that Article*."

190. Windows complies with Article 5(8) of the DMA because end users may use Windows, and business users may develop and distribute applications that run on Windows, without having to subscribe to or register with other CPSs provided by Microsoft that have been designated (*i.e.*, the LinkedIn online social networking service) or that meet the thresholds in Article 3(2)(b) of the DMA (*i.e.*, the Outlook.com number-independent interpersonal communication service, the Microsoft Edge web browser, the Microsoft Bing online search engine, and the Microsoft Advertising online advertising service).

A. End Users

191. Microsoft does not require end users to subscribe to or register with its other CPSs as a condition to use Windows.

192. As described in the section covering compliance with Article 5(2) of the DMA above, Windows does require users to sign-in to Windows, but end users are free to use Windows without authenticating to Microsoft's other CPSs. End users may elect to sign-in to Microsoft Edge, Microsoft Bing, or Microsoft Advertising using the same

[77] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

account the end user used to sign-in to Windows, but this is the end user's choice and there is no requirement to register for or use those services. If an end user registers for an Outlook.com account, then the end user may use that same account as their Microsoft Account with which to sign-in to Windows, but, again, this is the end user's choice and there is no requirement to do so. End users can create a Microsoft Account using an email address from a third-party email service.

193. In addition, when end users sign-in to Windows, they are no longer automatically signed-in to Microsoft applications and services running on Windows and so are no longer signed-in to Microsoft Edge or Bing that meet the thresholds in Article 3(2)(b) of the DMA. To the extent that Windows' pre-DMA practice of automatically signing-in a user who accesses Microsoft Edge or Bing might be considered to be a requirement to subscribe to or register with those services, that practice ended on PCs in the EEA before the DMA compliance deadline. Windows has never automatically created accounts for users of the LinkedIn online social networking service, Outlook.com, or Microsoft Advertising.

194. Thus, Windows complies with Article 5(8) of the DMA with respect to end users.

B. <u>Business Users</u>

195. Microsoft does not require business users to subscribe to or register with its other CPSs as a condition to use Windows or to develop applications or services for Windows.

196. Windows is an open platform and developers can freely develop applications or services for Windows and distribute them to end users, without ever contacting Microsoft. Business users may independently choose to register for other CPSs and may, for example, integrate services such as Microsoft Advertising into their applications, but there is no requirement to do so.

197. Thus, Windows complies with Article 5(8) of the DMA with respect to business users.

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[78]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

198. Microsoft refers to **<u>Section 2.1.2 (i)</u>** above.

b) when the measure was implemented;

199. Microsoft refers to **<u>Section 2.1.2 (i)</u>** above.

[78] For example, this may be particularly relevant to illustrate changes impacting user journeys.

c) the scope of the measure in terms of the products/services/devices covered;

200. The practices described above apply to the Windows PC OS installed locally on PCs as well as Microsoft's "desktop as a service" offerings (Azure Virtual Desktop and Windows 365) where the software runs in the cloud.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

201. The practices described above apply to Windows on PCs in the EEA.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

202. Microsoft refers to **Section 2.1.2 (i)** above.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[79] consent forms,[80] warning messages, system updates, functionalities available, or customer journey to access functionalities[81]);

203. Microsoft refers to **Section 2.1.2 (i)** above.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

204. None.

---

79 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

80 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

81 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

205. None.

i) any consultation[82] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high-level description of the topic of the consultation with those users/parties;

206. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

207. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

208. None.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

209. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

210. As described above, to the extent that Windows' pre-DMA practice of automatically signing-in a user who accesses Microsoft Edge or Bing might be considered to be a requirement to subscribe to or register with those services, that practice ended on PCs in the EEA as a result of Microsoft's measures to comply with Article 5(2) of the DMA.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant

[82] This information should include a description of the methodology for the consultation.

provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

211. Microsoft refers to **Section 2.1.2 (i)** above.

o) any type of market analysis or testing (in particular A/B testing[83]), business user surveys or consumer surveys or end user consent rates,[84] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[85]

212. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[86]

213. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

214. Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

---

83 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

84 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

85 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

86 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

r) any relevant data[87] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

215. As outlined in **Section 2.1.2 (ii) (q)** above, Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

216. Microsoft remains open to discussing any indicators and ways to monitor those indicators that would assist the Commission in its assessment of whether a particular measure is effective in achieving the objectives of the DMA, including metrics that track the choices made by users under mechanisms required by the DMA such as consent rates, installing and setting applications as the default, use of data portability mechanisms or others.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

217. None.

[87] Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

Regarding Article 5(9)

218. Microsoft refers to **Section 2.3** below.

Regarding Article 5(10)

219. Microsoft refers to **Section 2.3** below.

Regarding Article 6(2)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

220. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 6(2) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[88] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

221. Article 6(2) of the DMA provides:

> "*The gatekeeper shall not use, in competition with business users, any data that is not publicly available that is generated or provided by those business users in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services, including data generated or provided by the customers of those business users.*
>
> *For the purposes of the first subparagraph, the data that is not publicly available shall include any aggregated and non-aggregated data generated by business users that can be inferred from, or collected through, the commercial activities of business users or their customers, including click, search, view and voice data, on the relevant core platform services or on services provided together with, or in support of, the relevant core platform services of the gatekeeper*."

222. Article 6(2) of the DMA prohibits Microsoft from using non-public data collected from third-party applications by Windows on PCs in the EEA to compete with the third-party applications from which the data was collected.

223. As described above in the section discussing compliance with Article 5(2) of the DMA, there are three categories of data Windows collects: (i) Windows Diagnostic Data, (ii) Account Data, and (iii) Windows Required Service Data. As described below, Microsoft changed its data practices so that non-public Diagnostic Data collected about third-party applications by Windows on PCs in the EEA is isolated and used only for

[88] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

permitted purposes, which will exclude uses that might be considered in competition with the application provider. Neither Account Data collected by Windows nor Windows Required Service Data is used for competitive purposes and therefore no change was needed in relation to those two categories of data to comply with Article 6(2) of the DMA.

A. Diagnostic Data

224. To comply with Article 6(2) of the DMA for Windows Diagnostic Data, Microsoft will change its practices for data collected from PCs in the EEA. As described above, Windows Diagnostic Data includes information about what third-party applications are installed on a user's PC and, when collected at the optional level, information about a user's use of third-party applications. Additionally, Diagnostic Data may include information generated as a result of third-party applications running on Windows. The vast majority of applications running on Windows PCs are not provided by Microsoft and accessing Diagnostic Data from all applications regardless of the developer is critical to maintaining security and improving the Windows platform in the interest of business users and end users alike. To comply with Article 6(2) of the DMA, Microsoft introduced new data practices to isolate and control access to third-party application Diagnostic Data collected from PCs in the EEA, which prevent access to isolated data for prohibited purposes as described below.

225. Microsoft continues to use the isolated third-party application Diagnostic Data for the primary diagnostic data purpose, which is to monitor, detect, and remediate vulnerabilities, bugs, or other problems in the performance of Windows including the applications running on Windows and the hardware on which Windows runs. Microsoft, however, has stopped uses of isolated data for purposes that might be in competition with a third-party application provider. Microsoft has ceased to use the isolated data for A/B feature testing. In addition, in the future, when Microsoft resumes the use of Diagnostic Data in delivering Tailored Experiences as explained above in relation to compliance with Article 5(2) of the DMA, Microsoft will not use the isolated data for this purpose.

226. Prior to the DMA compliance deadline, Microsoft used Diagnostic Data, including this isolated data, for competitive business intelligence purposes, such as to measure relative usage of Microsoft and competing software. To comply with Article 6(2) of the DMA, Microsoft no longer uses isolated data for this purpose unless the data is first aggregated and made public, in which case, Microsoft will use only the aggregated publicly-available data for these competitive business intelligence purposes.

B. Account Data

227. Account data collected by Windows is not used for competitive purposes. As described above, Account Data is data associated with the user's account and typically made available through the Microsoft Graph. Windows uses Account Data only to deliver the associated features, such as backing up and restoring the user's settings, regardless of whether the data was provided or generated by third-party applications. Microsoft is not competing with an application provider by synchronizing data with the user's account.

C. Windows Required Service Data

228. Windows Required Service Data is not used for competitive purposes. As described above, some features of Windows are powered by cloud services. Windows sends Required Service Data to these services to provide the cloud-enabled features. Applications running on Windows, including third-party applications, can call APIs that will result in Windows sending Required Service Data to Microsoft. Microsoft is not competing with application providers when it uses data provided or generated by third-party applications to provide those applications with cloud-enabled features.

229. In addition to delivering the service required by the associated feature, Microsoft may aggregate or de-identify the Required Service Data and use it to improve the quality of the service. Microsoft is not competing with application providers when improving the quality of services used by applications because such improvements improve the quality of those applications.

230. Some cloud-enabled features may use Required Service Data to update the user's Account Data. Microsoft does not associate this data with the application that caused it to be stored, and as described above, Microsoft does not use Account Data to compete with business users.

D. Cybersecurity Protection

231. As described above in the section describing compliance with Article 5(2) of the DMA, Windows security features, such as the Defender Security Services, collect and use data, including data about third-party applications running on the PC, for the purpose of providing cybersecurity protection. The data is used for the purpose of providing security to Windows devices and other Microsoft products and services. Processing this data is critical to protecting all Windows users, as well as the integrity of all applications running on Windows, and consequently is not used in competition with those application providers.

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[89]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

232. As described above, Microsoft changed its data practices with respect to Diagnostic Data collected from PCs in the EEA to comply with the DMA.

b) when the measure was implemented;

233. Microsoft changed its data practices with respect to Diagnostic Data collected from PCs in the EEA to comply with the DMA in the months prior to the DMA compliance deadline.

[89] For example, this may be particularly relevant to illustrate changes impacting user journeys.

c) the scope of the measure in terms of the products/services/devices covered;

234. The practices described above apply to the Windows PC OS installed locally on PCs as well as Microsoft's "desktop as a service" offerings (Azure Virtual Desktop and Windows 365) where the software runs in the cloud.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

235. Microsoft changed its data practices with respect to Diagnostic Data only for data collected from PCs in the EEA.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

236. As described above, Microsoft updated its data platform to identify and isolate Diagnostic Data events that include data associated with third-party applications and limit their use to primary diagnostic purposes. Microsoft implemented event isolation by updating the routing rules in its data collection and storage platform for incoming events. Events that are "tagged" as being collected from PCs in the EEA and that are identified as relating to third-party applications are placed in an isolated location in Microsoft's storage platform and restricted to an appropriate use.

237. In addition to isolating this Diagnostic Data, Microsoft implemented updates to its data access and control process to ensure that the isolated data is used only for primary diagnostic purposes (*i.e.*, to diagnose and fix problems in Windows, applications, and hardware).

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[90] consent forms,[91] warning messages, system updates, functionalities available, or customer journey to access functionalities[92]);

238. None.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees,

90 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

91 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

92 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

239. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

240. None.

i) any consultation[93] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high-level description of the topic of the consultation with those users/parties;

241. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

242. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

243. None.

[93] This information should include a description of the methodology for the consultation.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

244. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

245. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

246. As described above, Windows security features collect and use data, including data about third-party applications running on the PC, to provide cybersecurity protection. This protects the integrity of Windows and the applications running on Windows and is not used in competition with application providers.

o) any type of market analysis or testing (in particular A/B testing[94]), business user surveys or consumer surveys or end user consent rates,[95] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[96]

247. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[97]

248. None.

---

94 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

95 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

96 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

97 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

249. Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

r) any relevant data[98] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

250. As outlined in **Section 2.1.2 (ii) (q)** above, Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

251. Microsoft remains open to discussing any indicators and ways to monitor those indicators that would assist the Commission in its assessment of whether a particular measure is effective in achieving the objectives of the DMA, including metrics that track the choices made by users under mechanisms required by the DMA such as consent rates, installing and setting applications as the default, use of data portability mechanisms or others.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access

[98] Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

(including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

252. None.

Regarding Article 6(3)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

253. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 6(3) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[99] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

254. Article 6(3) of the DMA includes the following obligation: "[t]*he gatekeeper shall allow and technically enable end users to easily un-install any software* applications *on the operating system of the gatekeeper, without prejudice to the possibility for that gatekeeper to restrict such un-installation in relation to software applications that are essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third parties.*"

255. Microsoft complies with Article 6(3) of the DMA because (i) users can easily uninstall applications on Windows 10 and 11 (**Section A**) and (ii) users can easily change default settings on Windows 10 and 11 (**Section B**). As Windows 10 and 11 have always allowed users to easily perform these functions, no new measures were required to comply with Article 6(3) of the DMA in terms of the process for uninstalling applications or changing default settings.

256. Microsoft, however, has (i) reviewed its approach to what features of Windows constitute software applications and made sure that all applications on Windows 10 and 11 are uninstallable[100] and (ii) ensured that for Windows devices in the EEA, when a user clicks on a link or file type, Windows uses the default application to open that link or file.

---

99 The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

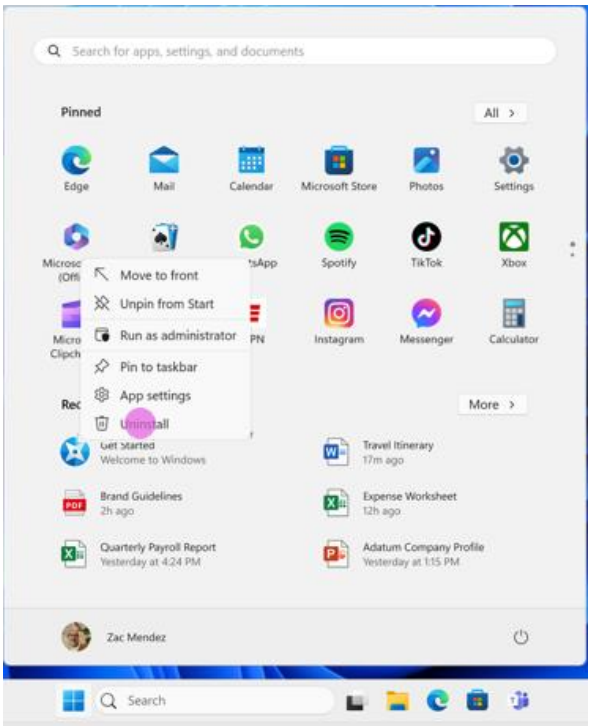
100 For example, Web Search from Microsoft Bing and Microsoft Edge were redesigned to become applications because the DMA characterizes web search and web browsing functionality as distinct from an OS. These are now applications that can also be easily uninstalled but only on PCs within the EEA.

A. Users Can Easily Uninstall Applications On Windows 10 And 11

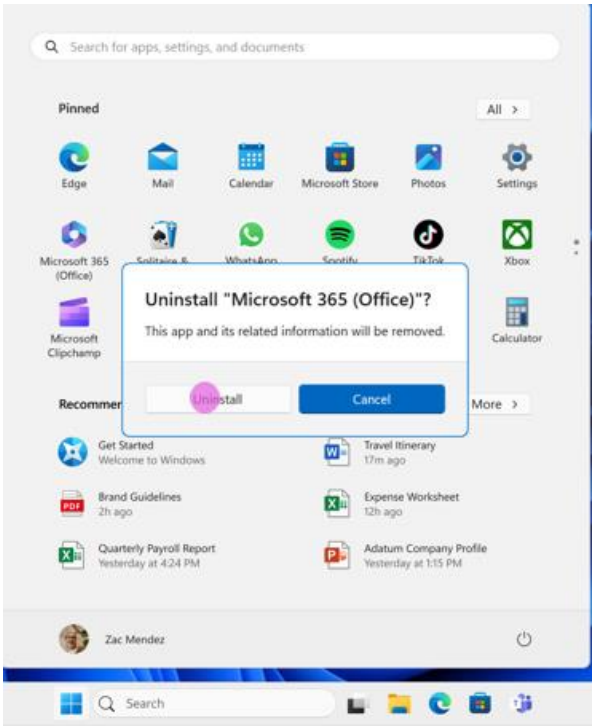
257. All applications can be uninstalled by the user on Windows 10 and 11.[101] This includes applications installed by the user or pre-installed by Microsoft or the PC original equipment manufacturer ("**OEM**"). The user can easily uninstall applications by either (i) right-clicking on the application in the Start Menu and choosing the "uninstall" option in the context menu for the application (*see* **Figure 11**), or (ii) choosing the "uninstall" option in Windows Settings > Apps > Installed apps (on Windows 11) (*see* **Figure 12**) or Windows Settings > Apps > Apps & features (on Windows 10) (*see* **Figures 13-14**). When a user uninstalls an application, Windows will show one confirmation message before uninstalling it. Applications can separately customize their own uninstallation process and present a variety of different experiences to users. For example, when users uninstall Microsoft Edge, they are shown a message about any applications or experiences that depend on Edge, such as installed progressive web apps ("**PWAs**") and widgets, that will no longer function if Edge is uninstalled. The user is asked to confirm that they would like to uninstall Edge in order to continue the uninstall process.

258. Once an application has been uninstalled from Windows, to reinstall the application, the user must download the application from the developer's website, the Microsoft Store, or a third-party application store, or obtain the application on some physical media such as a USB drive. This is true for all applications, including those that were preinstalled on Windows.

Figure 11. Uninstalling An Application From The Start Menu

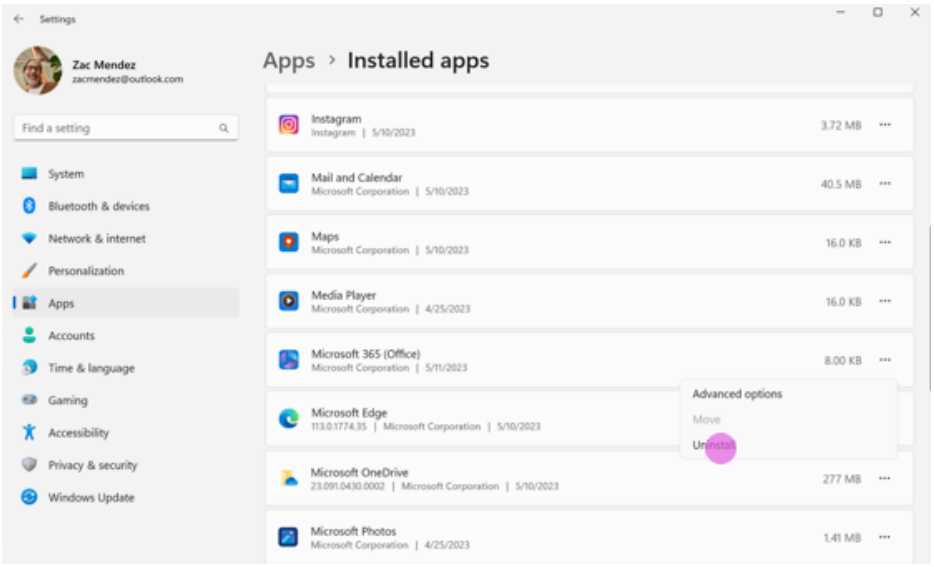


101 Windows is often also used by enterprises and enterprises have tools available to limit what end users can do. Where Windows is managed by an IT administrator that is not the end user, the administrator can control the policies for the installation and uninstallation of applications.



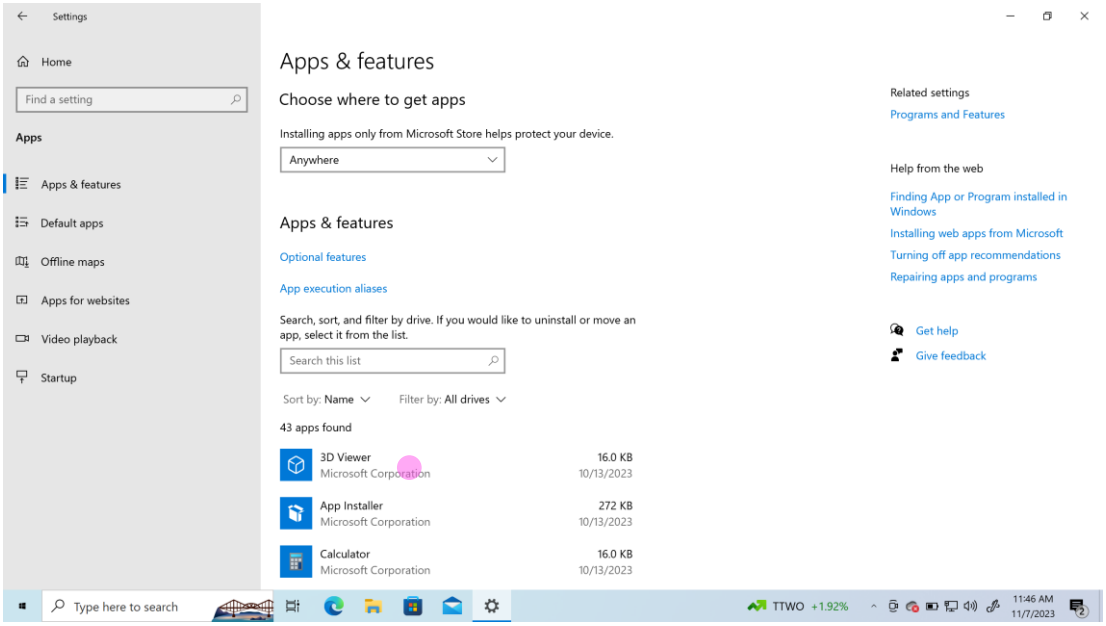
Source: Microsoft

Figure 12. Uninstalling An Application From The Installed Apps List In Settings On Windows 11



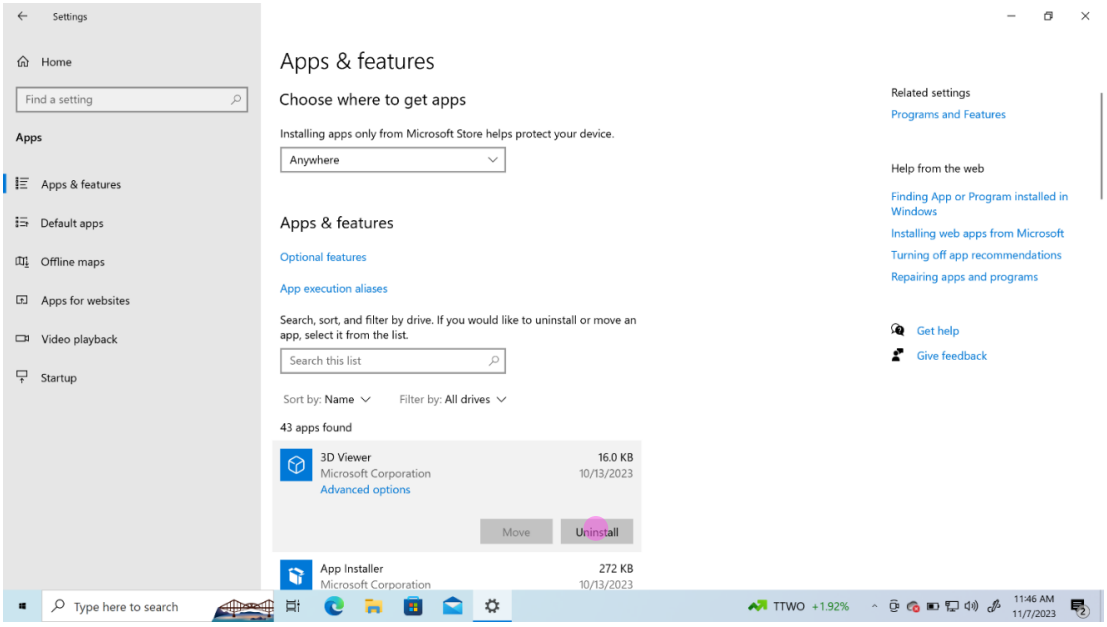
Source: Microsoft

Figure 13. Uninstalling An Application From The Apps & Features List In Settings On Windows 10



Source: Microsoft

Figure 14. Dialog To Uninstall An Application From The Apps & Features List In Settings On Windows 10

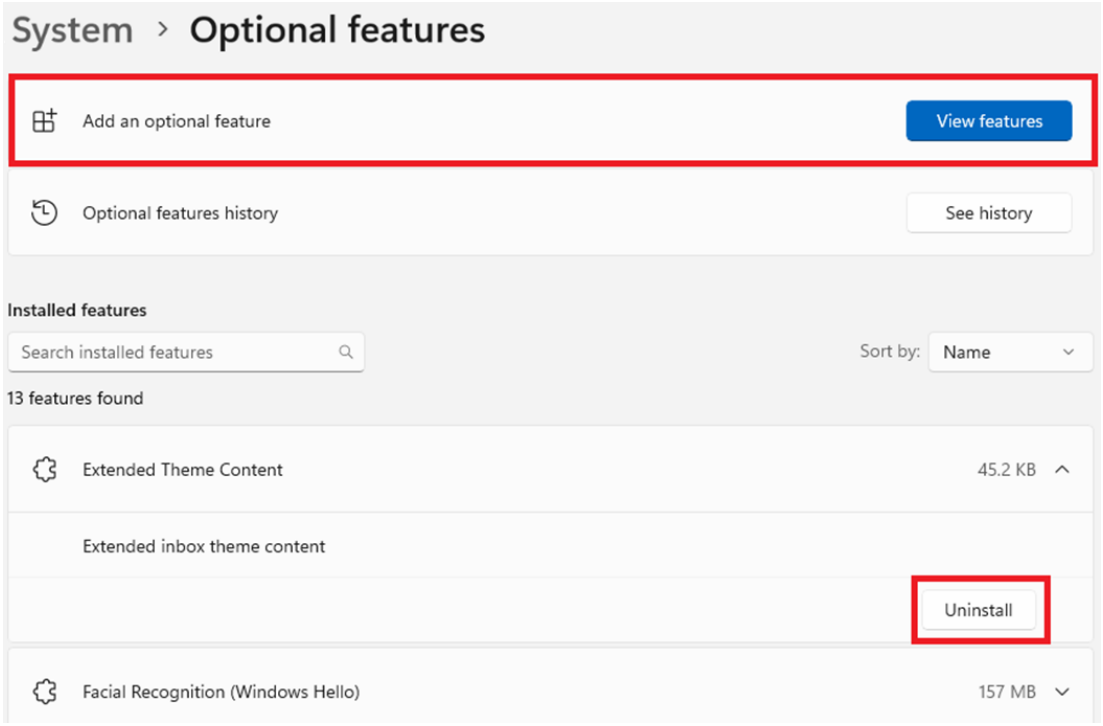


Source: Microsoft

259. In addition to applications that can be uninstalled through Start or Settings, there are a few legacy functions, designed as "Optional features," that remain in Windows, some of which may be considered as applications. This feature experience was created in the Windows 7 timeframe to enable the removal of code that was not often used but that was not associated with traditional uninstallable applications. Older system features,

some of which could be considered applications under the DMA definition,[102] were included in this experience, including legacy Internet Explorer and Windows Media Player. Internet Explorer has been deprecated, but Windows Media Player remains primarily for compatibility purposes. These legacy features on Windows have never been redesigned and although they have effectively been replaced by other functionality, they remain in Windows. All "Optional features," however, can also be easily uninstalled and reinstalled. Optional features can be uninstalled by the user by choosing the "uninstall" option in Windows Settings > System > Optional features (on Windows 11) (*see* **Figure 15**) or Windows Settings > System > Optional features (on Windows 10) (*see* **Figure 16**). These optional features can be reinstalled by the user choosing that option in Windows Settings > Apps > Optional features > Add an optional feature (on Windows 11) (*see* **Figure 15**) or Windows Settings > Apps > Apps & features > Optional features > Add a feature (on Windows 10) (*see* **Figure 16**).

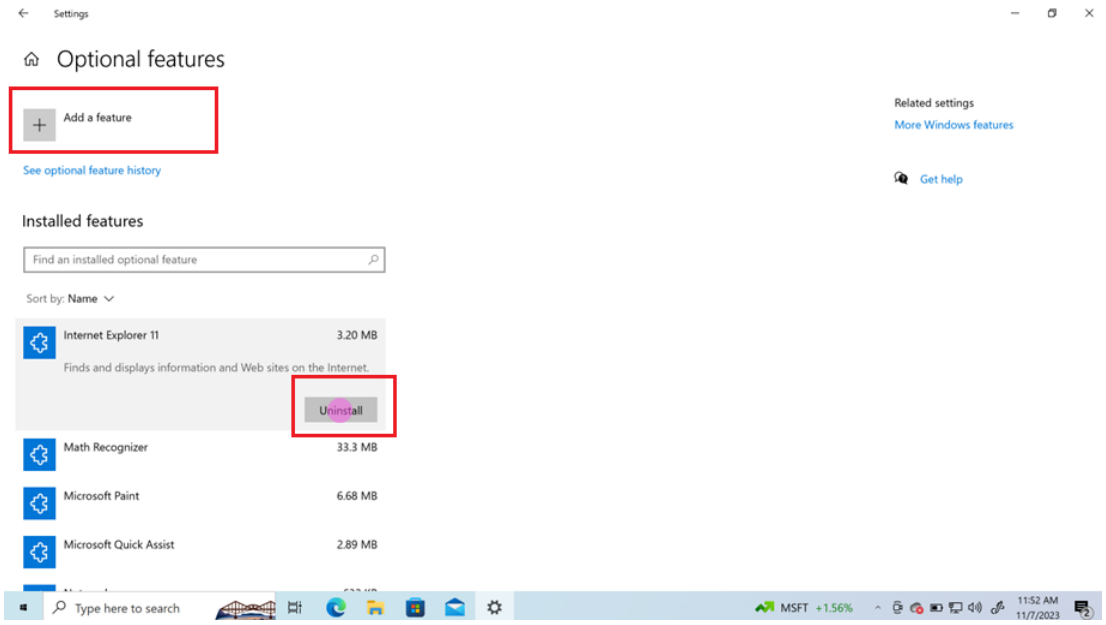
Figure 15. Uninstalling Or Reinstalling Optional Features On Windows 11



Source: Microsoft

[102] Article 2(15) of the DMA defines a software application as "*any digital product or service that runs on an operating system*."

Figure 16. Uninstalling Or Reinstalling Optional Features On Windows 10



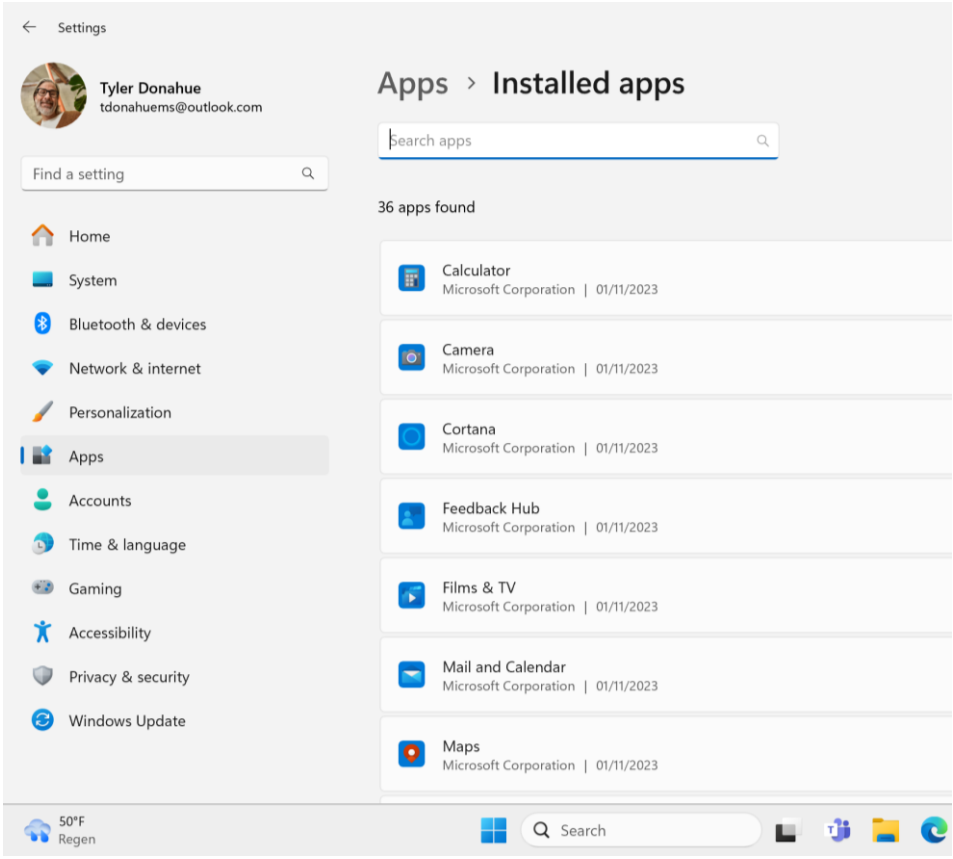
Source: Microsoft

260. Lastly, prior to the DMA, Microsoft already clearly delineated applications on Windows by listing them in the "All Apps" menu so users could access and launch them. This segmentation was not perfect, however, as the Windows "All Apps" menu also included some Windows system features that users may want to access directly and launch, such as Windows Settings or the Windows File Explorer. To comply with the DMA, Microsoft relabeled the "All Apps" menu as the "All" menu and clearly labeled the Windows system features in that menu with the word "System" to delineate applications versus OS functionalities. The following functionalities included in the "All" menu are part of the OS and are now clearly labeled "System:" Accessibility, Dev Home, File Explorer, Get Help and Tips, Get Started, Microsoft Store, Phone Link, Windows Backup, Windows Security, Windows Settings, and Windows Tools.

261. Microsoft reviewed the items on the "All" menu and ensured that all applications on it were uninstallable. Specifically, prior to the DMA, the following applications on the "All Apps" menu could not be uninstalled and to comply with the DMA, Microsoft made them uninstallable on a worldwide basis: Camera, Cortana, and Photos. In addition, Web Search from Microsoft Bing and Microsoft Edge were redesigned to become applications because the DMA characterizes web search and web browsing functionality as distinct from an OS. These are now applications that can also be uninstalled but only on PCs within the EEA.

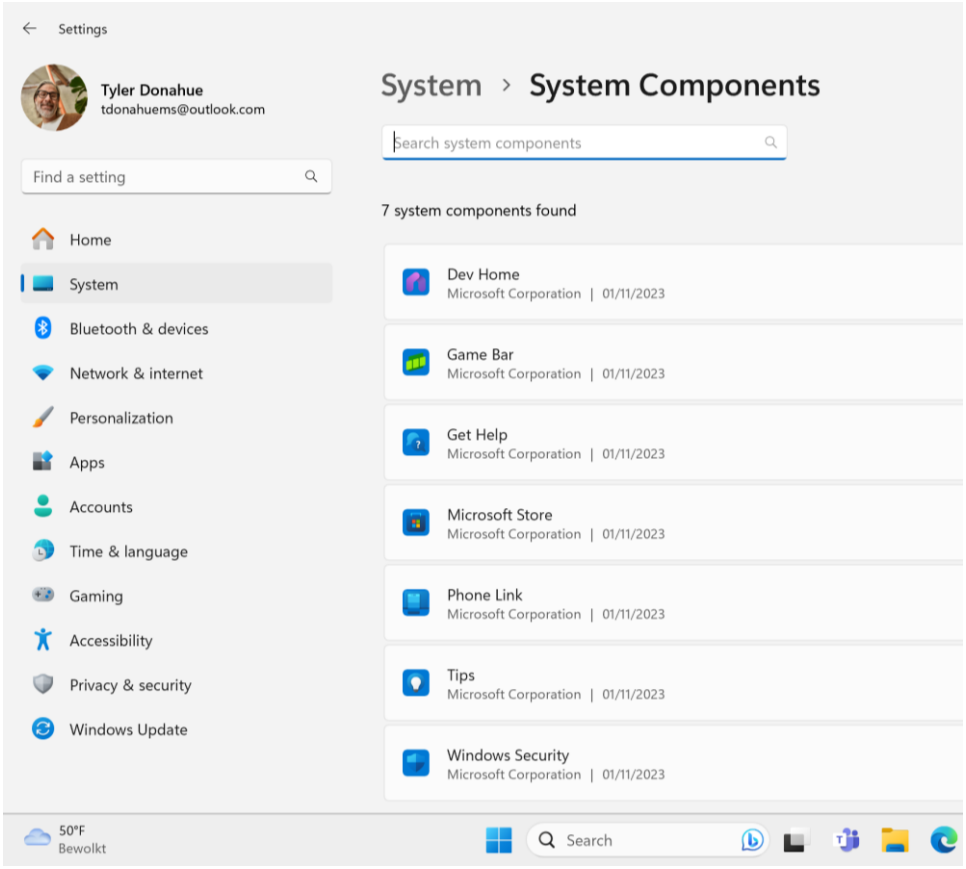
262. In addition to the "All" menu, users will be able to view the applications and features of the OS through Windows Settings. In Settings, users can navigate to Settings > Apps > Installed Apps to see a list of all installed applications (*see* **Figure 17**), and to Settings > System > System components to see a list of system components shown in Start (*see* **Figure 18**).

Figure 17. Settings List Of All Installed Applications



Source: Microsoft

Figure 18. Settings List Of Key System Components



Source: Microsoft

B. Users Can Easily Change Default Settings On Windows 10 And 11

263. Article 6(3) of the DMA includes the following obligation: "[t]*he gatekeeper shall allow and technically enable end users to easily change default settings on the operating system, virtual assistant and web browser of the gatekeeper that direct or steer end users to products or services provided by the gatekeeper. That includes prompting end users, at the moment of the end users' first use of an online search engine, virtual assistant or web browser of the gatekeeper listed in the designation decision pursuant to Article 3(9), to choose, from a list of the main available service providers, the online search engine, virtual assistant or web browser to which the operating system of the gatekeeper directs or steers users by default, and the online search engine to which the virtual assistant and the web browser of the gatekeeper directs or steers users by default*."

264. Microsoft describes below how users can easily change default settings, separately, on Windows 11 and 10. It also explains that for a Windows configuration called S mode where Microsoft Edge is the default web browser and Microsoft Bing is the default search engine, these settings cannot be changed while in S mode but users can easily switch out of S mode altogether, in compliance with Article 6(3) of the DMA. Microsoft has no online search engines, virtual assistants, or web browsers listed in the Designation Decision pursuant to Article 3(9) of the DMA. Therefore, the obligation to prompt end users, at the moment of the end users' first use of an online search engine, virtual assistant, or web browser does not apply to Windows.

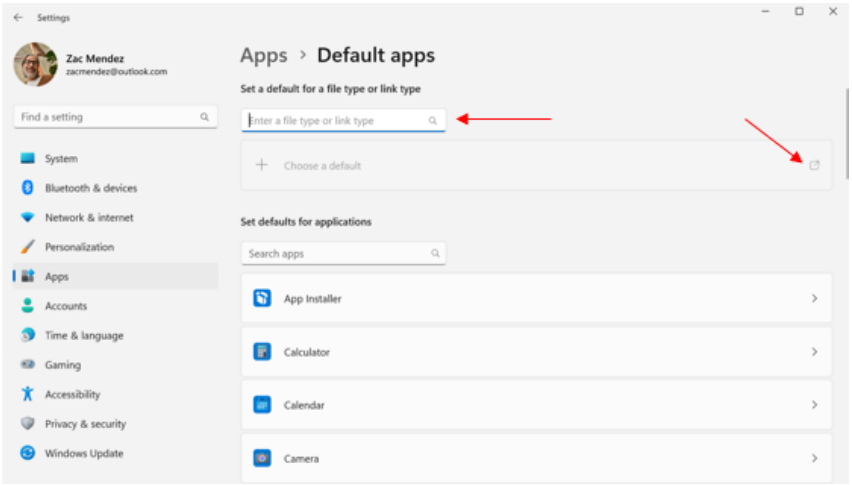
1. How Users Can Easily Change Default Settings On Windows 11

265. Windows has default settings for file types (*e.g.*, a .pdf file) and link types (*e.g.*, an http link) and they can be set and changed by the user at any time.[103] These settings identify the application or system component that will be opened by Windows to show the type of file or link when clicked on by the user. As detailed below in the section regarding Article 6(4), because of the DMA, dialogs that promoted Edge when a user changed their default browser have all been removed worldwide.

266. On Windows, default settings can be changed by (i) the application prompting users to set the application to be the default and (ii) the user changing default settings in Windows Settings. First, as discussed further in the section regarding compliance with Article 6(4) of the DMA, Windows makes it easier for users to change defaults after installing a new application. Windows automatically prompts the user with an "Open With" dialog to select a default application for a file or link type the first time that type is opened after a newly installed application registers support for that type. This allows the user to easily change default settings after installing a new application without the need to go to Settings. Second, the user can change default settings in Windows Settings (Settings > Apps > Default apps) in the following ways on Windows 11:

i. The user can set defaults by file or link type by using the search box at the top of the page. That search presents the user with the current default application for the file or link type (*see* **Figure 19**). By clicking the icon to the right of the default application, the user may access a list of installed applications that have registered for that file or link type and select their preferred default application (*see* **Figure 20**).

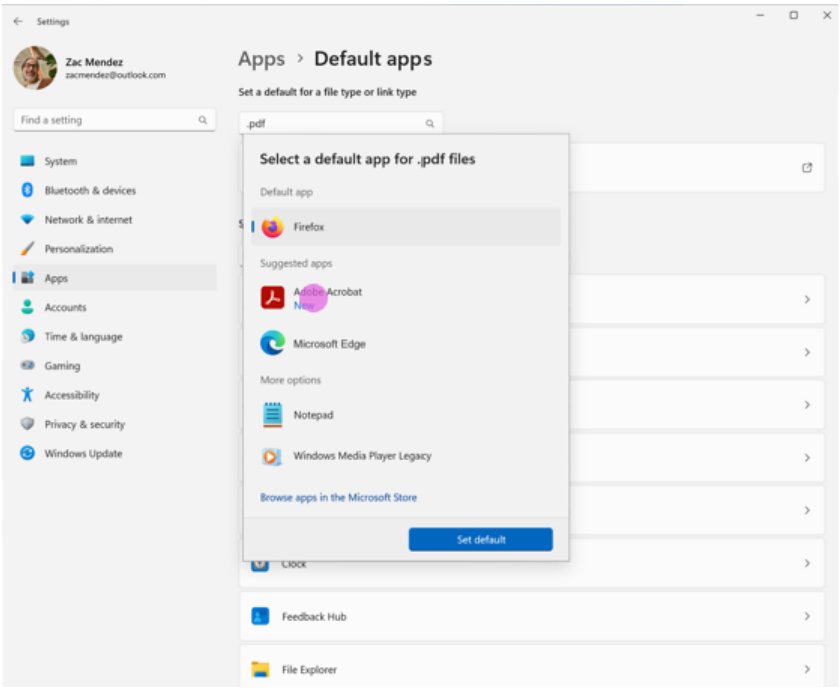
Figure 19. Setting Defaults By File Or Link Type Using The Search Box In The Default Apps Settings Page



Source: Microsoft

103 In an enterprise where Windows is managed by an administrator that is not the end user, the administrator can set default file and link types for applications.

Figure 20. Screenshot Of Dialog That Appears When A User Clicks The Icon Next To The Default Application

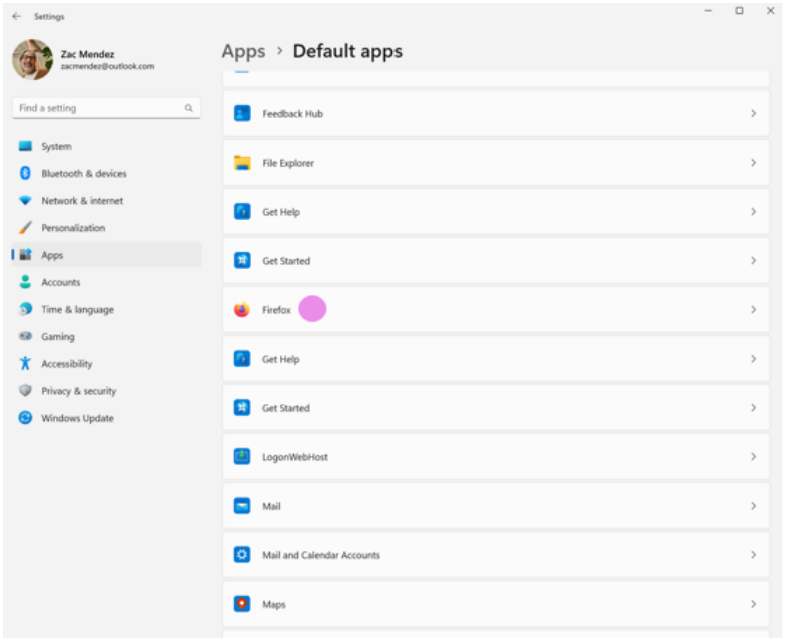


Source: Microsoft

ii. The user can also see the defaults that can be set by relevant application. Through the same page in Settings, the user may search for an application or scroll through a list of installed applications (*see* **Figure 21**) and, when an application is selected, the user sees all file and link types supported by that application and can configure the application as the default for handling the file and link types of the user's choice (*see* **Figure 22**). For applications that register for http or https, this experience contains a one-click "Set default" button at the top of the screen to change the default application for four link types that are commonly supported by browsers (http, https, .htm, and .html) (*see* **Figure 23**). Similarly, Windows has a documented API[104] that Microsoft and third-party applications can call that enables the application to open Windows Settings to the default applications page with the one-click "Set default" button for browser applications.

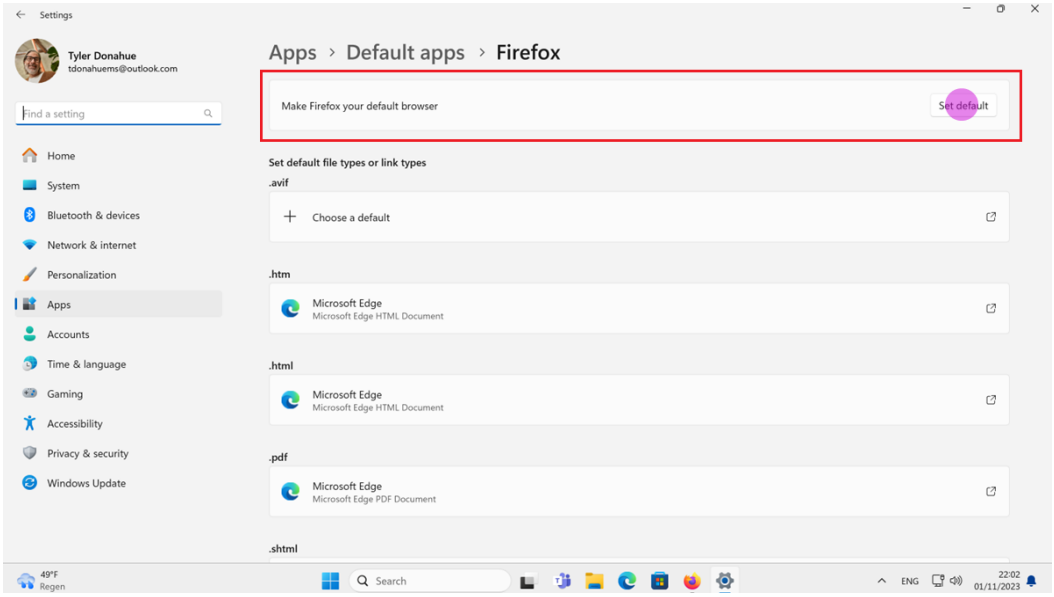
104 *See* https://learn.microsoft.com/en-us/windows/uwp/launch-resume/launch-default-apps-settings.

Figure 21. Screenshot Of Scrolling Through Installed Applications To Set A Default



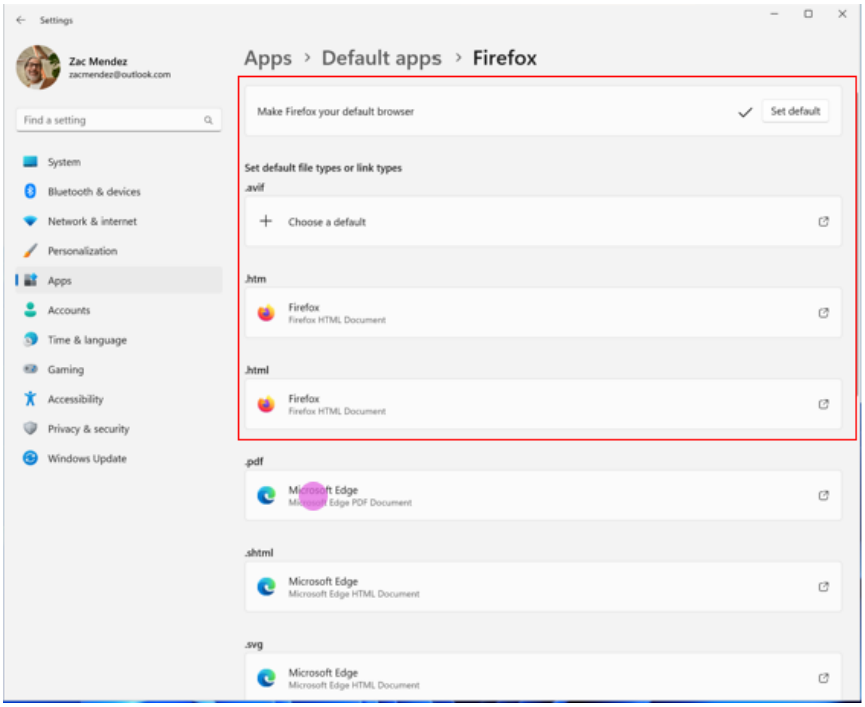
Source: Microsoft

Figure 22. Screenshot Of Link And File Types Associated With Default Application And The One-Click Button To Set A Browser As The Default Browser For Link Types http, https, .htm, and .html



Source: Microsoft

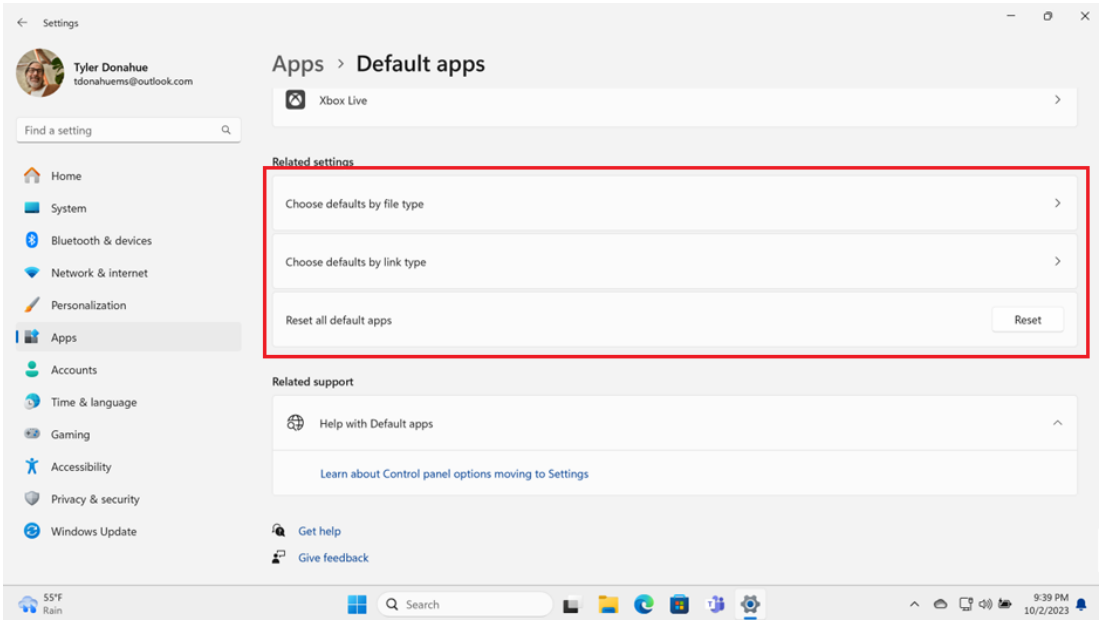
Figure 23. Screenshot Once Firefox (Or Any Browser) Is Set As The Default Browser For http, https, .htm, and .html Link Types



Source: Microsoft

iii. At the bottom of the same page in Settings, there are two additional options that allow the user to scroll through all registered file and link types and select defaults in that way (*see* **Figure 24**). For example, the user could navigate through those dialogs to find .pdf or .html and change the default handler for those settings. Users can also scroll through to see all the file and link types available on the system and what is set as the default for each.

Figure 24. Screenshot Of Settings Page To Choose Defaults By File Or Link Type



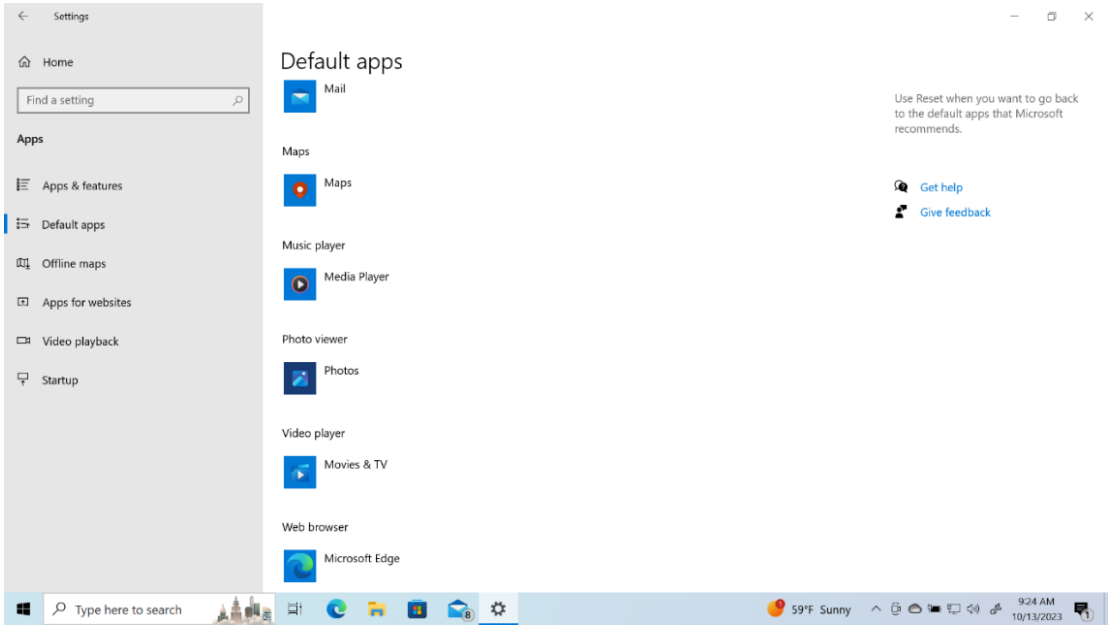
Source: Microsoft

2. How Users Can Easily Change Default Settings On Windows 10

267. On Windows 10, changing defaults is also easy. The user can change default settings by using the Windows Settings > Apps > Default apps page in the following ways:

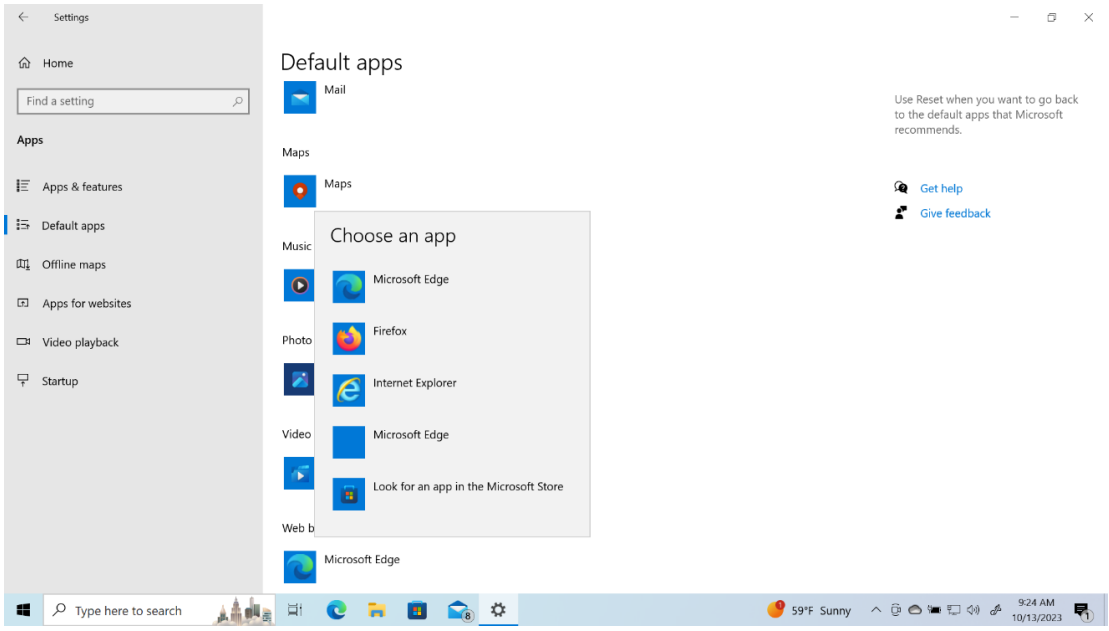
i. The user can choose a default application for the following predefined categories: Email (mailto link type), Maps (bingmaps link type), Music player (.mp3 file type), Photo viewer (.jpg, .jpeg, .png file types), Video player (.avi, .mp4 file types), and Web browser (http, https link types) (*see* **Figures 25-26**). Microsoft notes these categories have additional optional types that will also be set if the application registers for them. Changing the default for these application categories makes an application the default for a group of file types or links that are commonly associated with those types of applications.

Figure 25. Screenshot Of Default Apps Settings Page Showing Predefined App Categories



Source: Microsoft

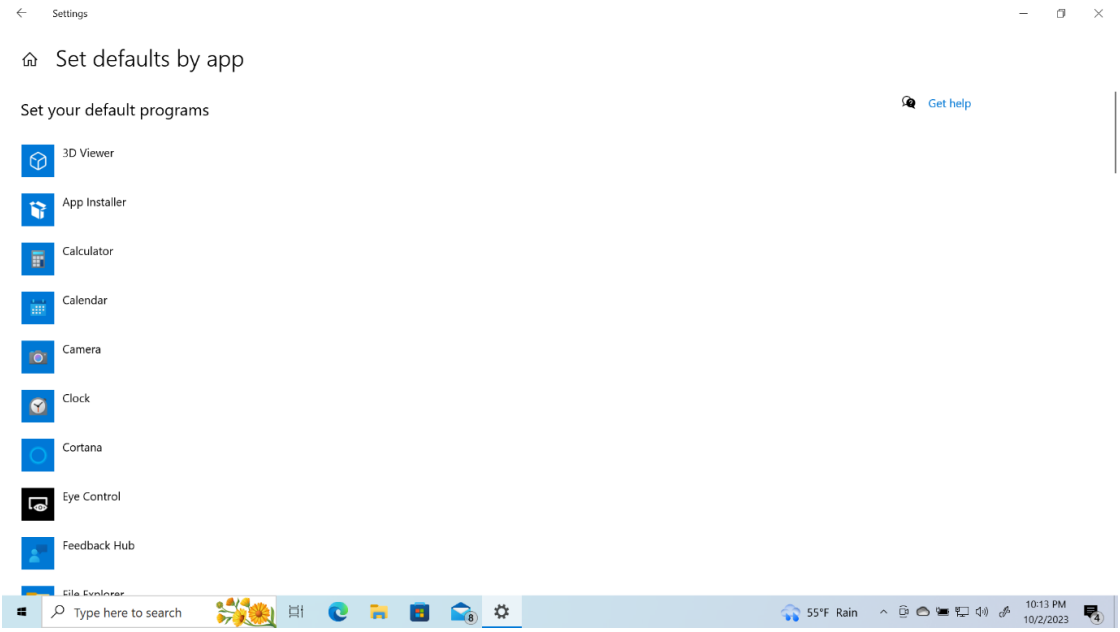
Figure 26. Screenshot Of Dialog To Choose An App After Clicking A Default Category



Source: Microsoft

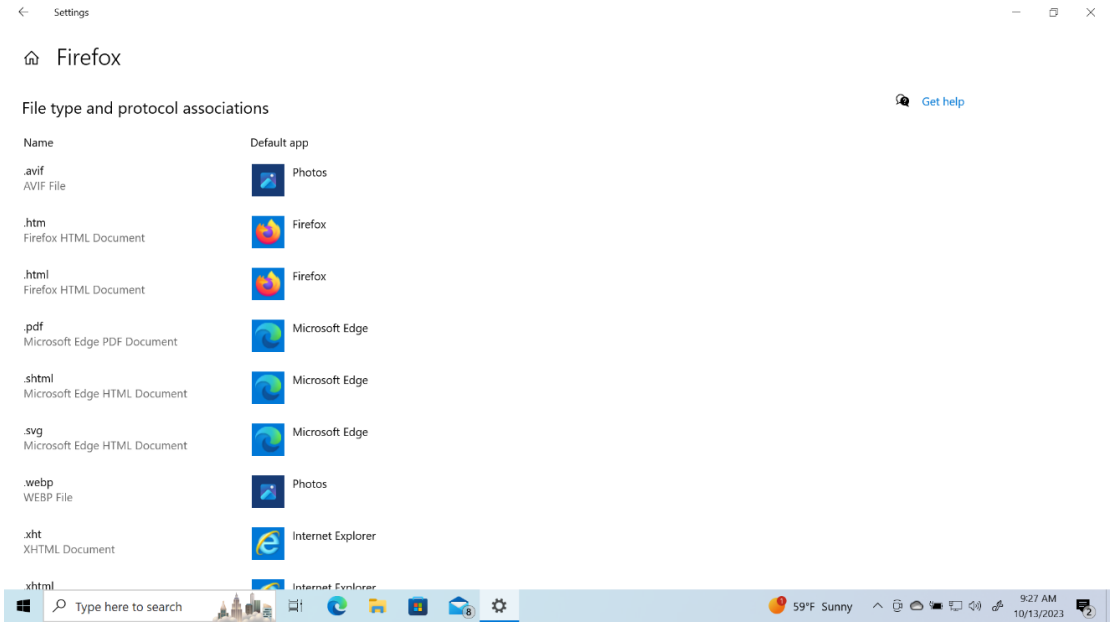
ii. The user can also set defaults by application. By selecting "Set defaults by app," the user may scroll through a list of installed applications (*see* **Figure 27**) and, when an application is selected, the user sees all file and protocol types (same as link type on Windows 11) supported by that application and can configure the application as the default for handling the file and link types they choose (*see* **Figures 28-29**).

Figure 27. List Of Installed Applications



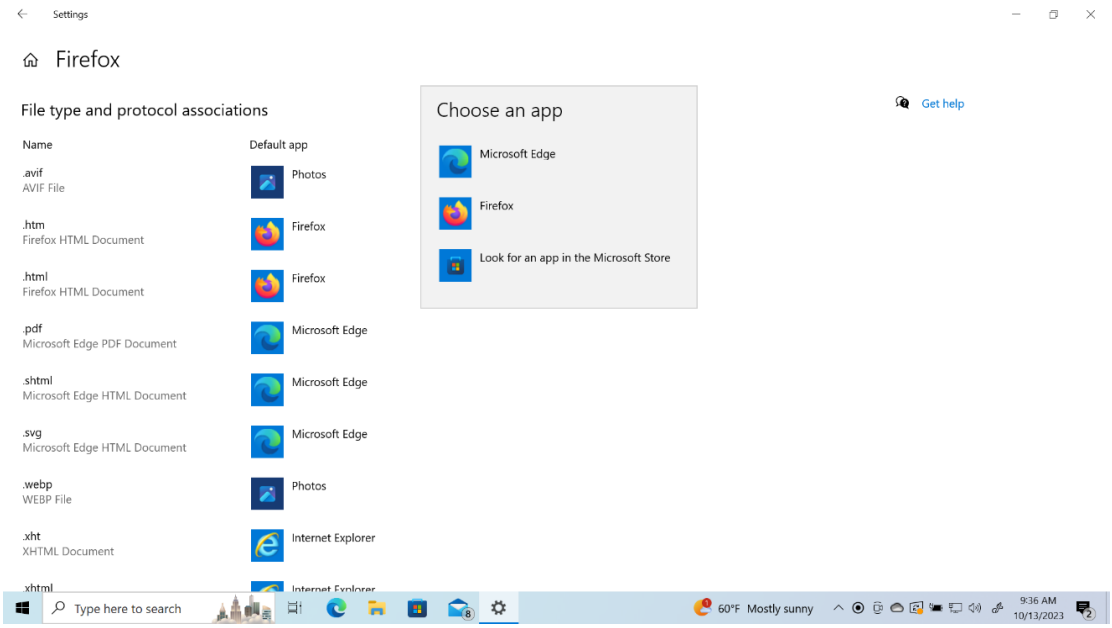
Source: Microsoft

Figure 28. Screenshot Of All File And Protocols Associated With The Firefox Application



Source: Microsoft

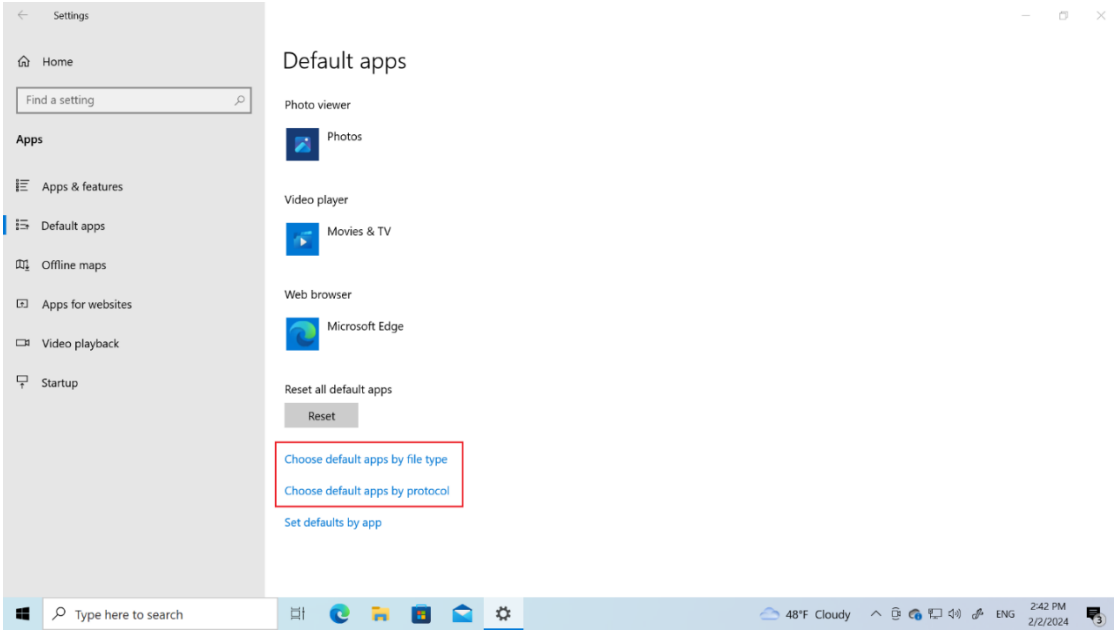
Figure 29. Screenshot Of The Dialog That Appears When A User Clicks On A Default Application To Change It



Source: Microsoft

iii. At the bottom of the same page in Settings, there are two additional options that allow the user to scroll through all registered file types and registered protocol types (same as link types on Windows 11) and select defaults in that way (*see* **Figure 30**).

Figure 30. Screenshot Of The Additional Options To Change Default Applications On The Settings Page



Source: Microsoft

3. Windows Uses The Default Application And Applications Can Use The Default Application Or A Different Application

268. As a result of the DMA, Microsoft has ensured that for both Windows 10 and 11, when a user clicks on a link or selects a file, Windows uses the default application to open that link or file. This is always the case for Windows devices in the EEA and mostly the case worldwide. Outside of the EEA, Windows uses Microsoft Edge, for example, to open links in help content or from the Spotlight feature on the lock screen.

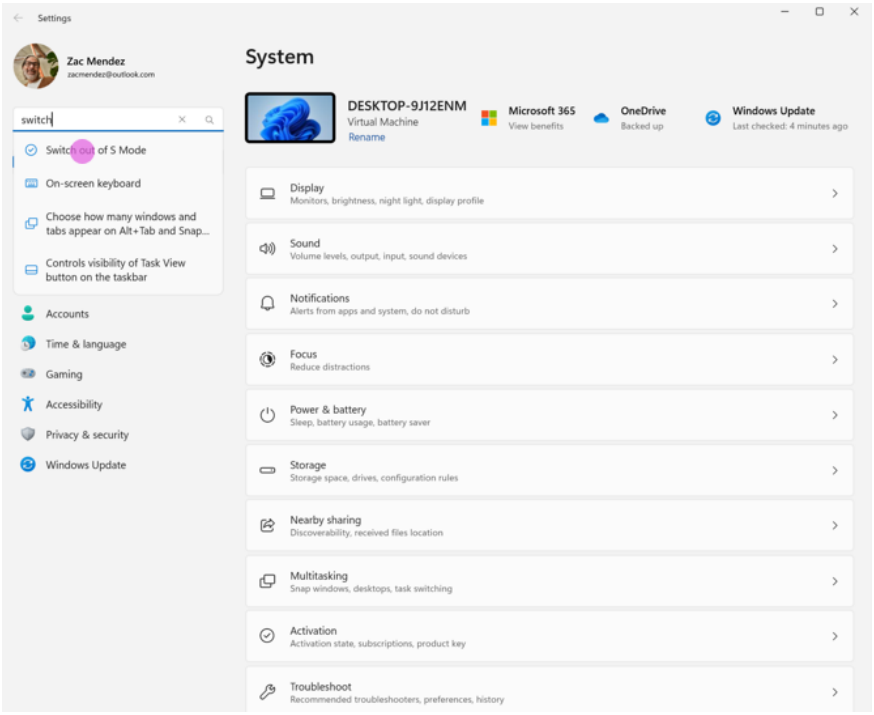
269. And as has always been the case, when the user clicks on a link or selects a file in a Microsoft or non-Microsoft application, the application may ask Windows to launch the application that has been set as the default, or it can launch a different application. Some applications are designed to use a specific application that is not the default application because it may provide the user with a more consistent end-to-end experience or enable the use of new features that are supported by the chosen specific application.

4. Users Can Easily Switch Out Of S Mode

270. Windows can be shipped in a configuration called S mode where Microsoft Edge is the default web browser and Microsoft Bing is the default search engine, and these settings cannot be changed. S mode is a configuration of Windows 10 and 11 designed to be more secure for novice users and more simple to use by limiting the applications that can be installed, or the way of installing applications, and limiting changes the user can make to the device. While in S mode, applications can be installed only from the Microsoft Store and some of the changes discussed above are not available. Users, however, can easily switch out of S mode altogether (*see* **Figures 31-35**), in compliance with Article 6(3) of the DMA.

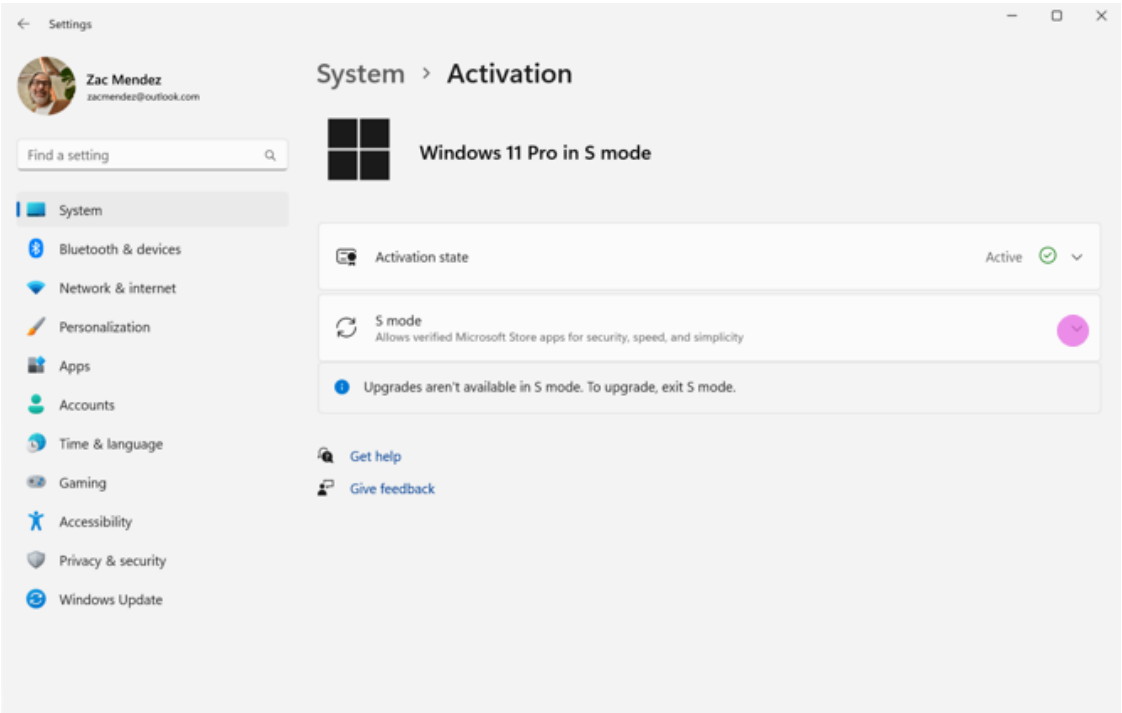
271. Once out of S mode, Windows 10 and 11 operate as normal, and notably, users can freely install applications outside of the Microsoft Store and configure defaults. Moreover, users cannot return to S mode. Once users are able to start downloading applications from the internet, the S mode restrictions cannot be reestablished. This is how S mode operated before the DMA was adopted and no changes were necessary to comply with the DMA.

Figure 31. Switching Out Of S Mode In Settings In The Search Bar On The Left, Type "Switch Out Of S Mode"



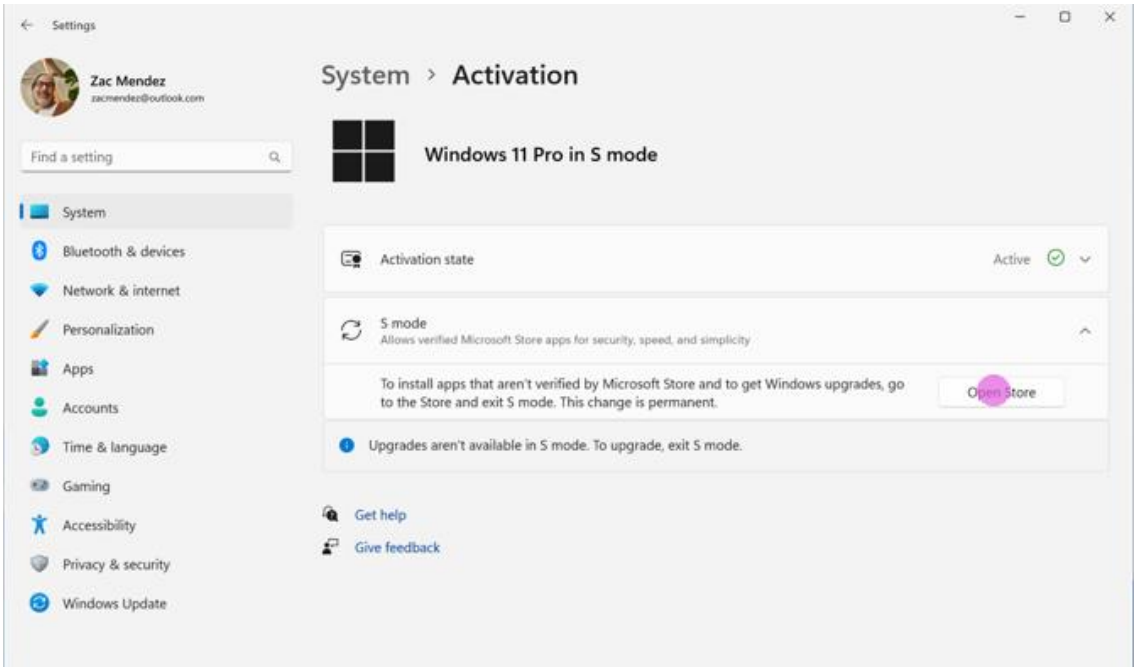
Source: Microsoft

Figure 32. Screenshot Of S Mode Page In Settings



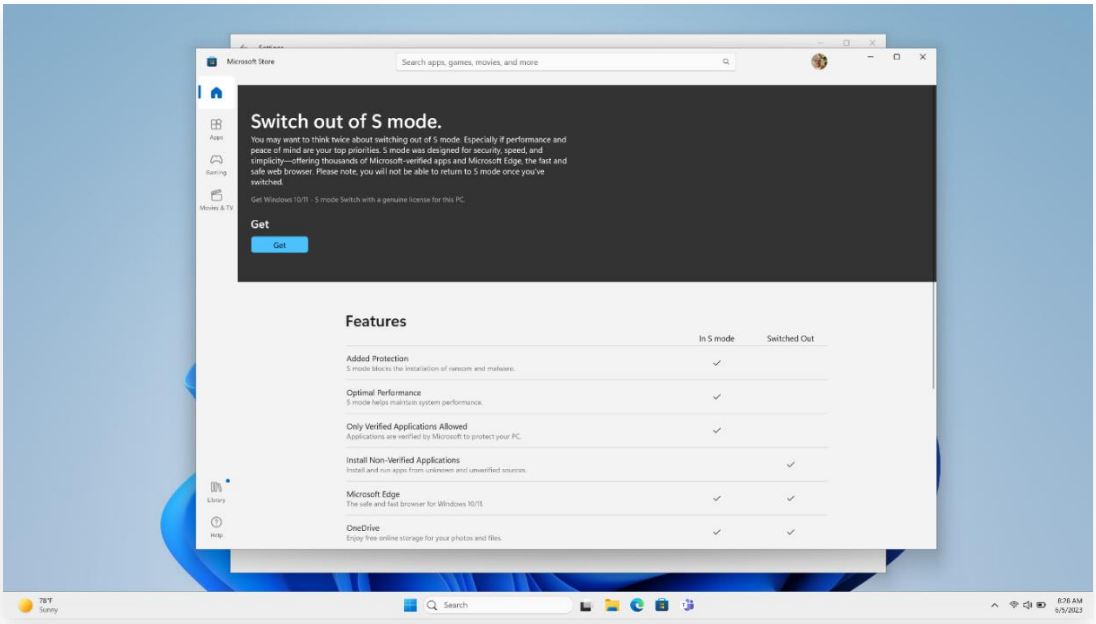
Source: Microsoft

Figure 33. Screenshot Of Page In Settings That Takes The User To The Microsoft Store To Switch Out Of S Mode



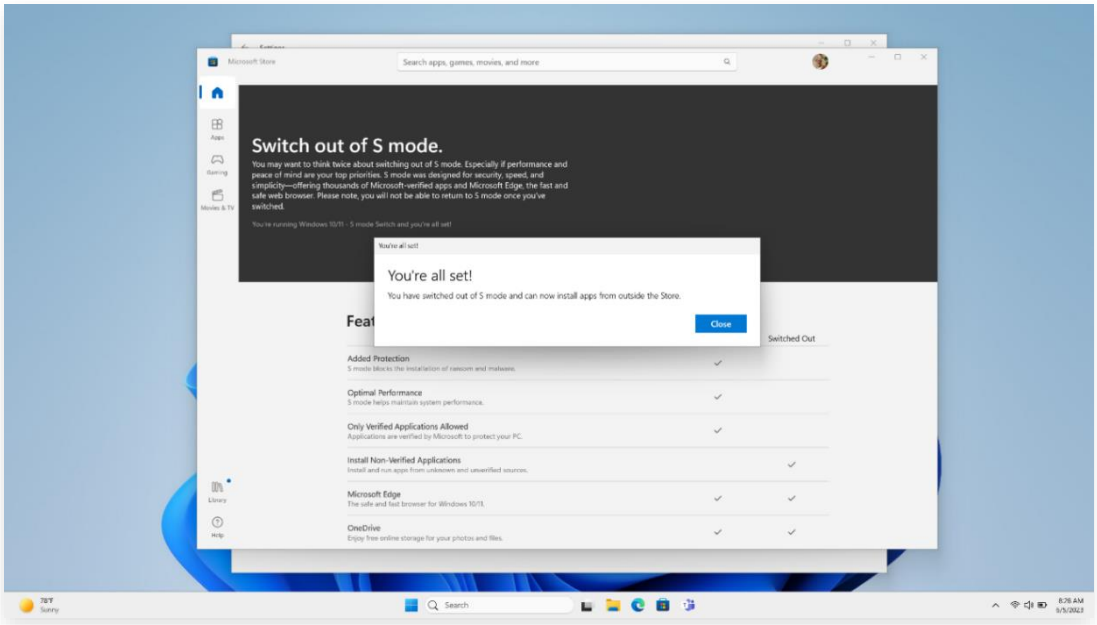
Source: Microsoft

Figure 34. Screenshot Of Microsoft Store Page To Switch Out Of S Mode



Source: Microsoft

Figure 35. Screenshot Of Verification That User Has Been Switched Out Of S Mode And Can Install Applications From Outside The Microsoft Store



Source: Microsoft

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[105]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

272. Microsoft refers to **Section 2.1.2 (i)** above.

b) when the measure was implemented;

273. Measures that were newly implemented for DMA compliance were implemented in Windows 10 22H2 build 19045.4123 (generally available on 29 February 2024) and Windows 11 23H2 build 22631.3235 (generally available on 29 February 2024). Microsoft also released through the Windows Insider Program ("**WIP**") Release Preview Channel for Windows 10 build 19045.3758 (generally available on 16 November 2023) and Windows 11 build 22631.2787(generally available on 16 November 2023). Any end user or business user of Windows can enroll in WIP (Settings > Windows Update > Windows Insider Program).[106]

c) the scope of the measure in terms of the products/services/devices covered;

274. Microsoft refers to the relevant versions of Windows defined in **Section 2.1** above.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

275. All applications that were made uninstallable are now uninstallable worldwide, with the exception of Microsoft Edge and Web Search from Microsoft Bing, which are applications and are uninstallable only in the EEA. The changes that ensure that all Windows system components use the default browser to open internet content were made available in the EEA. For the rest of the world, system components may use Microsoft Edge.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

276. Microsoft made required technical / engineering changes to Windows to meet the obligations of Article 6(3) of the DMA, as described above.

---

105 For example, this may be particularly relevant to illustrate changes impacting user journeys.

106 For details, *see* Windows Insider Program | Windows 10 - release information | Windows 11 – release information.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[107] consent forms,[108] warning messages, system updates, functionalities available, or customer journey to access functionalities[109]);

277. Microsoft refers to **Section 2.1.2 (i)** above. Microsoft made changes to the "All Apps" menu by relabeling it the "All" menu and clearly labeling Windows system features in the menu with "System" to delineate them from applications. Microsoft also removed dialogs promoting Microsoft Edge when users changed their default browser.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

278. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

279. None.

i) any consultation[110] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this

---

107 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

108 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

109 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

110 This information should include a description of the methodology for the consultation.

context and a high- level description of the topic of the consultation with those users/parties;

280. On 16 November 2023, Microsoft released a preview version of Windows 10 and 11 through the WIP (*see* above) and published a blog detailing the changes made to comply with the DMA so users and/or any interested parties could provide feedback.[111]

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

281. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

282. None.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

283. On 16 November 2023, Microsoft released a preview version of Windows 10 and 11 through the WIP (*see* above) and published a blog detailing the changes made to comply with the DMA so users and/or any interested parties could provide feedback.[112] Microsoft received feedback made publicly available by Mozilla and Vivaldi.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

284. To comply with Article 6(4) of the DMA, Microsoft has documented how third-party applications may prompt the user to set such applications as the default by linking to the location in Windows Settings where the user may set defaults by application, as described above.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are

---

111 *See* https://blogs.windows.com/windows-insider/2023/11/16/previewing-changes-in-windows-to-comply-with-the-digital-markets-act-in-the-european-economic-area/.

112 *See* https://blogs.windows.com/windows-insider/2023/11/16/previewing-changes-in-windows-to-comply-with-the-digital-markets-act-in-the-european-economic-area/.

strictly necessary and justified and there are no less restrictive means to achieve these goals;

285. Windows Security is an extension of the Settings component, focused on security settings and status including anti-virus protection, network firewalls, and data encryption. On Windows 10 and 11, Windows Security functionality cannot be uninstalled for security reasons, but its features may be controlled and configured by the user. Windows Security includes (i) Virus & threat protection (ii) Account protection; (iii) Firewall & network protection; (iv) App & browser control; (v) Device security; (vi) Device performance & health; (vii) Family options; and (viii) Protection history (Windows 11 only).

286. Virus & threat protection includes the Microsoft Defender Antivirus. If an alternative antivirus provider is installed, Microsoft Defender Antivirus will automatically be disabled. If the alternative antivirus is uninstalled, Microsoft Defender Antivirus will turn back on automatically.[113] Other features in Windows Security can be configured by the user through the (i) Windows Security controls, (ii) "Turn Windows features on or off' setting (Control Panel > Programs and Features > 'Turn Windows features on or off' on the left pane), and/or the (iii) Microsoft Edge Settings.

287. All applications and application stores on Windows are classified by Microsoft Defender and treated accordingly to protect the integrity of Windows. If a business user ships a malicious application, the user can be warned and/or the application could be blocked from running on Windows in order to protect the user.[114]

o) any type of market analysis or testing (in particular A/B testing[115]), business user surveys or consumer surveys or end user consent rates,[116] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[117]

288. Microsoft refers to **Section 2.1.2 (ii) (b)** above regarding the WIP.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or

---

113 For more information, *see* https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963.

114 *See* How Microsoft identifies malware and potentially unwanted applications.

115 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

116 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

117 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[118]

289. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

290. Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

r) any relevant data[119] **which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;**

291. As outlined in **Section 2.1.2 (ii) (q)** above, Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

292. Microsoft remains open to discussing any indicators and ways to monitor those indicators that would assist the Commission in its assessment of whether a particular measure is effective in achieving the objectives of the DMA, including metrics that

---

118 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

119 Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

track the choices made by users under mechanisms required by the DMA such as consent rates, installing and setting applications as the default, use of data portability mechanisms or others.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

293. Microsoft refers to **Section 2.1.2 (i)** above.

Regarding Article 6(4)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

294. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 6(4) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[120] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

295. Article 6(4) of the DMA provides:

"*The gatekeeper shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper. The gatekeeper shall, where applicable, not prevent the downloaded third-party software applications or software application stores from prompting end users to decide whether they want to set that downloaded software application or software application store as their default. The gatekeeper shall technically enable end users who decide to set that downloaded software application or software application store as their default to carry out that change easily.*

The gatekeeper shall not be prevented from taking, to the extent that they are strictly necessary and proportionate, measures to ensure that third-party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper, provided that such measures are duly justified by the gatekeeper.

Furthermore, the gatekeeper shall not be prevented from applying, to the extent that they are strictly necessary and proportionate, measures and settings other than default settings, enabling end users to effectively protect security in relation to third-party software applications or software application stores, provided that such

[120] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

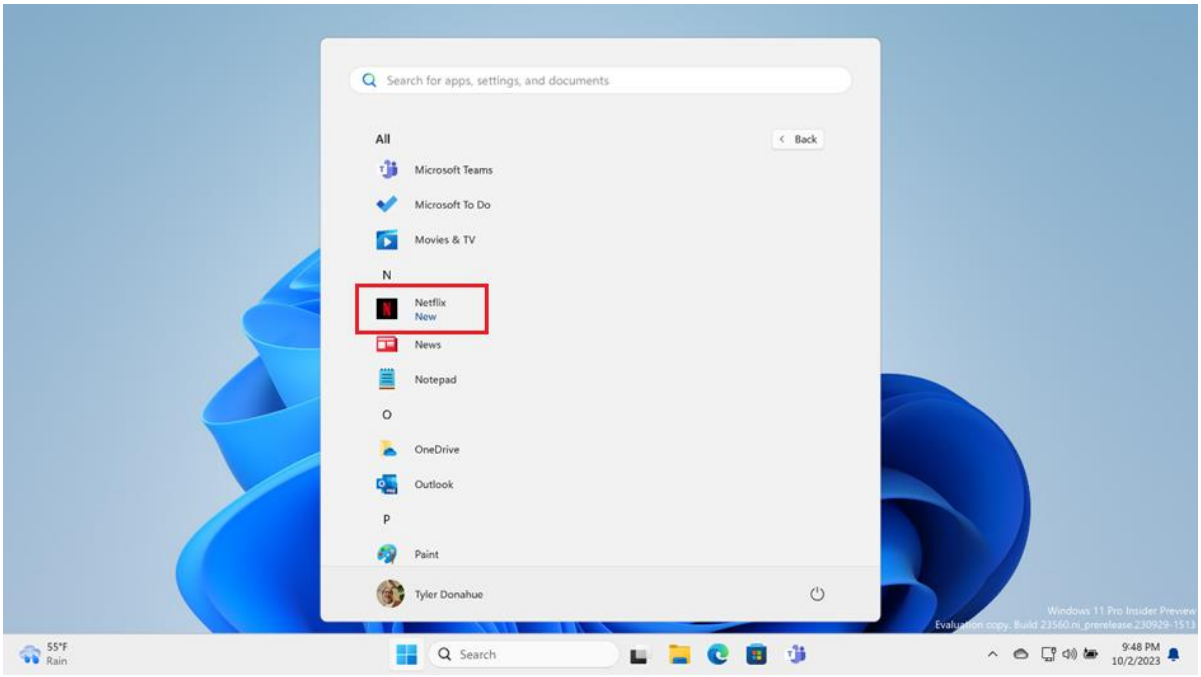
measures and settings other than default settings are duly justified by the gatekeeper."

296. Microsoft complies with Article 6(4) of the DMA, as applicable to Windows. Users can install and effectively use third-party applications and application stores on Windows (**Section A**) and third-party applications can prompt users to choose whether to set the application as the default (**Section B**). Windows has always allowed users to perform these functions. But, as a result of the DMA, Microsoft has also now removed dialogs promoting Microsoft products, as described below (**Section C**).

A. Users Can Install And Effectively Use Third-Party Applications And Application Stores On Windows

297. Windows has always been designed to be an open platform where users can freely install applications or application stores from the internet or from the Microsoft Store, and users can use those applications and stores on Windows.[121] No changes were required for DMA compliance. The Epic Games Store, for example, is available in the Microsoft Store and the internet. In addition to allowing users to freely install applications, Windows further assists users by helping them discover newly installed applications. Windows does this by putting a "New" label next to the application in the Start "All" menu, and "Recently added" in the "Recommended" section, and "New" label in the "Open With" dialog to set default applications (*see* **Figures 36-38**).

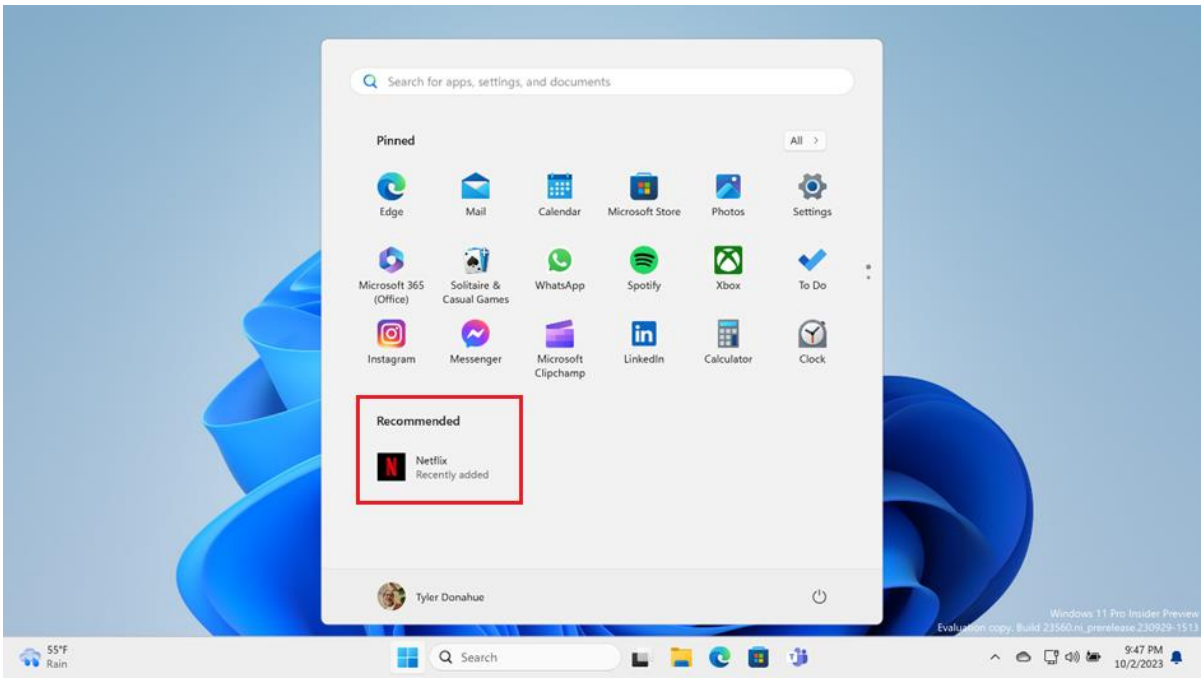
Figure 36. Netflix Application With "New" Label In The All Section Of Start



Source: Microsoft

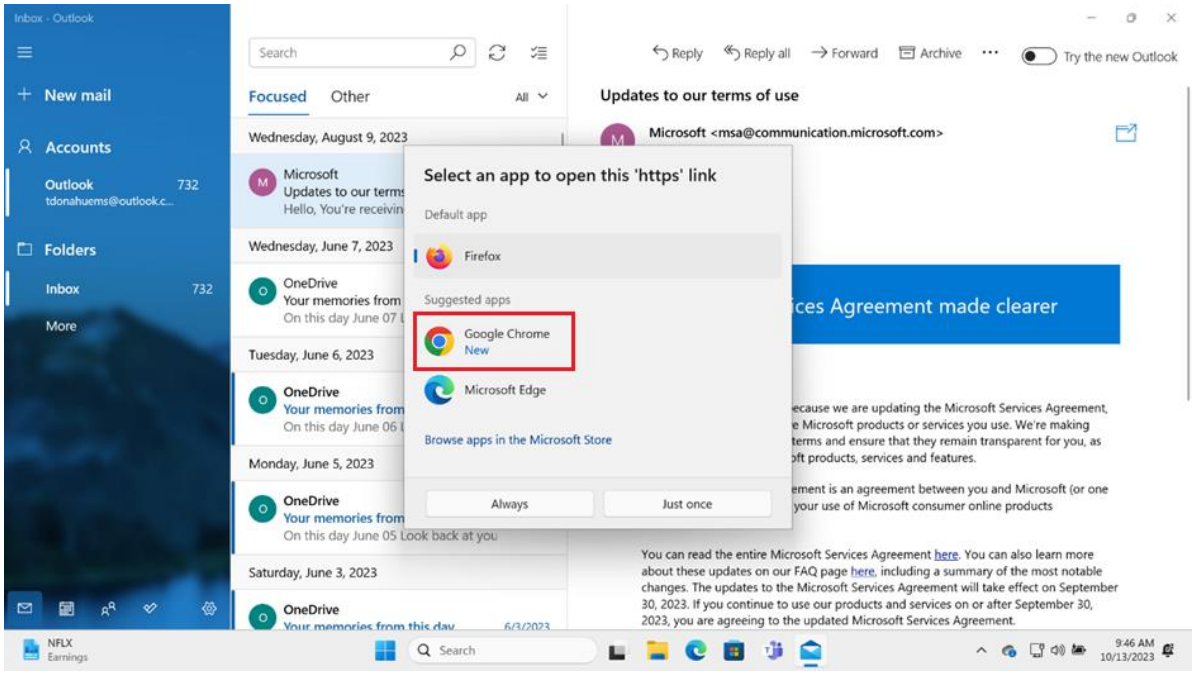
121 Microsoft will block malicious applications to protect the integrity of Windows. Microsoft publicly posts how it determines if an application is malicious; *see* https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/criteria?view=o365-worldwide.

Figure 37. Netflix Application With "Recently added" Label In Recommended Section In Start



Source: Microsoft

Figure 38. Google Chrome Application With "New" Label In "Open With" Dialog



Source: Microsoft

298. If an application developer elects to distribute an application through the Microsoft Store – which is completely optional – the Microsoft Store policies and terms apply.[122]

[122] *See* https://learn.microsoft.com/en-us/windows/apps/publish/store-policies-and-code-of-conduct.

The Microsoft Store terms allow for all manner of applications to be distributed through the Microsoft Store. The Microsoft Store also allows for the distribution of third-party application stores. Thus, the Microsoft Store policies and terms comply with Article 6(4) of the DMA.

299. In addition, as described in the compliance section for Article 6(3) of the DMA, Windows 10 and 11 are available in S mode, which is a pre-configured version of Windows where users cannot install applications outside of the Microsoft Store or change the default Microsoft Edge browser or the default Microsoft Bing search engine. It is designed to be more secure by limiting the applications that can be installed. S mode complies with Article 6(4) of the DMA because users can easily switch out of S mode altogether, and most users do. Once out of S mode, users cannot return to it because the pre-configured mode cannot be re-established once users start downloading applications from the internet. Further, once out of S mode, Windows 10 and 11 operate as explained above – notably, users can freely install applications outside of the Microsoft Store and configure defaults.

B. Applications On Windows May Prompt Users To Set The Application As The Default

300. Windows has a documented API that applications can call to prompt the user to set the application as the default for a file or link type.[123] This documented method enables an application to take the user directly to the Windows Settings default applications page where the user can easily carry out that change.[124]

301. In addition, Windows makes it easy for users to change defaults after installing a new application. Windows 10 and 11 automatically prompt the user to select a default application for a file or link type the first time that type is opened after a newly-installed application registers support for that type. This allows the user to easily change default settings after installing a new application without the need to go to Settings (*see* **Figures 39-40**).

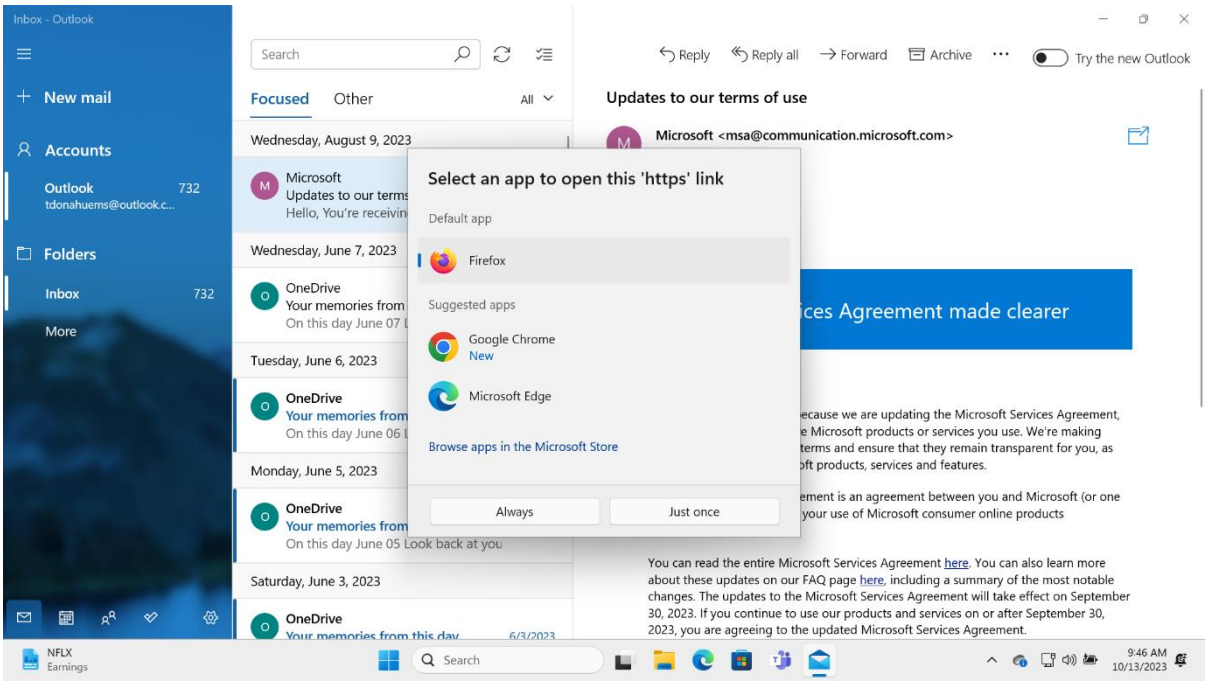
302. The "Open With" dialog lists the default application first under the "Default app" heading. Next, under "Suggested apps," it first lists all newly-installed applications alphabetically with a "New" label. An application is considered new if it has been installed since the last time the file or link type was opened. Any action by the user (except to dismiss the dialog) will reset new applications and they will no longer appear with the "New" label again in the "Open With" dialog. Following all newly-installed applications, all installed applications that have registered for the file or link type are listed alphabetically. The "Just once" option is provided for a user that only wants to use an application to open a file or link type once. And the "Always" option is provided for the user that wants to use the application as the default for a file or link type every time.

---

123 *See* https://learn.microsoft.com/en-us/windows/uwp/launch-resume/launch-default-apps-settings.

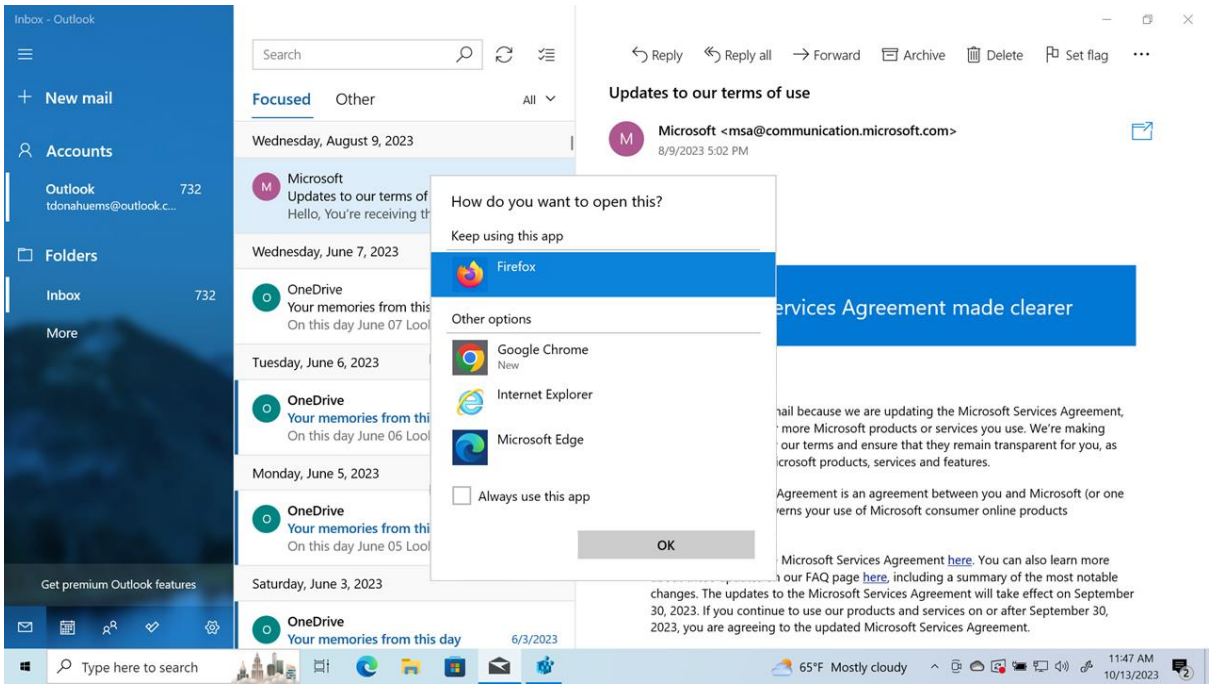
124 Microsoft notes there is no "default setting" for application stores as by its nature an application store needs to be launched by the user when wanting to find an application for installation.

Figure 39. Screenshots On Windows 11 Showing Open With Dialog After Installation Of A New Application That Registers For https File Type



Source: Microsoft

Figure 40. Screenshots Of Windows 10 Showing Open With Dialog After Installation Of A New Application That Registers For https File Type



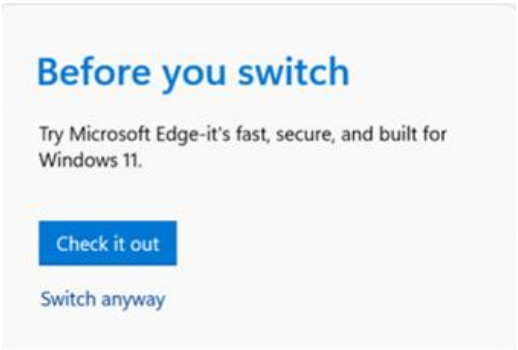
Source: Microsoft

C. Microsoft Removed Dialogs Promoting Microsoft Products

303. Because of the DMA, dialogs promoting Microsoft products have been eliminated from the experience described in the previous section. For example, dialogs promoting

Microsoft Edge have been removed from this experience when users want to switch browsers (*see* **Figures 41-43**). In Windows 10 and 11, Microsoft previously prompted users with a dialog promoting Microsoft Edge when the user clicked on a different browser to make it the default. Specifically, the user would see the dialog in **Figure 41** before changing browser defaults. This change was made worldwide.

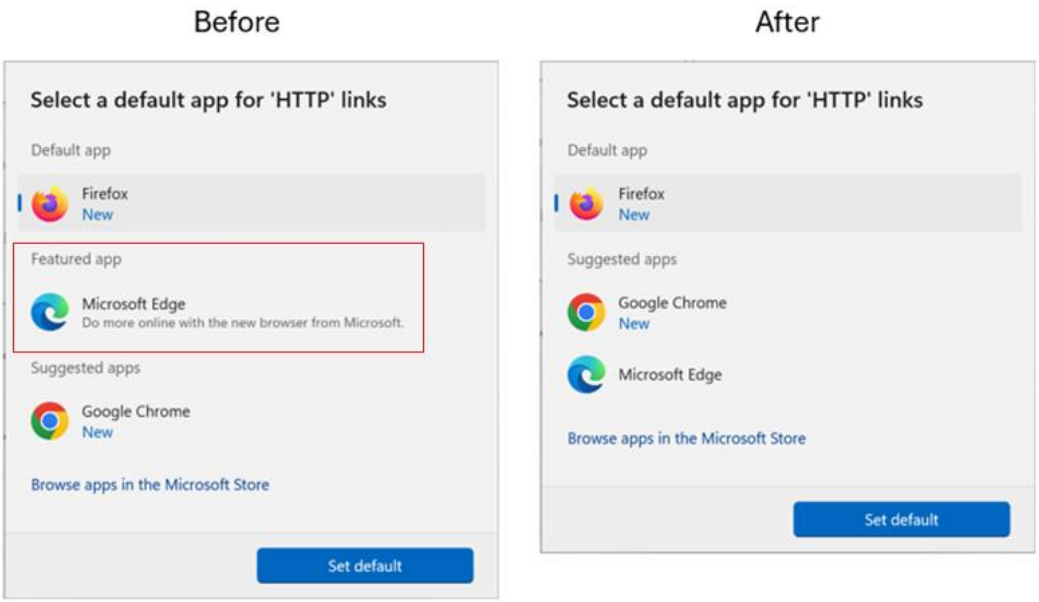
Figure 41. Screenshot Of Dialog Promoting Edge That Users Saw When They Wanted To Switch Browsers – This Is Now Removed



Source: Microsoft

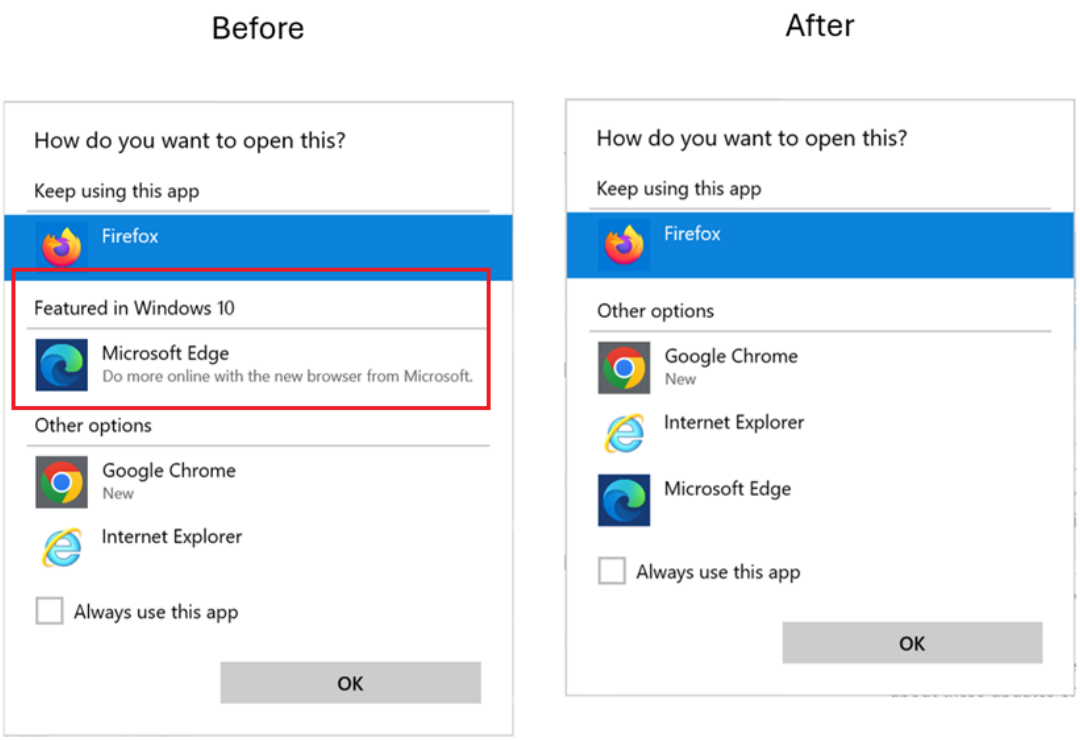
304. Similarly, the "Open With" dialog box previously had a "Featured app" section that listed Microsoft Edge, as shown in the image under "Before" in **Figure 42** and **Figure 43**. The "Featured app" heading with Microsoft Edge underneath has been removed because of the DMA and now looks like the image under "After." This change was made worldwide and was similarly made to eliminate showing any relevant Microsoft application as "featured" in the relevant default dialog screen.

Figure 42. Removal Of "Featured App" Heading Promoting Microsoft Edge In Open With Dialog In Windows 11



Source: Microsoft

Figure 43. Removal Of "Featured App" Heading Promoting Microsoft Edge In Open With Dialog In Windows 10



Source: Microsoft

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[125]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

305. Microsoft refers to **Section 2.1.2 (i)** above.

b) when the measure was implemented;

306. Measures that were newly implemented for DMA compliance were implemented in Windows 10 22H2 build 19045.4123 (generally available on 29 February 2024) and Windows 11 23H2 build 22631.3235 (generally available on 29 February 2024). Microsoft also released through the WIP Release Preview Channel for Windows 10 build 19045.3758 (generally available on 16 November 2023) and Windows 11 build 22631.2787(generally available on 16 November 2023). Any end user or business user of Windows can enroll in WIP (Settings > Windows Update > Windows Insider Program).[126]

125 For example, this may be particularly relevant to illustrate changes impacting user journeys.

126 For details, *see* Windows Insider Program | Windows 10 - release information | Windows 11 – release information.

c) the scope of the measure in terms of the products/services/devices covered;

307. Microsoft refers to the relevant versions of Windows defined in **Section 2.1** above.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

308. Microsoft refers to **Section 2.1.2 (i)** above.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

309. None.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[127] consent forms,[128] warning messages, system updates, functionalities available, or customer journey to access functionalities[129]);

310. Microsoft refers to **Section 2.1.2 (i) – Section C** above that describes the removal of the dialogs promoting Microsoft products worldwide.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

311. None.

---

127 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

128 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

129 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

312. None.

i) any consultation[130] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high- level description of the topic of the consultation with those users/parties;

313. On 16 November 2023, Microsoft released a preview version of Windows 10 and 11 through the WIP (*see* above) and published a blog detailing the changes made to comply with the DMA so users and/or any interested parties could provide feedback.[131]

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

314. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

315. None.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

316. On 16 November 2023, Microsoft released a preview version of Windows 10 and 11 through the WIP (*see* above) and published a blog detailing the changes made to comply with the DMA so users and/or any interested parties could provide feedback.[132] Microsoft received feedback made publicly available by Mozilla and Vivaldi.

---

130 This information should include a description of the methodology for the consultation.

131 *See* https://blogs.windows.com/windows-insider/2023/11/16/previewing-changes-in-windows-to-comply-with-the-digital-markets-act-in-the-european-economic-area/.

132 *See* https://blogs.windows.com/windows-insider/2023/11/16/previewing-changes-in-windows-to-comply-with-the-digital-markets-act-in-the-european-economic-area/.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

317. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

318. Microsoft provides solutions on Windows to protect customers from malicious applications, as do other third-party security providers. If a business user ships a malicious application the user can be warned and/or the application could be blocked from running on Windows in order to protect the user.[133]

o) any type of market analysis or testing (in particular A/B testing[134]), business user surveys or consumer surveys or end user consent rates,[135] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[136]

319. Microsoft refers to **Section 2.1.2 (ii) (b)** above regarding the WIP.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[137]

320. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of

---

133 For the publicly disclosed classification criteria, *see* https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/criteria?view=o365-worldwide.

134 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

135 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

136 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

137 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

321. Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

r) any relevant data[138] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

322. As outlined in **Section 2.1.2 (ii) (q)** above, Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

323. Microsoft remains open to discussing any indicators and ways to monitor those indicators that would assist the Commission in its assessment of whether a particular measure is effective in achieving the objectives of the DMA, including metrics that track the choices made by users under mechanisms required by the DMA such as consent rates, installing and setting applications as the default, use of data portability mechanisms or others.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be

[138] Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

independently audited, data access policies, data retention policies and measures to enable secure data access).

324. None.

Regarding Article 6(5)

325. Microsoft refers to **Section 2.3** below.

Regarding Article 6(6)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

326. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 6(6) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[139] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

327. Article 6(6) of the DMA provides: "*The gatekeeper shall not restrict technically or otherwise the ability of end users to switch between, and subscribe to, different software applications and services that are accessed using the core platform services of the gatekeeper, including as regards the choice of Internet access services for end users*."

328. Users on Windows can obtain or install applications from many sources. Applications for Windows can be easily obtained from the internet or the Microsoft Store, and some applications are pre-installed on the PC by Microsoft or the PC manufacturer. Windows users are free to open and close these applications and switch between them as they choose. Users are also free to choose any internet access service to connect Windows to the internet. This was true before the DMA was adopted, is the same wherever Windows is available, and no change was necessary to comply with the DMA.

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[140]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

329. None.

---

139 The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

140 For example, this may be particularly relevant to illustrate changes impacting user journeys.

b) when the measure was implemented;

330. None.

c) the scope of the measure in terms of the products/services/devices covered;

331. None.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

332. None.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

333. None.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[141] consent forms,[142] warning messages, system updates, functionalities available, or customer journey to access functionalities[143]);

334. None.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure

141 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

142 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

143 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

335. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

336. None.

i) any consultation[144] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high- level description of the topic of the consultation with those users/parties;

337. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

338. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

339. None.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

340. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

341. None.

144 This information should include a description of the methodology for the consultation.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

342. None.

o) any type of market analysis or testing (in particular A/B testing[145]), business user surveys or consumer surveys or end user consent rates,[146] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[147]

343. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[148]

344. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

345. None.

r) any relevant data[149] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform

---

145 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

146 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

147 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

148 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

149 Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

346. None.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

347. None.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

348. None.

Regarding Article 6(7)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

349. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 6(7) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[150] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

350. Article 6(7) of the DMA provides:

> "*The gatekeeper shall allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system or virtual assistant listed in the designation decision pursuant to Article 3(9) as are available to services or hardware provided by the gatekeeper. Furthermore, the gatekeeper shall allow business users and alternative providers of services provided together with, or in support of, core platform services, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features, regardless of whether those features are part of the operating system, as are available to, or used by, that gatekeeper when providing such services.*
>
> *The gatekeeper shall not be prevented from taking strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the operating system, virtual assistant, hardware or software features provided by the gatekeeper, provided that such measures are duly justified by the gatekeeper.*"

351. Microsoft complies with Article 6(7) of the DMA because Windows provides a robust set of publicly-documented APIs that can be called by Microsoft and third-party applications and which ensure effective interoperability with the hardware and software features controlled by Windows. Typically, Microsoft applications use the same

[150] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

publicly documented APIs to call into Windows as are available to third-party applications and, in all instances, Microsoft ensures that Microsoft and third-party applications can effectively access the hardware and software features controlled by Windows to enable third-party applications to provide the same functionality on Windows as Microsoft services and hardware do by leveraging the same Windows features.[151] This includes both access to underlying functionality as well as how users experience the applications, such as by how users can pin applications to the Windows Taskbar or set them as the default for a file or link type.

352. There are a handful of areas where Microsoft has created new extensibility for the purposes of the DMA as described below.

A. Microsoft And Third-Party Applications Use The Same Documented API To Ask Users To Pin An Application To The Taskbar And Start

353. All applications and application stores on Windows can be pinned or unpinned by the user to Start and the Taskbar by right-clicking the application or application store and making the desired selection in the context menu (*see* **Figures 44-45**). Similarly, to ensure effective interoperability on Windows, Microsoft provides a publicly-available API[152] that enables all applications and application stores on Windows to prompt users to pin to the Taskbar or Start (*see* **Figure 46**). Microsoft and third-party applications use this same API to serve this prompt to the user.[153] The publicly-available API to pin applications to Start and the Taskbar existed already prior to entry into force of the DMA and no changes were made because of the DMA. Whether pinned or not, an installed application will be available and accessible to the user in the "All" menu from the Start button.

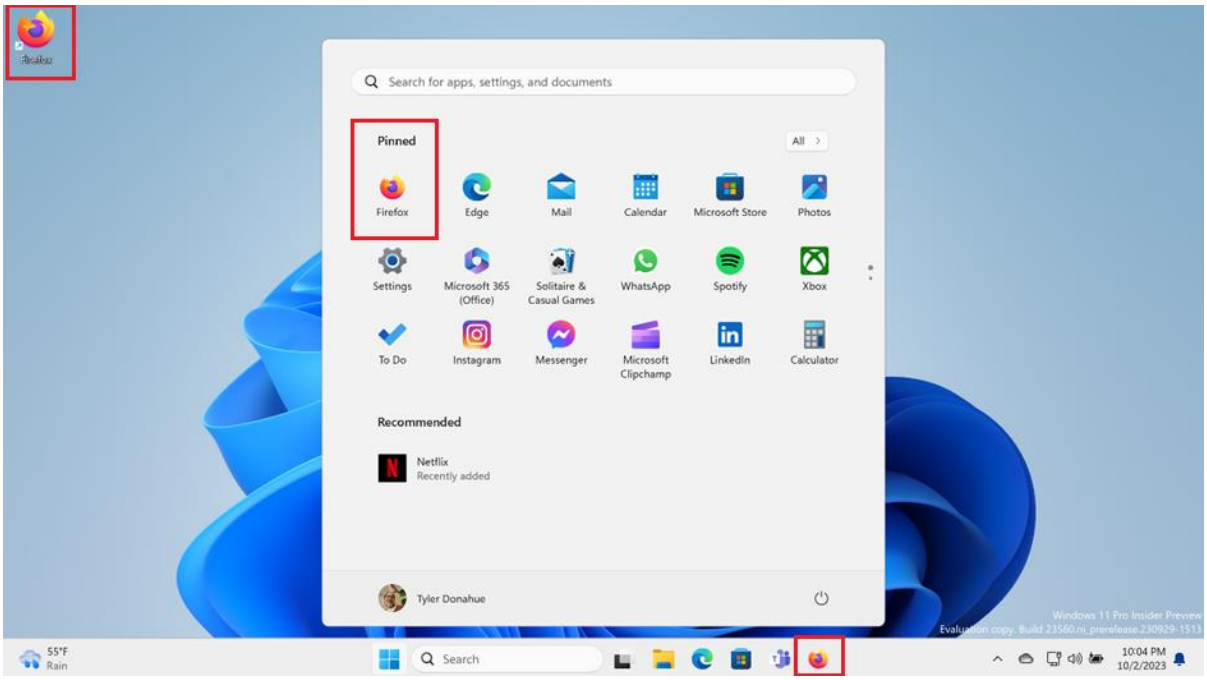
---

151 For completeness, Microsoft will block malicious applications from accessing the APIs that its products and services rely upon. Microsoft provides solutions on Windows to protect users and the integrity of the OS from malicious applications, as do other third-party security providers. If a business user ships a malicious application, the user can be warned and/or the application could be blocked from running on Windows in order to protect the user and Windows. For the criteria Microsoft uses to determine if an application is malicious, *see* https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/criteria?view=o365-worldwide.

152 *See* Pin your app to the Taskbar public API documentation.

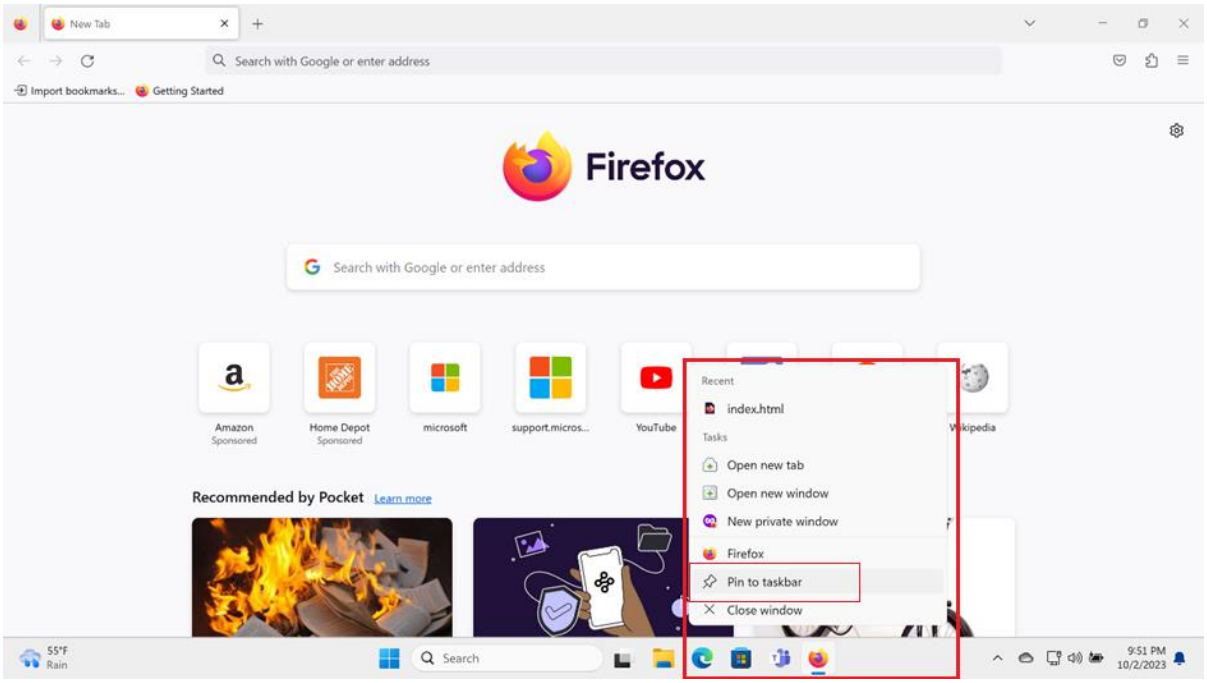
153 New Windows devices that are shipped by OEMs come with a set of preinstalled applications from Microsoft and the OEM and some of these applications are pre-pinned to the Taskbar. The user can unpin these applications at any time.

Figure 44. Screenshot Of Firefox With Desktop Shortcut, Pinned To Start, And Pinned To Taskbar



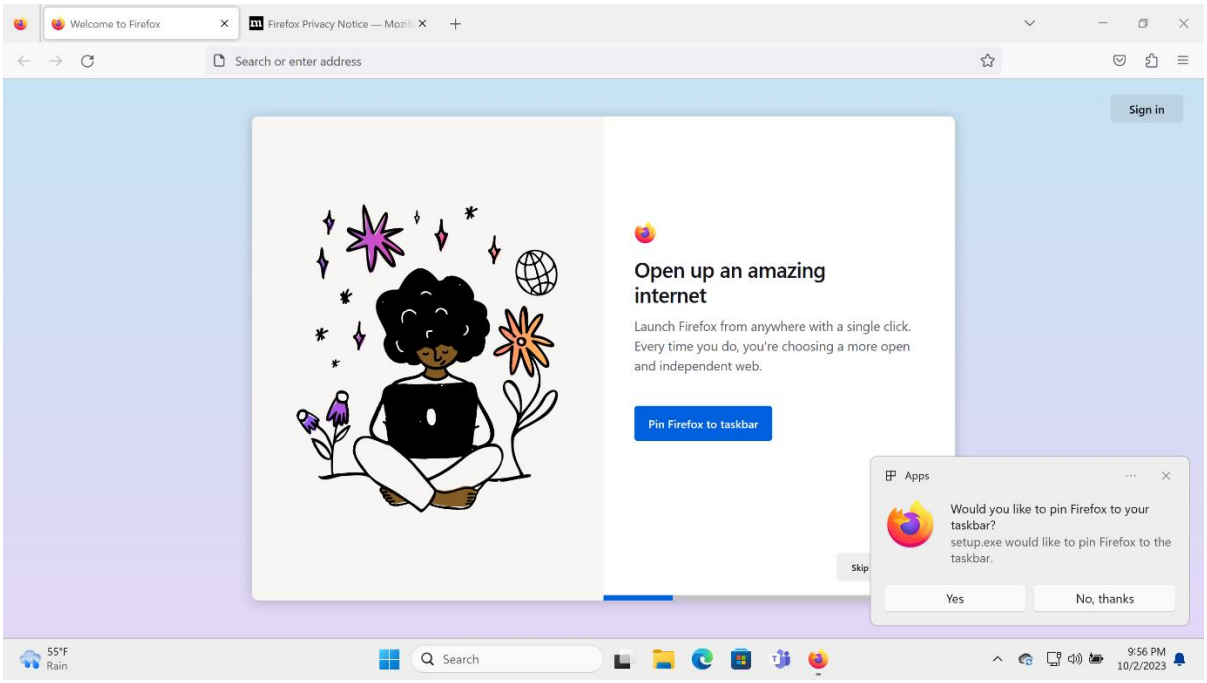
Source: Microsoft

Figure 45. Screenshot Of Firefox Context Menu In Taskbar With Pin Action



Source: Microsoft

Figure 46. Screenshot Of Firefox Using Programmatic Pinning API



Source: Microsoft

B. Microsoft And Third-Party Applications Use The Same Documented API To Ask The User To Set The Application As The Default

354. Windows has a documented API that Microsoft and third-party applications can call whenever the application is running to prompt the user to set the application as the default for a file or link type.[154] This documented method enables the application to open Windows Settings to the default applications page for their application where the user can easily carry out that change. Prior to the DMA compliance deadline, Microsoft Edge relied upon a slightly different mechanism to set itself as the default on Windows PCs, but it no longer does so in the EEA.

C. Third-Party Applications Can Be Accessed Through The Windows User Interface In The Same Way As Comparable Microsoft Applications

355. Most commonly, Microsoft and third-party applications present experiences to users in the exact same way by the user launching the application that opens a window, which hosts the user experience of the application. That experience within the application is controlled by the application developer and is their design decision. In a few instances, parts of the Windows user interface also provide more unique extensibility points for certain types of applications. For Windows, these extensibility points are available to Microsoft and third-party applications equally. To access these unique surface areas, applications need to be properly manifested applications packaged for the Microsoft Store. Those places are File Explorer, Windows Search, and the Widgets Board, and

154 *See* https://learn.microsoft.com/en-us/windows/uwp/launch-resume/launch-default-apps-settings.

they are described in detail below.[155] A packaged application is packaged using MSIX technology[156] and contains a manifest[157] that declares the package identity and system capabilities the application can request permission to use.

D. Windows File Explorer

356. Windows 10 and 11 enable both Microsoft and third-party applications to extend Windows File Explorer. All types of applications can use public APIs to extend File Explorer in many ways: for example, to add folder locations in the navigation pane and/or add entries to the context menu of files. Only properly-manifested applications packaged for the Microsoft Store, however, can implement a cloud file provider with additional points of integration in Windows File Explorer that, for example, can show an icon next to a file indicating its status (*see* **Figure 47**).[158]

357. Microsoft OneDrive is a preinstalled properly-manifested packaged application for the Microsoft Store on Windows that adds folder locations in the navigation pane, adds entries in File Explorer context menus, and implements a cloud file provider using public APIs and is enabled to appear in Windows File Explorer. The extensibility of Windows File Explorer existed prior to the DMA and is available wherever Windows is offered.

---

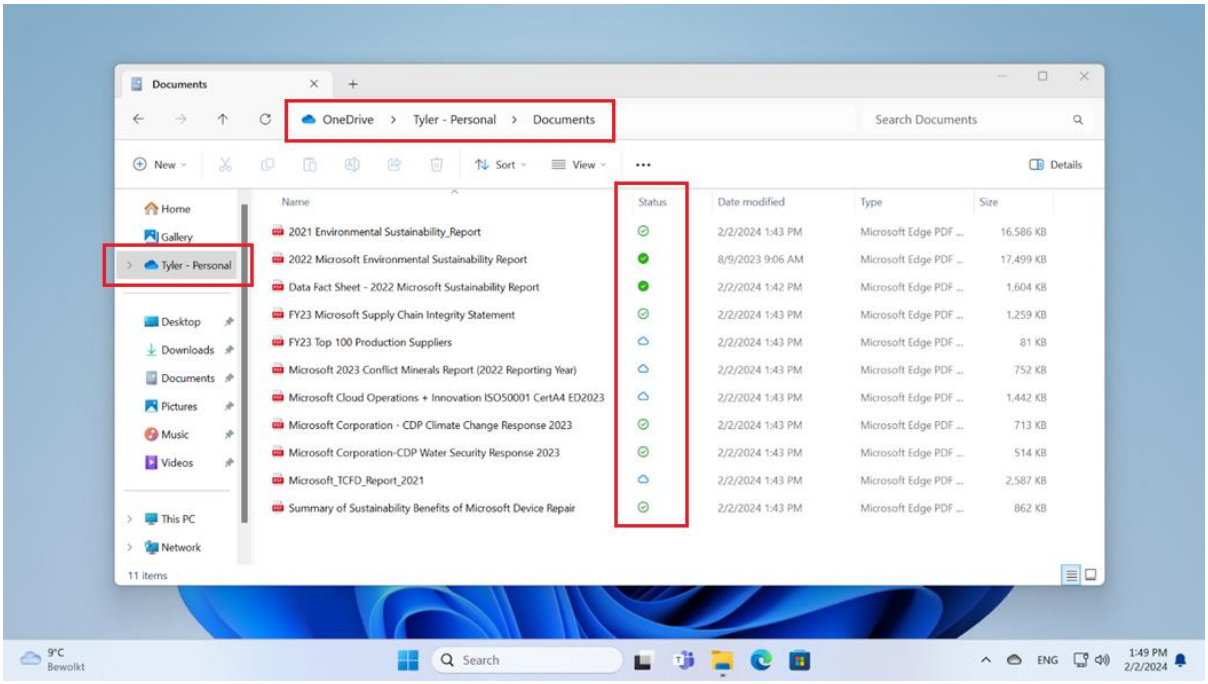
155 If an application chooses to use the Microsoft Store as a means to distribute its software, so that it may show itself in Windows in these unique extensibility points, or for another reason, it must comply with the Microsoft Store policies. *See* https://learn.microsoft.com/en-us/windows/apps/publish/store-policies.

156 *See* https://learn.microsoft.com/en-us/windows/msix/overview.

157 *See* https://learn.microsoft.com/en-us/uwp/schemas/appxpackage/appx-package-manifest.

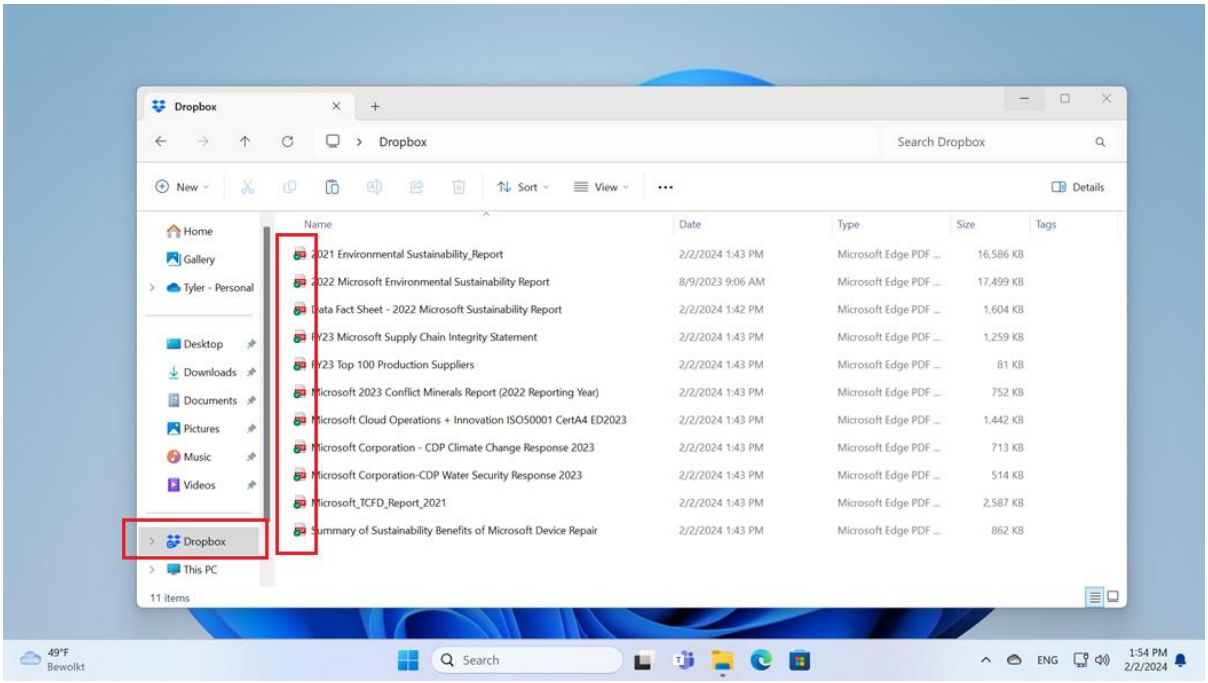
158 *See* Build a Cloud Sync Engine that Supports Placeholder Files public API documentation.

Figure 47. Screenshot Of Experience With OneDrive (Implements A Cloud File Provider) (Note: Status Icons)



Source: Microsoft

Figure 48. Screenshot Of Experience With Dropbox (Does Not Use the Cloud File Sync Engine And Implements Its Own Sync Icon Design)



Source: Microsoft

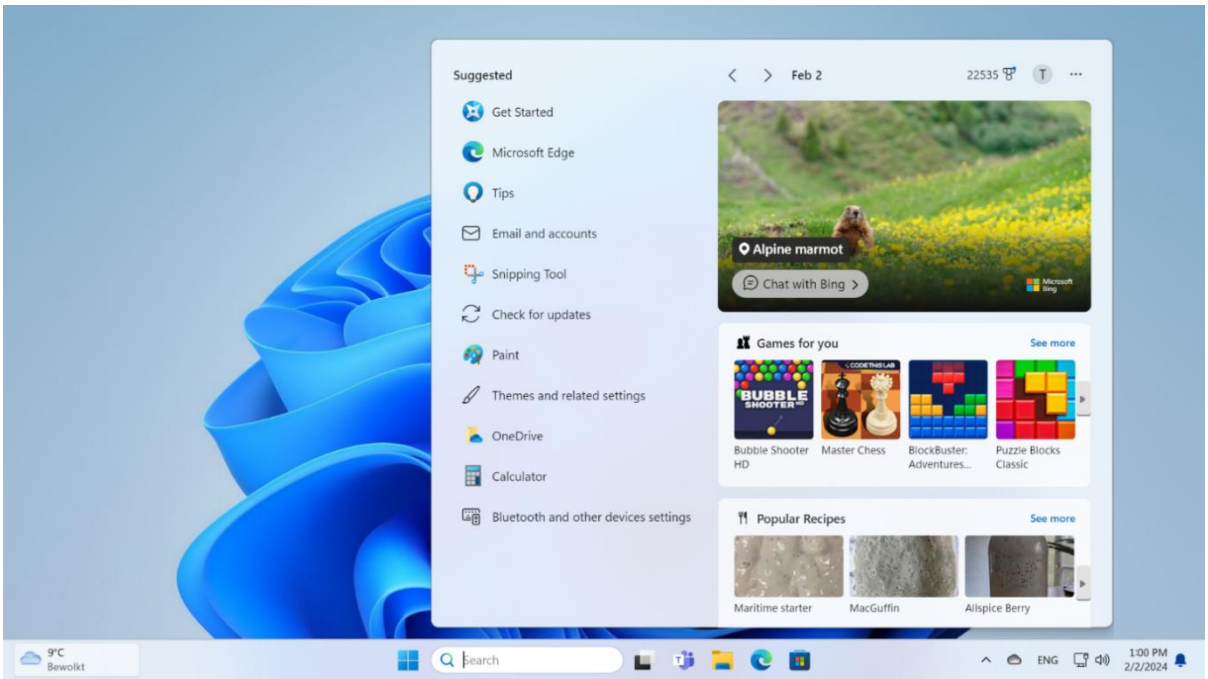
E. The Windows Search Box

358. Windows 10 and 11 have a search box on the Taskbar that opens an experience where applications can provide web search functionality. Only properly manifested applications packaged for the Microsoft Store can implement a web search provider

using public APIs to appear in the Windows Search experience.[159] Web search providers can specify (i) what to show when the user has not entered any search query (*see* **Figure 54**); (ii) search results when the user has entered a query (*see* **Figure 55**); (iii) an image that appears in the search box on the taskbar (*see* **Figure 56**); and (iv) the link type to use if the user clicks on something in the web search provider's user interface. If a user installs an application that has implemented a web search provider, a notification will appear in the Windows search experience notifying the user that a new web search provider is available with a link to Settings for the user to enable that provider (through clicking: Settings > Privacy & Security > Search permissions > Web search) (*see* **Figures 51-52**).

359. Web Search from Microsoft Bing is a preinstalled properly-manifested-application packaged for the Microsoft Store on Windows that implements a web search provider using public APIs and is enabled in the Windows Search experience (*see* **Figures 49-50**). The extensibility of the Windows 10 and 11 search experience described above was added because of the DMA and is offered only in the EEA. Outside of the EEA, users may freely install and use third-party search applications on Windows but only Web Search from Microsoft Bing may be accessed through the search box on the Windows Taskbar.

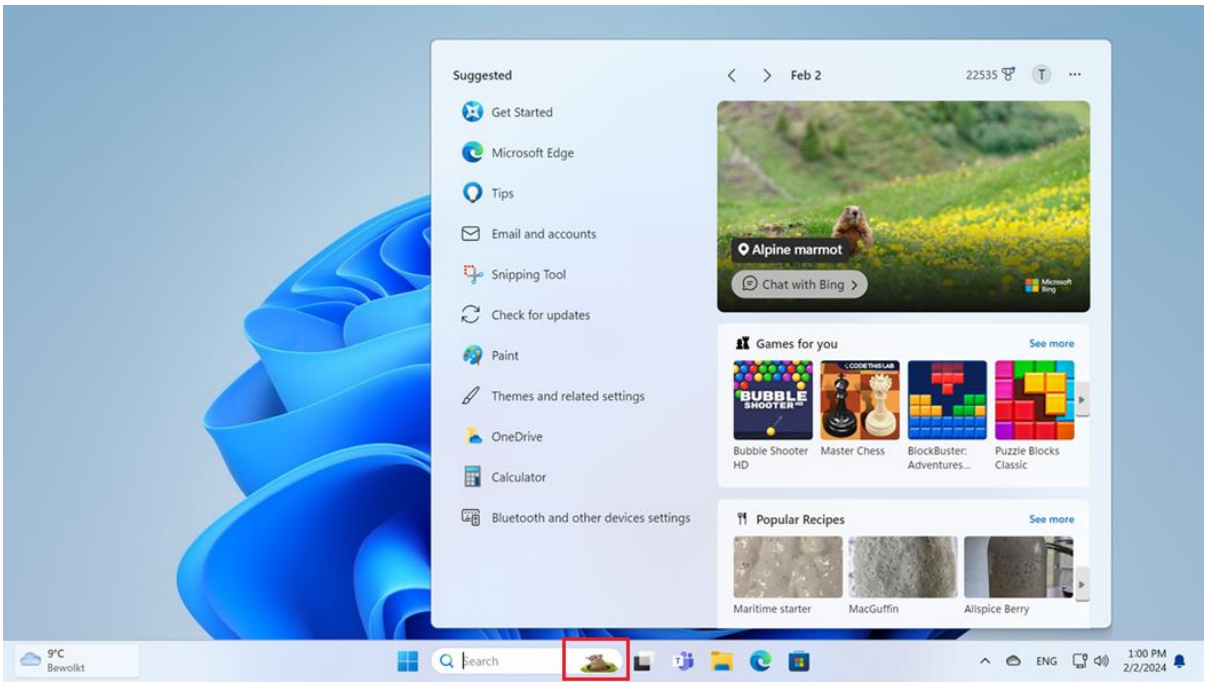
Figure 49. Screenshot Of The Experience With Web Search From Microsoft Bing Enabled In Windows Search



Source: Microsoft

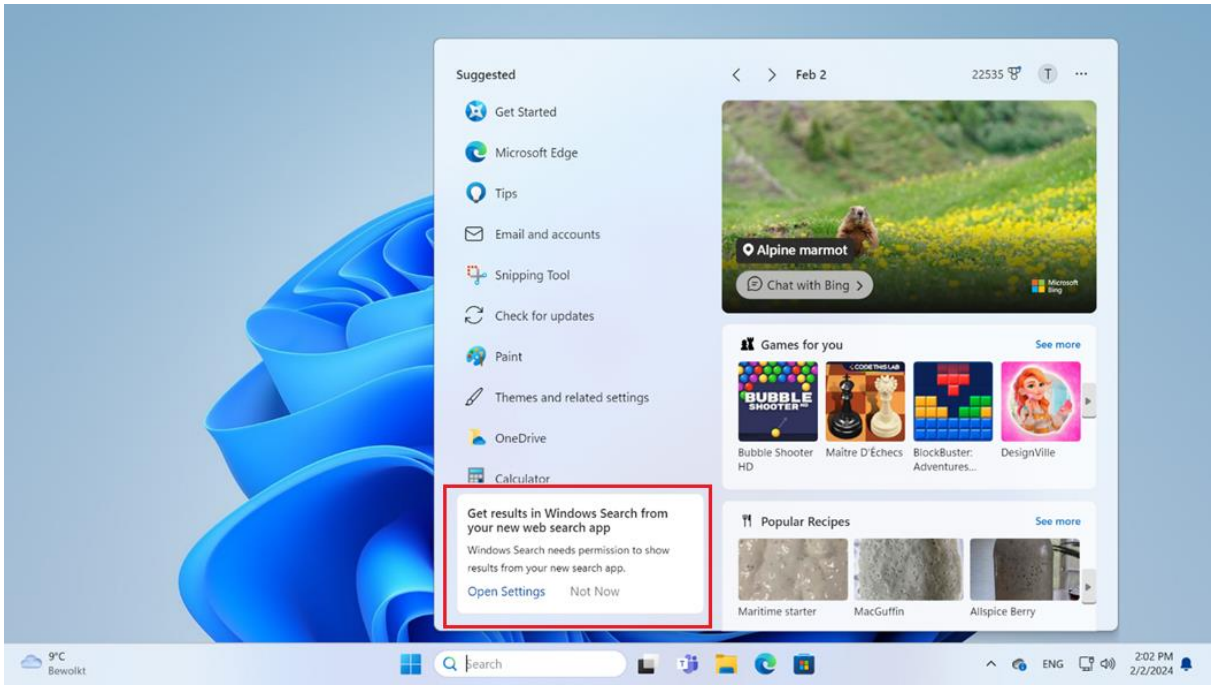
159 *See* Windows Search providers public API documentation.

Figure 50. Web Search From Microsoft Bing Powered Image On The Taskbar ("Gleam")



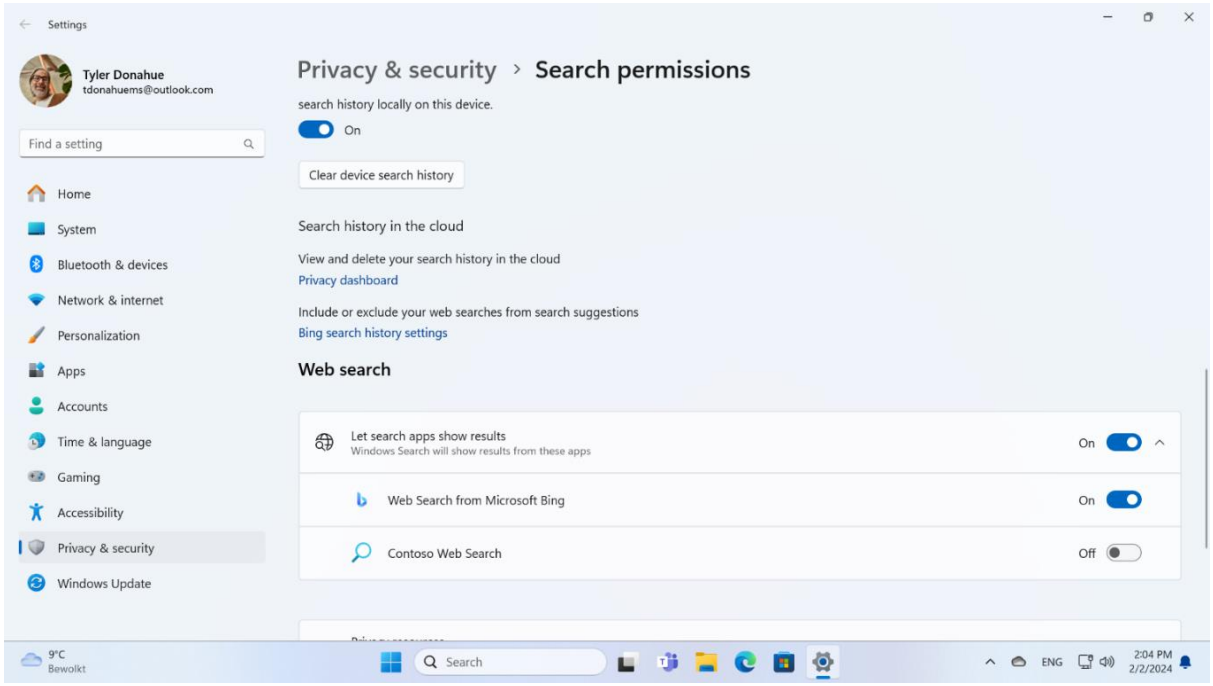
Source: Microsoft

Figure 51. Screenshot Of Notification That Appears When A New Web Search Provider Is Available With A Link To Settings



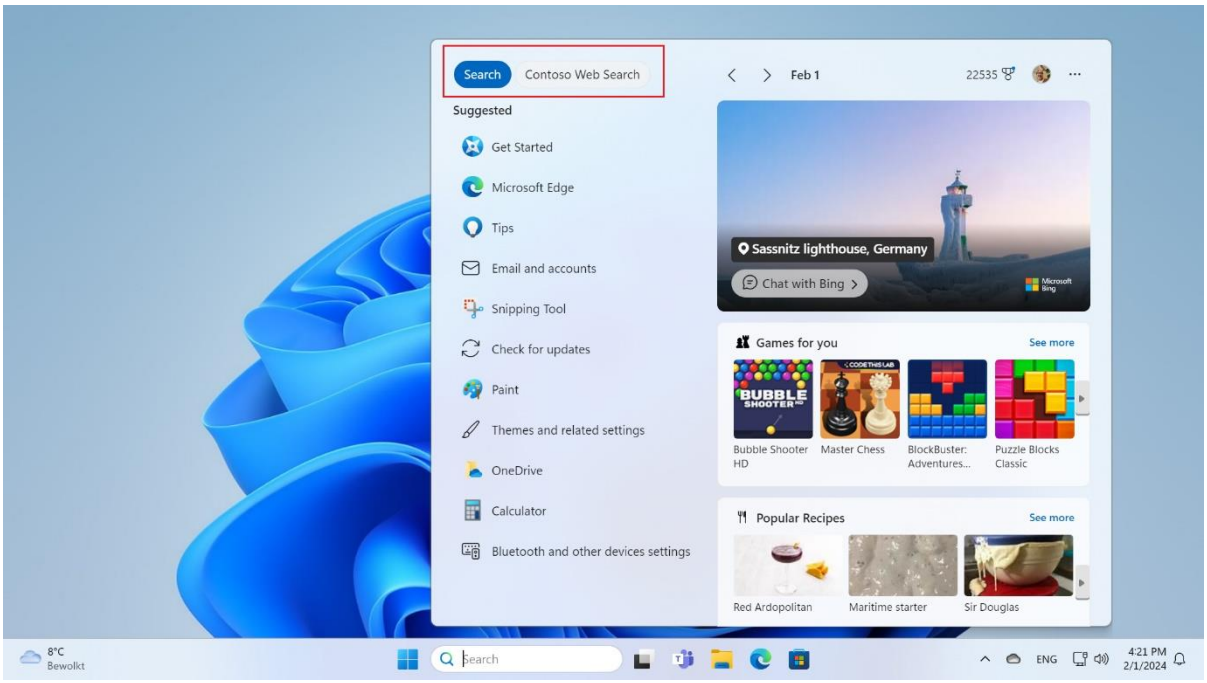
Source: Microsoft

Figure 52. Screenshot of Settings Page Where Users Can Configure Web Search Providers



Source: Microsoft

Figure 53. The Experience With Web Search From Microsoft Bing and Another Web Search Provider Enabled In Windows Search

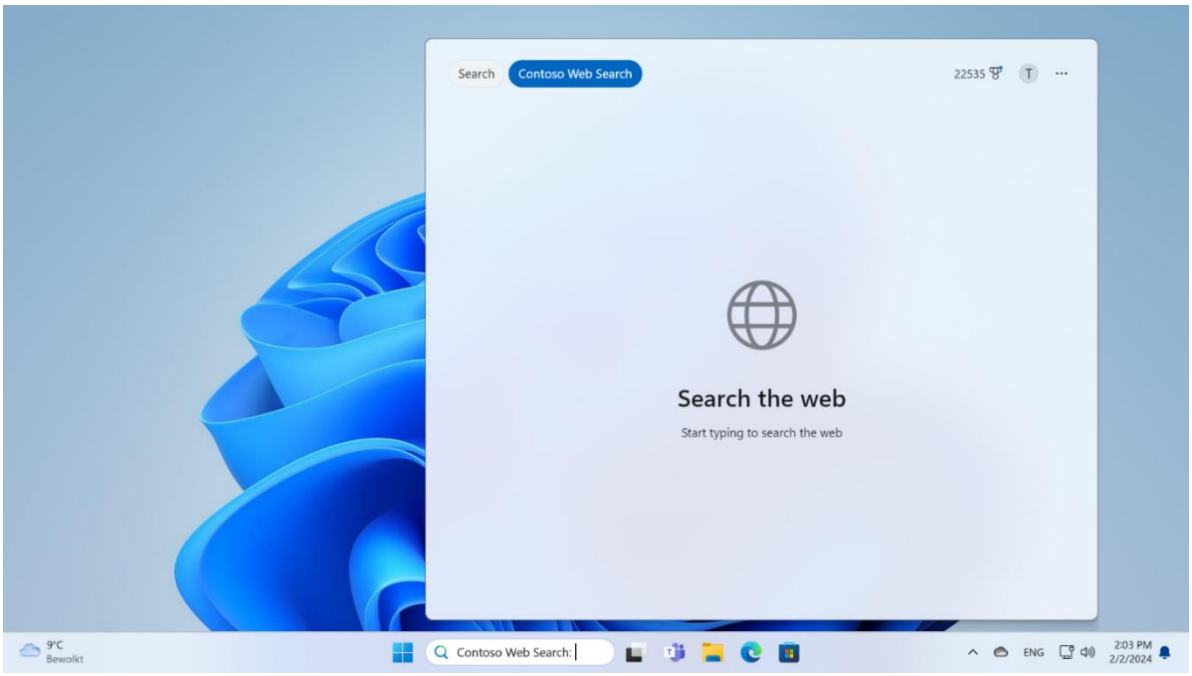


Source: Microsoft

F. Mockups Of What A Third-Party Web Search Provider Could Choose To Do In Windows Search

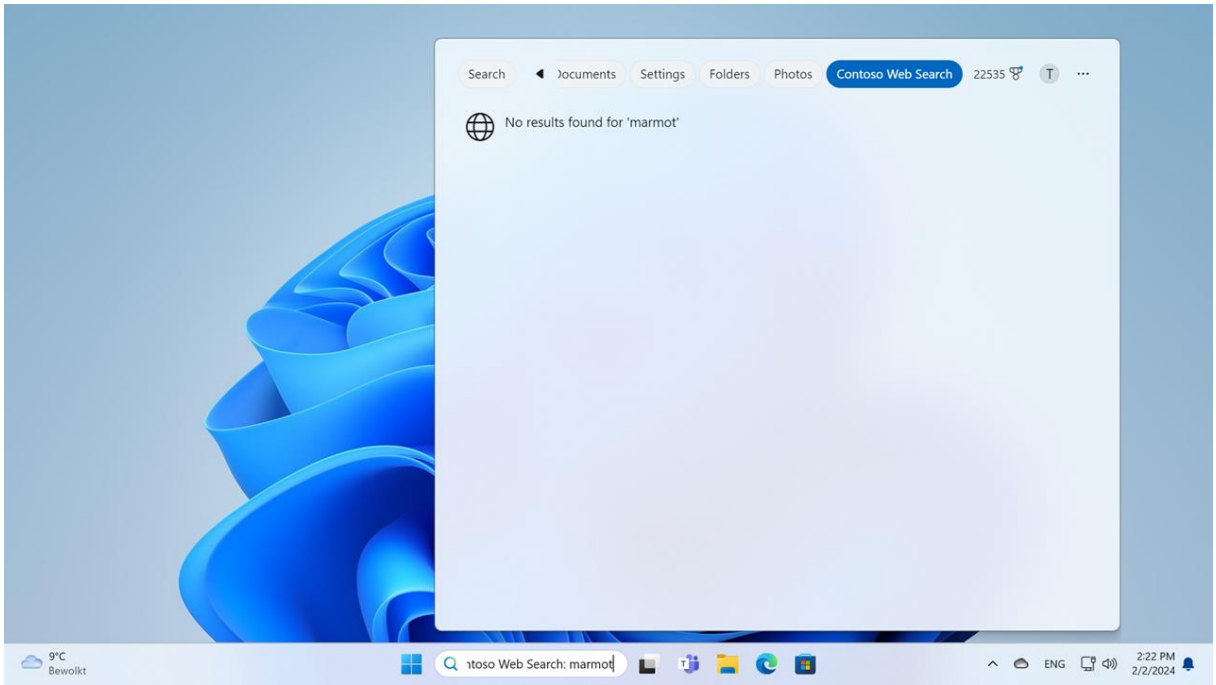
360. Microsoft provides below mockups of what a third-party web search provider could choose to do in Windows Search.

Figure 54. Option 1: Third-Party Web Search Providers Can Specify What To Show When The User Has Not Entered A Search Query



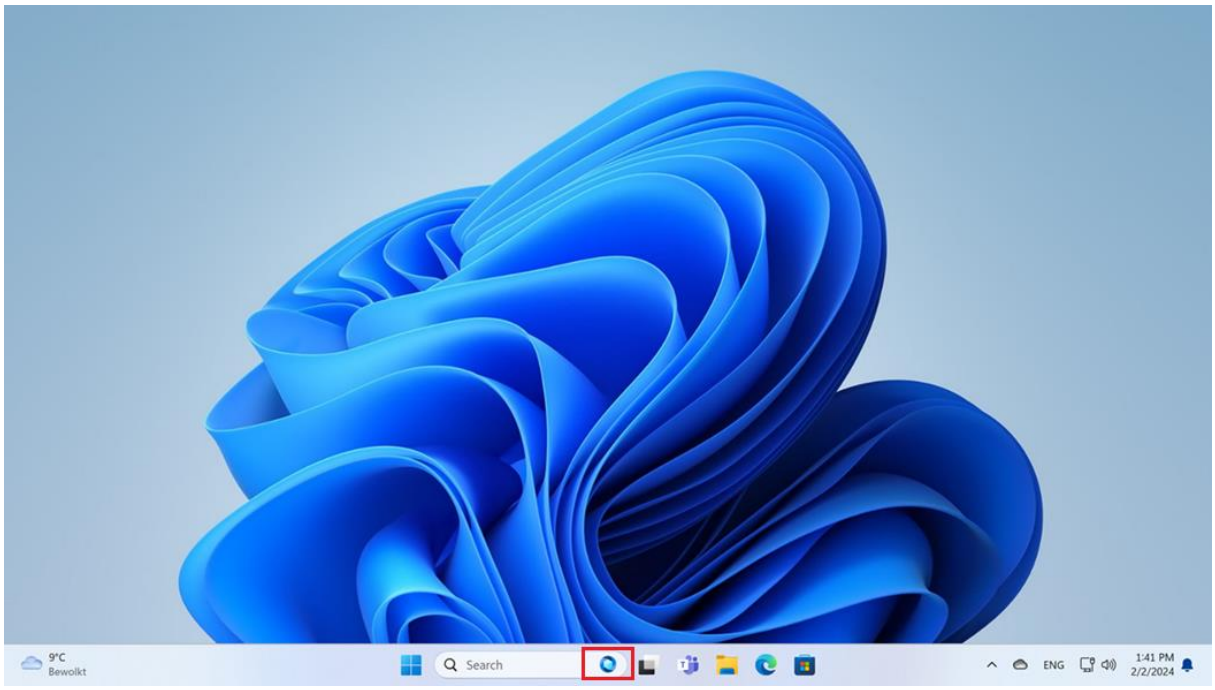
Source: Microsoft

Figure 55. Option 2: Third-Party Web Search Providers Can Specify What To Show When The User Has Entered A Search Query



Source: Microsoft

Figure 56. Option 3: Third-Party Web Search Providers Can Specify What Image ("Gleam") Appears In The Search Box On The Taskbar



Source: Microsoft

G. Windows 11 Widgets Board And Windows 10 Desk Bands

361. Windows 11 has a Widgets Board that is accessed through the Weather icon on the Taskbar, which opens an experience where Microsoft and third-party applications can provide widget and/or feed functionality. Only properly-manifested packaged applications for the Microsoft Store and PWAs offered through the Microsoft Store can implement a widget and/or feed provider using public APIs to display a widget and/or feed in the Windows Widgets Board.[160] Microsoft Edge is a preinstalled properly-manifested application distributed through a Microsoft Installer ("**MSI**") that implements widgets and feeds in the Widgets Board.[161] Already prior to the entry into force of the DMA, any application could implement a widget in the Widgets Board using public APIs equivalent to the widgets provided by Microsoft Edge, but only Microsoft Edge could be the feed provider. Microsoft Edge was designed as a part of Windows and Microsoft Edge-backed widgets and feeds used undocumented APIs to plug into the Widgets Board. Because of the DMA, Microsoft has built a set of publicly-documented APIs that allow third-party applications to be a feed provider on the Widgets Board on Windows 11 PCs in the EEA, which are similar to the news feed provided by Microsoft Edge. The Microsoft Edge-backed widgets and feeds will be redesigned to use the same public APIs.

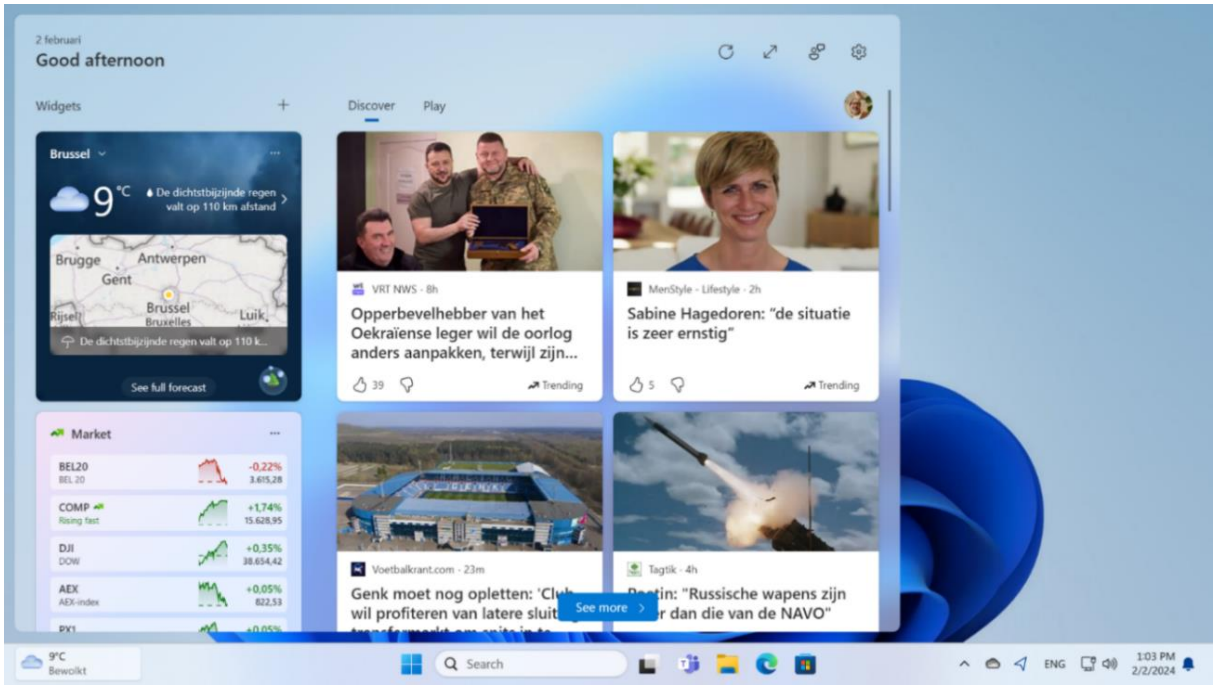
362. Starting in March 2024, Windows began rolling out a redesigned Widgets Board with an improved layout that makes it easier for users to use and identify their preferred

160 *See* Widgets overview public API documentation and Feed providers public API documentation.

161 Microsoft Edge was an OS component but is now an application in the EEA. It ships in the Microsoft Store with a verified publisher, manifest and capabilities declared, and is distributed through an MSI installer.

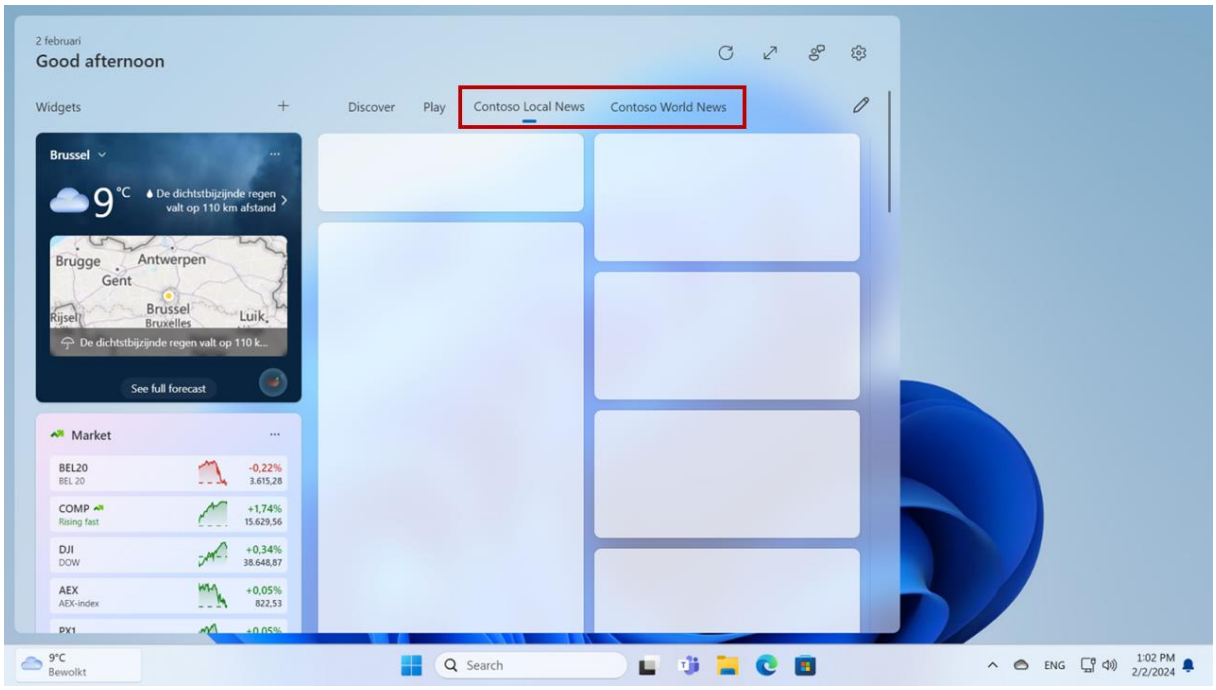
providers. The extensibility model for widgets and feeds will remain the same. In the original Widgets Board, widgets and feeds were next to each other on a single "board" (*see* **Figure 57**). The redesigned Widgets Board supports multiple "boards," including a dedicated widgets board and a dedicated feeds board for each installed and enabled feed provider (*see* **Figures 59-60**). The Widgets Board will open with the last board used.

Figure 57. Screenshot Of The Experience With Microsoft Edge As A Widget And Feed Provider Enabled In The Widgets Board



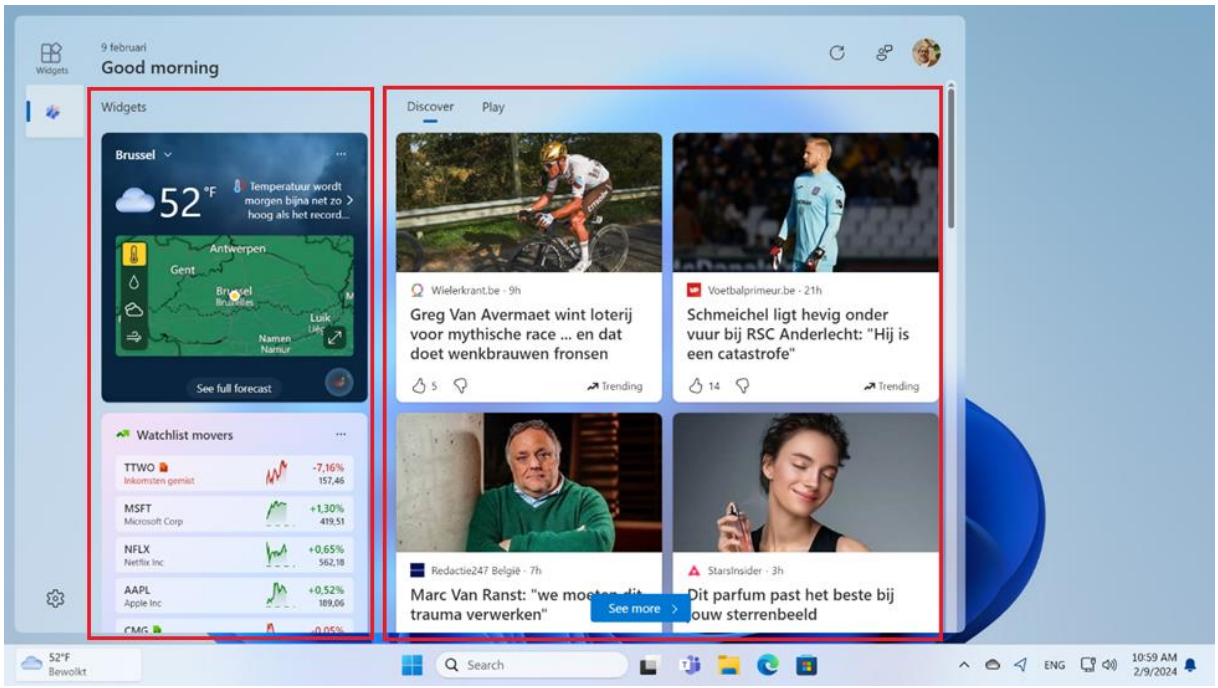
Source: Microsoft

Figure 58. Mockup Of What A Third-Party Feed Provider (Contoso) Could Do In The Widgets Board



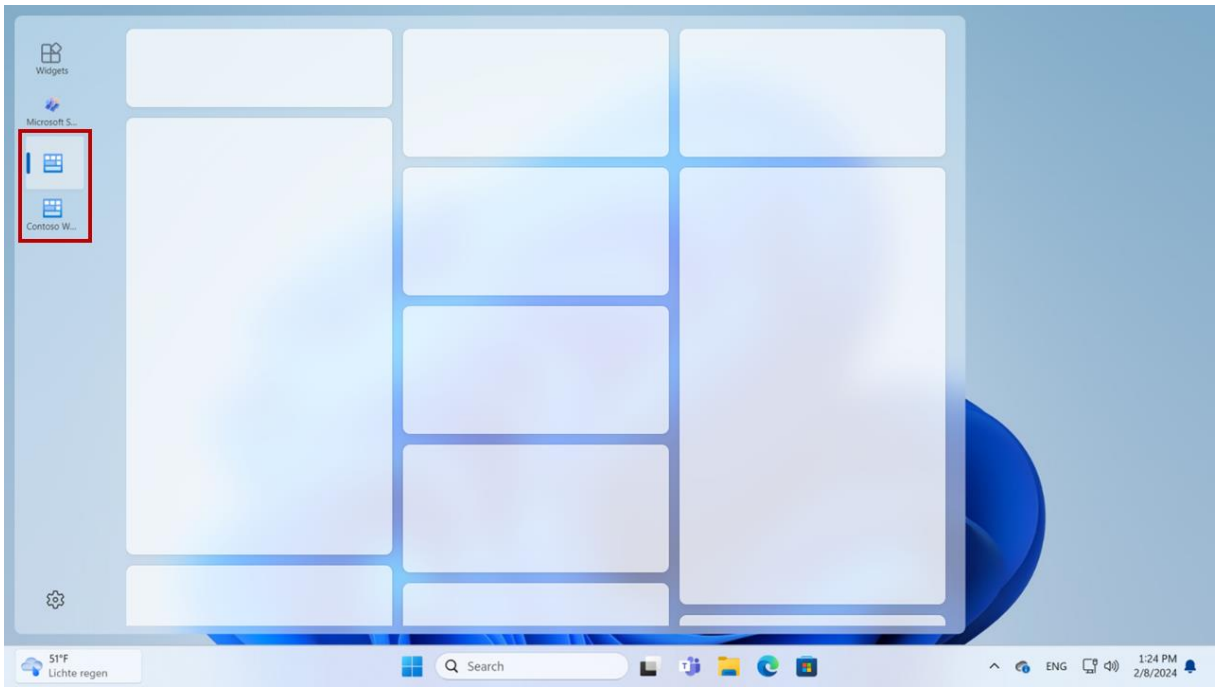
Source: Microsoft

Figure 59. Screenshot Of The Newly Designed Widgets Board With Microsoft Edge As A Widget (Left Box) And Feed Provider (Right Box) Enabled



Source: Microsoft

Figure 60. Screenshot Of The Newly Designed Widgets Board With Microsoft Edge And A Third-Party Feed Provider Enabled As A Widget And Feed Provider

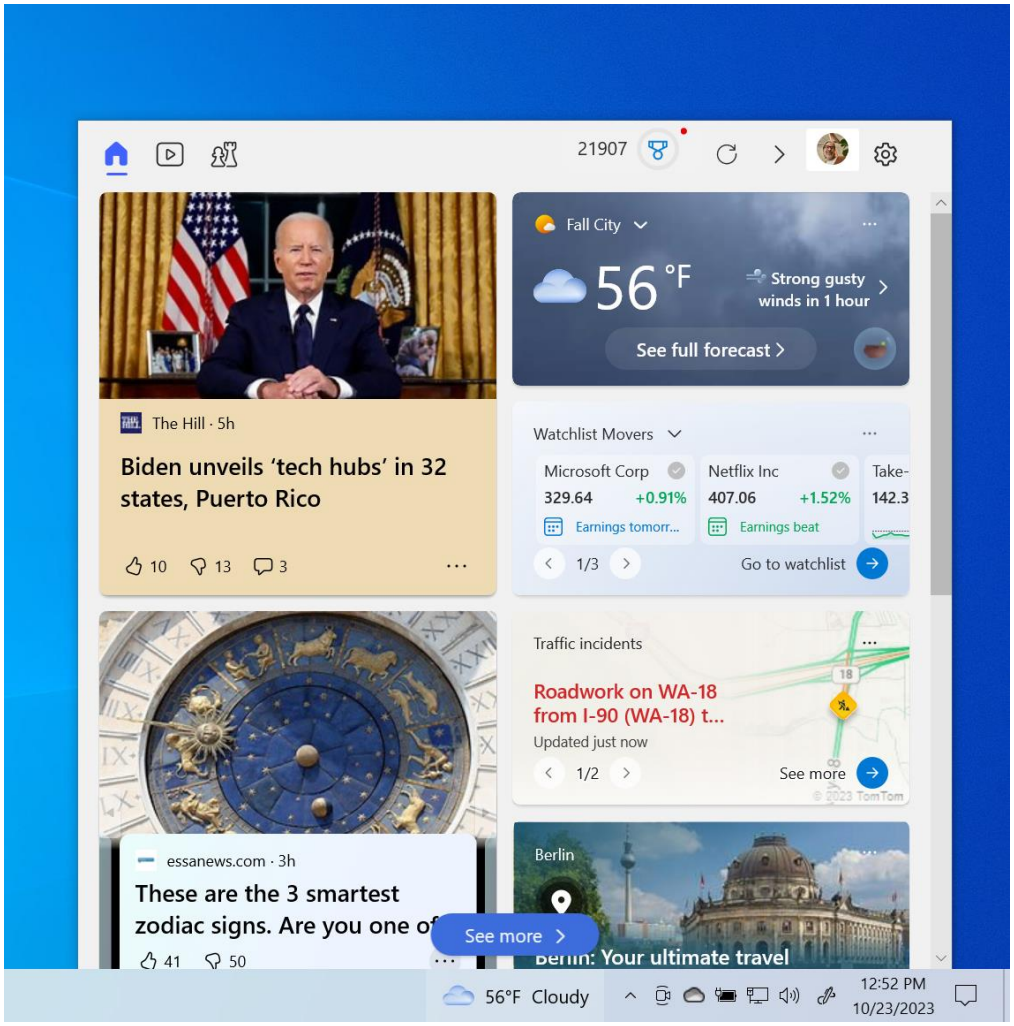


Source: Microsoft

363. Windows 10 does not have a Widgets Board. Microsoft Edge on Windows 10 has a related feature that is a dockable window on the Taskbar that, when clicked, opens a News and Interests feed (*see* **Figure 61**). Any application can create a similar dockable window on the Taskbar to display application content using public APIs to implement a Desk Band.[162] If a user installs an application that has implemented a Desk Band provider, that Desk Band provider can appear on the Taskbar. The extensibility of Desk Bands on the Taskbar existed before the entry into force of the DMA and is offered worldwide.

162 *See* Creating Custom Explorer Bars, Tool Bands, and Desk Bands public API documentation.

Figure 61. Windows 10 News And Interests Feed



Source: Microsoft

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[163]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

364. Microsoft refers to **Section 2.1.2 (i)** above.

b) when the measure was implemented;

365. Measures that were newly implemented for DMA compliance were implemented in the Windows 10 22H2 build 19045.4123 (generally available on 29 February 2024) and Windows 11 23H2 build 22631.3235 (generally available on 29 February 2024). Microsoft also released through the WIP Release Preview Channel for Windows 10 build 19045.3758 (generally available on 16 November 2023) and Windows 11 build 22631.2787 (generally available on 16 November 2023). Any end user or business user

163 For example, this may be particularly relevant to illustrate changes impacting user journeys.

of Windows can enroll in WIP (Settings > Windows Update > Windows Insider Program).[164]

c) the scope of the measure in terms of the products/services/devices covered;

366. Microsoft refers to the relevant versions of Windows defined in **Section 2.1** above.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

367. Prior to the entry into force of the DMA, Microsoft Edge relied upon a slightly different mechanism to set itself as the default on Windows PCs, but it no longer does so in most regions of the world, including the EEA. The extensibility of the Windows 10 and 11 Search Box was added because of the DMA and is offered only in the EEA. Outside of the EEA, users may freely install and use third-party search applications on Windows but only Web Search from Microsoft Bing may be accessed through the Windows 10 and 11 Search Box. The extensibility of the Windows 11 feeds in the Widgets Board was added because of the DMA and is offered only in the EEA. Outside of the EEA, widgets are extensible but feeds are not.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

368. Microsoft made required technical / engineering changes to Windows to meet the obligations of Article 6(7) of the DMA as described above.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[165] consent forms,[166] warning messages, system updates, functionalities available, or customer journey to access functionalities[167]);

369. Microsoft refers to **Section 2.1.2 (i)** above.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees,

---

164 For details, *see* Windows Insider Program | Windows 10 - release information | Windows 11 – release information.

165 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

166 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

167 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

370. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

371. None.

i) any consultation[168] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high- level description of the topic of the consultation with those users/parties;

372. On 16 November 2023, Microsoft released a preview version of Windows 10 and 11 through the WIP (*see* above) and published a blog detailing the changes made to comply with the DMA so users and/or any interested parties could provide feedback.[169]

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

373. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

374. None.

---

168 This information should include a description of the methodology for the consultation.

169 *See* https://blogs.windows.com/windows-insider/2023/11/16/previewing-changes-in-windows-to-comply-with-the-digital-markets-act-in-the-european-economic-area/.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

375. On 16 November 2023, Microsoft released a preview version of Windows 10 and 11 through the WIP (*see* above) and published a blog detailing the changes made to comply with the DMA so users and/or any interested parties could provide feedback.[170] Microsoft received feedback made publicly available by Mozilla and Vivaldi.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

376. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

377. Microsoft provides solutions on Windows to protect customers from malicious applications, as do other third-party security providers. If a business user ships a malicious application the user can be warned and/or the application could be blocked from running on Windows in order to protect the user.[171]

o) any type of market analysis or testing (in particular A/B testing[172]), business user surveys or consumer surveys or end user consent rates,[173] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[174]

378. Microsoft refers to **Section 2.1.2 (ii) (b)** above regarding the WIP.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or

---

170 *See* https://blogs.windows.com/windows-insider/2023/11/16/previewing-changes-in-windows-to-comply-with-the-digital-markets-act-in-the-european-economic-area/.

171 *See* How Microsoft identifies malware and potentially unwanted applications the publicly disclosed classification criteria.

172 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

173 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

174 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[175]

379. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

380. Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

r) any relevant data[176] **which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;**

381. As outlined in **Section 2.1.2 (ii) (q)** above, Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

382. Microsoft remains open to discussing any indicators and ways to monitor those indicators that would assist the Commission in its assessment of whether a particular measure is effective in achieving the objectives of the DMA, including metrics that

---

175 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

176 Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

track the choices made by users under mechanisms required by the DMA such as consent rates, installing and setting applications as the default, use of data portability mechanisms or others.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

383. None.

Regarding Article 6(8)

384. Microsoft refers to **Section 2.3** below.

Regarding Article 6(9)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

385. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 6(9) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[177] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

386. Article 6(9) of the DMA provides: "[t]*he gatekeeper shall provide end users and third parties authorised by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data*."

387. As described above in relation to Windows' compliance with Article 5(2) of the DMA, there are three categories of data that Windows collects: (i) Windows Diagnostic Data, (ii) Account Data, and (iii) Windows Required Service Data. **Sections A to D** below describe how Microsoft complies with Article 6(9) of the DMA with respect to each data category, as well as explain data portability limitations necessary to protect users against cyberattacks.

A. Diagnostic Data

388. As described in relation to Windows' compliance with Article 5(2) of the DMA, Windows collects Windows Diagnostic Data to diagnose and solve problems to keep Windows up-to-date, secure, and operating properly, and to make product improvements.[178]

---

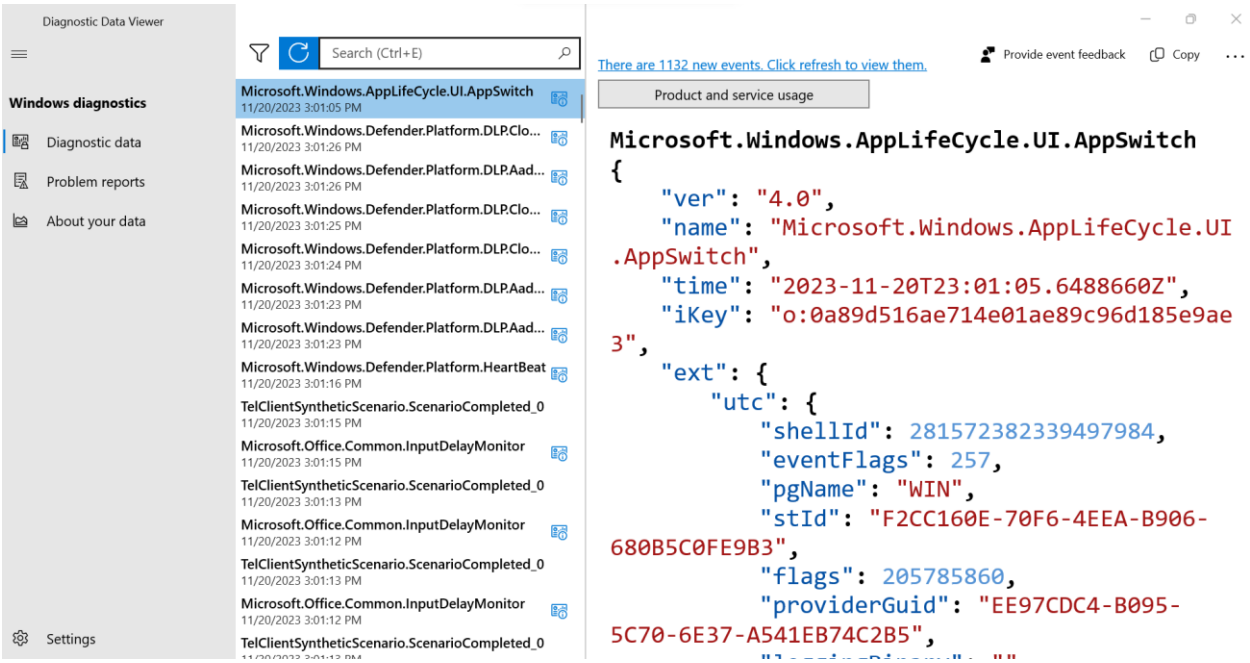
177 The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

178 *See* Diagnostics, feedback, and privacy in Windows.

389. Microsoft provides end users with access to the Diagnostic Data collected by Windows on their PC through a tool that permits viewing and exporting Diagnostic Data. In addition, end users can authorize a third party to access their Diagnostic Data by installing an application that uses publicly documented Windows APIs to retrieve and process Diagnostic Data on the PC.

390. End users can view and export Windows Diagnostic Data using the Diagnostic Data Viewer application ("**DDV**"),[179] as illustrated in **Figure 62**, which is available to all users free of charge from the Microsoft Store, if not preinstalled on the device.

Figure 62. Windows Diagnostic Data Viewer Application

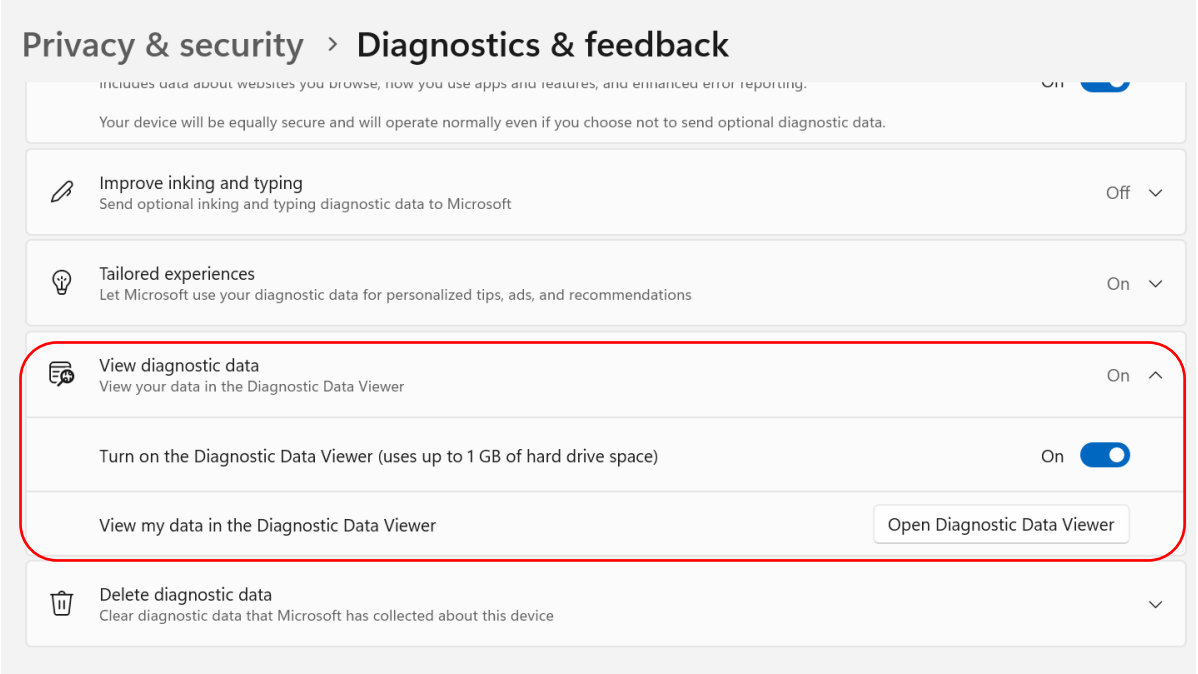


Source: Microsoft

391. To use DDV, users must first enable DDV in Windows Settings (*see* **Figure 63**). This is because enabling DDV can consume a significant amount of space (up to 1GB of hard drive space).

179 *See* Diagnostic Data Viewer Overview.

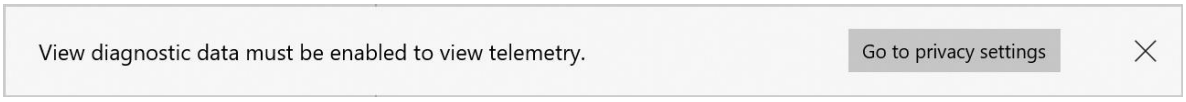
Figure 63. Diagnostic Data Viewer Setting In Windows Settings



Source: Microsoft

392. If a user attempts to run DDV before enabling this setting, then DDV prompts the user to enable the setting and provides a link directly to the setting in Windows Settings (*see* **Figure 64**).

Figure 64. DDV Prompt To Enable Telemetry In Windows Privacy Settings



Source: Microsoft

393. Once the DDV setting is enabled, Windows stores Diagnostic Data in a local file stored on the PC. By default, this file will fill with as much Diagnostic Data from the last 30 days as will fit within 1GB of disk space, but the end user can adjust both the number of days and the file size in the DDV application. End users can use DDV to view, filter, and export Windows Diagnostic Data in a portable format (DDV exports events into a comma-separated values ("CSV") file with each event's data provided in JSON format). End users can delete the Diagnostic Data that Microsoft has collected from the PC through Windows Settings.

394. Following industry-practice data minimization principles, Windows only generates Diagnostic Data through the activity of the end user when it will be collected and used for a diagnostic purpose. Windows only generates optional Diagnostic Data if the end user provides consent for Windows to collect optional Diagnostic Data. As described in relation to Windows' compliance with Article 5(2) of the DMA, Windows collects some optional Diagnostic Data from only a small sample of devices. Windows only generates sampled data if the PC is included in the sample. Consequently, the DDV will show optional Diagnostic Data only if the user provided consent for Microsoft to collect optional Diagnostic Data, and it will show sampled Diagnostic Data events only

if the PC is included in the sample, because the data only exists if these conditions are met.

395. Third-party applications can retrieve Windows Diagnostic Data in the same way as DDV using a publicly-documented API.[180] The end user must enable the DDV setting in Windows Settings and install a third-party application to authorize the third party to process Windows Diagnostic Data. Any third-party developer can access this API through the Windows Software Development Kit ("**SDK**") and can obtain information about how it functions through Microsoft's public developer documentation, which describes how to use the API and the data returned.

396. Windows sends Diagnostic Data to Microsoft on a schedule designed to minimize impact on the user and not in "real time." The Windows Telemetry Client is software that is part of Windows and is responsible for managing the Diagnostic Data gathered on the device. The Telemetry Client pre-processes and caches Diagnostic Data on the PC before periodically sending it to Microsoft. The Telemetry Client is aware of the state of the PC, such as available network bandwidth and battery state, which it uses to determine the best time to transmit the data.

397. Both the DDV and the associated API provide continuous and real-time access to Diagnostic Data on the PC. Since Windows sends Diagnostic Data to Microsoft only periodically, the end user has access to the data through the DDV likely more quickly than Microsoft receives it.

B. Account Data

398. Account Data is data associated with the user's account. End users can authorize third parties to access their Account Data through the Microsoft Graph API. Microsoft also makes Account Data available to end users through a website located at account.microsoft.com ("**AMC**") or through the software that collects the Account Data.

399. When Account Data may be useful to end users outside the context of Windows, Microsoft makes this data available to end users through AMC. Data made available through AMC is available to the user by signing-in to the website, where they can view Account Data and export it in a portable format (some exports of data may take a short time to make the data available, typically only a few minutes depending upon the amount of data). Some Account Data collected by Windows from an end user's PC may only synchronize to the cloud periodically. Account Data will only be available through AMC and the Microsoft Graph API after Microsoft receives it from the PC, but it is subsequently available continuously and in real time.

400. Some Account Data is more effectively made available to end users through the software that collects it. For example, with consent, Windows will synchronize Windows Settings into the user's Account Data, but the best place to view the current settings is in Windows Settings. Windows Settings data can be synchronized to other Windows PCs into which the user signs-in.

---

180 *See* developer document for the diagnosticdataquery.h header.

401. Regardless of whether Account Data is visible to end users through AMC or only through the software that collected it, Microsoft makes Account Data stored by Windows on the Microsoft Graph available to third parties authorized by the end user through the Microsoft Graph API. This allows third parties to develop applications that access the user's Account Data, with consent, and to port it to other platforms.

402. Some Account Data cannot be exported because it is not useful outside the context of Windows. For example, Windows may store the user's software license details about the Windows license purchased for a device, which can be used to revalidate the Windows license if a user reinstalls Windows on their PC. This Account Data is not useful other than to validate the software license. Another example is BitLocker, which is a feature of Windows that securely encrypts the Windows filesystem. BitLocker stores a backup of the user's encryption keys in Account Data, but this data cannot be easily exported because it is not useful except to unlock the encrypted filesystem.

403. Any third-party developer can access Account Data using the Microsoft Graph API provided that the end user consents by authenticating with the Microsoft Graph. Developers can obtain information about the Microsoft Graph API through Microsoft's public developer documentation, which describes how to use the API and the data returned, and Microsoft provides several SDKs for accessing the Microsoft Graph using different programming languages.[181]

C. Windows Required Service Data

404. As described in relation to Windows' compliance with Article 5(2) of the DMA, some features of Windows are powered by cloud services. Windows sends Required Service Data to these services to provide the cloud-enabled features.

405. Required Service Data is ephemeral and consequently cannot be made portable and exported. Most Required Service Data is discarded once the service is provided to the user. Some features store the Required Service Data for a short period of time, typically less than two days, before discarding it. In either case, the data is not stored for long enough to be made available to end users.

406. There are two situations where cloud-enabled features may store data after processing Required Service Data. Some cloud-enabled features result in changes to the user's Account Data. When cloud-enabled features store data as Account Data, it is available to end users as described in the previous section.

407. As described in relation to Windows' compliance with Article 5(2) of the DMA, Microsoft sometimes retains Required Service Data in aggregated or de-identified form, which is used to improve the corresponding cloud service. This data is no longer personal data because it is not linked or linkable to an individual user and consequently cannot be made portable.

D. Cybersecurity Protection

408. Windows comes with security features, such as the Defender Security Services, described in relation to Windows' compliance with Article 5(2) of the DMA, to protect

[181] *See* Microsoft Graph SDK overview.

users against cyberattacks. The Defender Security Services provide security protection to Windows users.

409. Microsoft limits the portability of certain data directly from Defender Security Services to protect the cybersecurity of Microsoft users. Defender Security Services scan for and block malicious software, downloads, and websites and prevent malicious actors from creating fake Microsoft accounts for fraud and other bad purposes. If the data contained in Defender Security Services was made available for export directly from these services, motivated abusers would be able to analyze the precise data points collected and how the services use that data to protect Windows PCs, learning to better reverse engineer the services and circumvent their inner workings. Thus, these bad actors would be better able to develop strategies for exploiting or evading the protections offered by these services, harming the security of Windows users and the Windows ecosystem at large.

410. This limitation has no impact on end users' ability to change to competing third-party products. Defender Security Services function by actively analyzing data contained elsewhere on the Windows PC. In contrast to many other types of digital services, the utility of the data collected by Defender Security Services is to actively monitor what is happening elsewhere on the PC. Defender Security Services collect data to monitor from Windows via publicly documented APIs. Competing third-party products are able to actively monitor the same Windows data points by collecting it in the same manner as Defender Security Services via these publicly documented APIs. A user needs only to install and set up a competing product for it to begin to collect the Windows data it monitors – this is not impacted by the limitation of direct data portability from Defender Security Services. Direct data export from Defender Security Services is immaterial for users looking to change to competing products.

411. Much of the data collected by Defender Security Services is available for export from Windows outside of Defender Security Services. Users are empowered to export their Windows personal data from Windows, without the exploitable insight into the functions of Defender Security Services.

E. <u>On-Device Data</u>

412. The categories of data described above cover data that Microsoft collects from Windows PCs. Windows stores some data provided by end-users or generated from user-activity on the PC. Article 6(9) of the DMA requires this data to be made effectively portable to support scenarios such as switching or multi-homing. As described above, not all data generated from user activity is useful away from the PC to which it relates. For example, as described above, a user's BitLocker key need not be made portable because it can only be used with a specific encrypted device and isn't useful if ported to another device.

413. As described above, the data Windows stores can generally be seen within the feature that collects the data. For example, users can see and change settings in the Windows Settings feature.

414. The data is typically also available through publicly documented APIs or through publicly available tools, available for download from Microsoft. This means that third parties write applications to port data from Windows to other devices on behalf of end-

users. Microsoft will monitor feedback it receives related to data portability to assess any additional requests from developers.

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[182]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

415. The practices described above in **Section 2.1.2 (i)** generally existed prior to the entry into force of the DMA. To comply with Article 6(9) of the DMA, Microsoft made changes to the Microsoft Graph API to provide access to some Account Data that was not previously portable through this means, such as Windows Settings.

b) when the measure was implemented;

416. Microsoft made changes to the Microsoft Graph API in the months prior to the DMA coming into effect.

c) the scope of the measure in terms of the products/services/devices covered;

417. The practices described above apply to the Windows PC OS installed locally on PCs as well as Microsoft's "desktop as a service" offerings (Azure Virtual Desktop and Windows 365) where the software runs in the cloud.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

418. The practices described above apply worldwide.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

419. Microsoft refers to **Section 2.1.2 (i) (b)** for a description of the relevant changes to the Microsoft Graph API to provide access to some Account Data that was not previously portable through this means, such as Windows Settings.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer

[182] For example, this may be particularly relevant to illustrate changes impacting user journeys.

interface, choice screens,[183] consent forms,[184] warning messages, system updates, functionalities available, or customer journey to access functionalities[185]);

420. No change has been made to the customer experience as a result of Windows' compliance with Article 6(9) of the DMA.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

421. No change has been made to the remuneration flow or terms and conditions as a result of Windows' compliance with Article 6(9) of the DMA.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

422. All changes required to comply with Article 6(9) of the DMA, as applicable to Windows, are described in the above sections.

i) any consultation[186] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high-level description of the topic of the consultation with those users/parties;

423. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an

183 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

184 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

185 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

186 This information should include a description of the methodology for the consultation.

explanation of the reasons why the recommendations made by the external consultants were not followed;

424. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

425. None.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

426. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

427. Windows Account Sync data is only synchronized between a user's PC and the Microsoft Graph if the user consents through the new consent described in relation to Windows' compliance with Article 5(2) of the DMA. Consequently, the user must consent to synchronize this data for the data to be available to third parties through the Microsoft Graph API.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

428. Microsoft refers to **Section 2.1.2 (i) – Section D** for the information collected by Windows to protect users' cybersecurity.

o) any type of market analysis or testing (in particular A/B testing[187]), business user surveys or consumer surveys or end user consent rates,[188]

[187] A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

[188] End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[189]

429. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[190]

430. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

431. Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

r) any relevant data[191] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

432. As outlined in **Section 2.1.2 (ii) (q)** above, Microsoft remains open to discussing any indicators or data that would assist the Commission in its assessment whether a particular measure is effective in achieving the objectives of the DMA. In assessing such metrics, it will be important to consider whether the pre-existing design and operation of the platform was largely consistent with the provisions in question or

189 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

190 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

191 Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

whether significant changes were required. In the former circumstance one would not expect to see measurable changes in end user or business user behavior and metrics may not be indicative of effectiveness.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

433. Microsoft remains open to discussing any indicators and ways to monitor those indicators that would assist the Commission in its assessment of whether a particular measure is effective in achieving the objectives of the DMA, including metrics that track the choices made by users under mechanisms required by the DMA such as consent rates, installing and setting applications as the default, use of data portability mechanisms or others.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

434. Microsoft refers to **Section 2.1.2 (i)**.

Regarding Article 6(10)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

435. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 6(10) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[192] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

436. Article 6(10) of the DMA provides: "[t]*he gatekeeper shall provide business users and third parties authorised by a business user, at their request, free of charge, with effective, high-quality, continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of the use of the relevant core platform services or services provided together with, or in support of, the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users. With regard to personal data, the gatekeeper shall provide for such access to, and use of, personal data only where the data are directly connected with the use effectuated by the end users in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end users opt in to such sharing by giving their consent*."

437. Article 6(10) of the DMA requires Microsoft to make certain data collected by Windows on PCs in the EEA ("**Business User Data**") available to business users at their request, and to third parties authorized by those business users. Business User Data is data that is either provided or generated by those business users in the context of their use of Windows, including data generated by end users engaging with products or services offered by those business users.

438. For the purposes of Windows compliance with Article 6(10) of the DMA, business users are providers of non-Microsoft applications that run on Windows. These are the business users using Windows to deliver products and services to end users from which Windows might collect data. Microsoft must also make personal data collected by

[192] The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

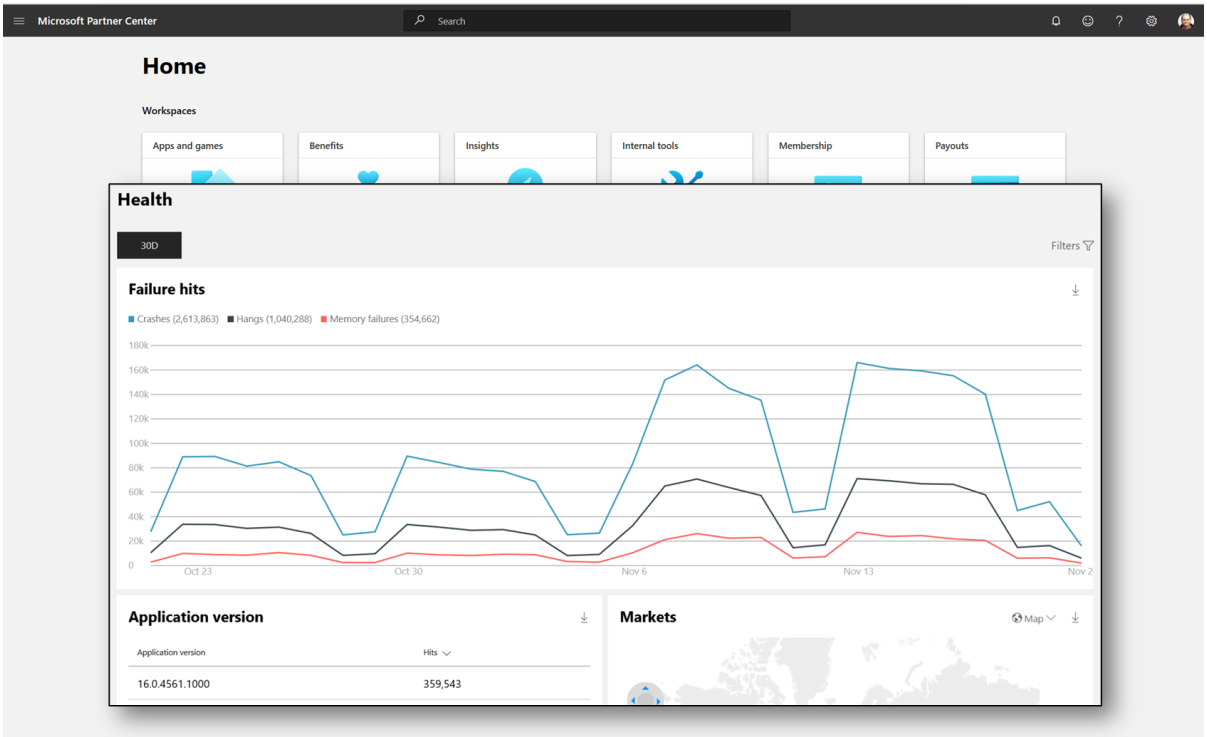
Windows from end users available to a business user to the extent the personal data is directly connected to the end user's use of the business user's software ("**3P End User Data**"), and only if the end user opts-in to share the data by providing consent.

439. As described above in relation to Windows' compliance with Article 5(2) of the DMA, there are three categories of data that Windows collects: (i) Windows Diagnostic Data, (ii) Account Data, and (iii) Windows Required Service Data. Below, Microsoft describes how it complies with Article 6(10) of the DMA with respect to each data category, to the extent they constitute Business User Data. Microsoft will monitor feedback it receives from business users related to data access to address any gaps in what is available to business users.

440. **Diagnostic Data.** As described in relation to Windows' compliance with Article 5(2) of the DMA, Windows collects Windows Diagnostic Data to diagnose and solve problems to keep Windows up-to-date, secure, and operating properly, and to make product improvements.[193]

441. Business users can access Business User Data created from Diagnostic Data collected in the context of their non-Microsoft applications through the Microsoft Partner Center application ("**Partner Center**"), as shown in **Figure 65**, which illustrates an application health report showing crashes in a business user's application.

Figure 65. Partner Center Portal With Example Report (Application Health And Failure Report)



Source: Microsoft

193 *See* Diagnostics, feedback, and privacy in Windows.

442. Partner Center provides business users, free-of-charge, with access to aggregated Diagnostic Data.[194] As described above regarding Windows compliance with Article 5(2) of the DMA, Microsoft receives Diagnostic Data from PCs only periodically, so it is not always available in "real-time." After Microsoft receives Diagnostic Data, some processing is required to aggregate data from multiple end users and to create the relevant Business User Data before it is made available through Partner Center. Microsoft's practice is to ensure that Business User Data is available within 24 to 48 hours of receipt of the relevant Diagnostic Data. This is consistent with the time it takes Microsoft to process and aggregate Diagnostic Data for its own purposes.

443. In general, the applicable Diagnostic Data to which Microsoft must provide business users with access under Article 6(10) of the DMA is optional Diagnostic Data. This data is only generated on PCs where the end user consents to the collection of diagnostic data at the optional level. For end users who do not consent, the diagnostic data is not created and there is nothing to make available to business users.

444. Microsoft makes only aggregated data available through Partner Center to protect the privacy of individual end users. Partner Center provides access to a subset of the data it collects about third-party applications covering the most important scenarios where business users need data from Microsoft in the aggregate to troubleshoot issues. If a business user wishes to gain access to all 3P End User Data containing Diagnostic Data, then that business user will need to collect it directly from the end user's PC with their consent. The relevant end users will need to install software from the business user to collect this data as described above in relation to Windows compliance with Article 6(9) of the DMA. The software from the business user can access Diagnostic Data collected by Windows using the publicly-documented Diagnostic Data APIs in Windows.

445. In practice, application developers typically incorporate their own telemetry client into applications to gather detailed telemetry specific to their application in just the same way that Microsoft instruments its applications that are not part of Windows. The most critical information for business users that may only be available from Microsoft is the Diagnostic Data needed to investigate crashes and other issues that impact the functioning of the telemetry itself thereby preventing the collection of the application's own telemetry. In these situations, Microsoft helps vendors with any information it has available, which is typically available through Partner Center.

446. To access Partner Center, business users must create a Microsoft developer account[195] and register the applications for which they wish to see data. Developer accounts can be created for individuals or for a company.[196] Company accounts require greater verification so that Microsoft can validate that the person creating the account is authorized to create the account for said company. There is a small one-time fee to register a developer account, and data is subsequently made available free-of-charge to registered developers through Partner Center.[197] Developer accounts are subject to the

---

194 *See* Partner Center Overview.

195 *See* Open a developer account in Partner Center.

196 *See* Account types, locations, and fees.

197 Currently c. USD 19 for individual accounts and c. USD 99 for company accounts (the exact amount varies depending on the user's country or region).

terms and conditions of the Microsoft App Developer Agreement.[198] Microsoft's public developer documentation website provides details of Partner Center and the data available there.[199]

447. If a business user distributes its application through the Microsoft Store, then the application will automatically be registered to the developer account used to upload the application to the Microsoft Store. For Windows applications distributed outside the Microsoft Store, which covers most applications, the business user must first follow a process to register the application before they can see data in Partner Center.[200] Before Microsoft can share Business User Data with a business user, Microsoft must verify that the business user is the owner of the application. To accomplish this, the business user must use a code signing certificate (obtained from a trusted third party) to sign their application and then take steps to demonstrate to Microsoft that they possess the code signing certificate.

448. As described above in relation to Windows compliance with Article 5(2) of the DMA, Microsoft may process Diagnostic Data on behalf of customers, in which case Microsoft processes data only in accordance with the customer's instructions, which do not include making aggregated data available to application providers through Partner Center. Consequently, business users who want access to such data must contact the customer directly and request that data be shared with them.

449. **Account Data.** As described above in relation to Windows compliance with Article 5(2) of the DMA, Account Data is personal data associated with the user's account. Data that Windows stores in the user's Account Data is not typically associated with non-Microsoft applications. For example, if the user adds a word to their custom dictionary while using non-Microsoft applications, the custom dictionary stored in the Account Data does not record which application caused the word to be stored. Consequently, most Account Data is not part of Business User Data.

450. To the extent that any Account Data is Business User Data because it is directly connected with the end user's use through Windows of the business user's products and services, and because Account Data is personal data, Microsoft may only make it available to business users consistent with Article 6(10) of the DMA with the end user's consent. As described above in relation to Windows' compliance with Article 6(9) of the DMA, Account Data stored in the Microsoft Graph is available to third parties (including business users) through the Microsoft Graph API subject to the end user's consent.

451. **Windows Required Service Data.** As described above in relation to Windows' compliance with Article 6(9) of the DMA, Windows Required Service Data is ephemeral and consequently cannot be made portable and exported. Even when data is retained after processing Required Service Data, the Required Service Data typically does not indicate which software caused Windows to send it to Microsoft. Consequently, this data is not part of the Business User Data because it cannot be

198 *See* App Developer Agreement.

199 *See, e.g.*, Analyze app performance.

200 *See* Windows Desktop Application Program.

correlated to a specific business user and there is no Required Service Data that must be made available to business users under Article 6(10) of the DMA.

452. **Cybersecurity Protection Data.** As described above in relation to Windows' compliance with Article 6(9) of the DMA, Microsoft limits the portability of certain data directly from Defender Security Services to protect the cybersecurity of Microsoft users. Defender Security Services collect data to monitor from Windows via publicly-documented APIs and business users can collect the same data from software installed on an end user's PC with the end user's consent.

453. **On-Device Data.** The categories of data described above cover data that Microsoft collects from Windows PCs. Windows stores some data on the PC when applications run on Windows and some of this data may be Business User Data subject to Article 6(10) of the DMA. Windows typically makes this information available to third party applications through publicly documented APIs. For example, Windows writes information to the "Event Log" when errors occur, including some errors caused by third-party applications, and Windows provides an API for applications to read from the Event Log.[201] As described above in relation to Windows' compliance with Article 6(9) of the DMA, Diagnostic Data is also available as "On-Device Data" through the DDV and related API.

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[202]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

454. None.

b) when the measure was implemented;

455. None.

c) the scope of the measure in terms of the products/services/devices covered;

456. None.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

457. None.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities,

201 *See* About Event Logging.

202 For example, this may be particularly relevant to illustrate changes impacting user journeys.

parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

458. None.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[203] consent forms,[204] warning messages, system updates, functionalities available, or customer journey to access functionalities[205]);

459. None.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

460. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

461. None.

i) any consultation[206] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this

---

203 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

204 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

205 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

206 This information should include a description of the methodology for the consultation.

context and a high-level description of the topic of the consultation with those users/parties;

462. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

463. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing open standards and/or state of the art implementations and the reasons for not choosing them;

464. None.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

465. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

466. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

467. None.

o) any type of market analysis or testing (in particular A/B testing[207]), business user surveys or consumer surveys or end user consent rates,[208] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[209]

468. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[210]

469. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are *'effective in achieving the objectives of this Regulation and of the relevant obligation'*, as required by Article 8 of Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

470. None.

r) any relevant data[211] which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch,

---

207 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

208 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

209 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

210 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

211 Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;

471. None.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

472. None.

t) where applicable, when compliance requires granting third parties current sign-in practices (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

473. None.

Regarding Article 6(11)

474. Microsoft refers to **Section 2.3** below.

Regarding Article 6(12)

475. Microsoft refers to **Section 2.3** below.

Regarding Article 6(13)

2.1.1. The following statement confirming compliance with the obligation in line with Article 8(1) of Regulation (EU) 2022/1925:

476. Microsoft confirms that as of the date of this report it has ensured compliance with the obligation laid down in Article 6(13) of the DMA, as applicable to Windows, by the compliance deadline of 7 March 2024.

2.1.2. An exhaustive explanation of how the Undertaking complies with the obligation, including any supporting data[212] and internal documents. Please provide a detailed description of any measures that ensure such compliance, indicating whether such measures were already in place pre-designation or if they were implemented post-designation.

The description of all the above-mentioned measures must enable the Commission to verify whether the Undertaking has demonstrated compliance pursuant to Article 8(1) of Regulation (EU) 2022/1925 and should, at a minimum, include:

i) an explanation on how the Undertaking complies with the obligation based on all measures that were already in place pre-designation or that the Undertaking has implemented post-designation, and

477. Article 6(13) of the DMA provides: "[t]*he gatekeeper shall not have general conditions for terminating* the *provision of a core platform service that are disproportionate. The gatekeeper shall ensure that the conditions of termination can be exercised without undue difficulty*."

478. Windows is commonly licensed with a PC and subject to a perpetual license. Nearly all consumers obtain Windows in this way and most commercial customers do as well. Perpetual licenses are not terminated, and thus Article 6(13) of the DMA does not impact the commercial terms by which Microsoft provides Windows to customers.

479. There are other programs that are directed at commercial customers, by which Microsoft makes Windows available to users on a subscription or consumption basis.

480. Depending on the customers' profile and purchasing selections, customers can terminate a subscription by canceling the subscription through the Microsoft 365 admin center, by turning off recurring billing for the subscription (in which case the customer can use the subscription until it expires at the end of the subscription term), or by closing their account with Microsoft.[213] In some cases, the customer will receive a prorated credit or refund. Under standard terms, the customer can avoid further charges for the terminated subscriptions at the next contracted billing cycle.

---

212 The Undertaking shall have any underlying raw data ready to be made available to the Commission in the event the Commissions requests this raw data.

213 *See* Cancel your subscription in the Microsoft 365 admin center.

481. These termination provisions are all proportional to the programs to which they apply and are not unduly difficult to exercise. And every customer has the option of acquiring Windows with their PC through a perpetual license.

482. This was true before the DMA was adopted, is the same wherever Windows is available, and no change was necessary to comply with Article 6(13) of the DMA.

ii) specific information (including, if applicable, data points, visual illustrations and recorded demos[214]) for each measure implemented in the context of Regulation (EU) 2022/1925, regarding:

a) the relevant situation prior to the implementation of the measure and how the newly introduced measure ensures compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925;

483. None.

b) when the measure was implemented;

484. None.

c) the scope of the measure in terms of the products/services/devices covered;

485. None.

d) the geographic scope of the measure (e.g., if the implementation of the measure extends beyond the EEA, please specify);

486. None.

e) any technical/engineering changes that were made in connection with the implementation of the measure concerned (e.g., on data flows and internal data usage policies, security aspects, tracking of new metrics, Application Programming Interfaces (APIs), operation system (OS) functionalities, parameters of ranking algorithms and methodologies used to rank, classify or make results more prominent, or parameters of online advertising auctions);

487. None.

f) any changes to the customer experience made in connection with the implementation of the measure concerned (e.g., changes in the customer interface, choice screens,[215] consent forms,[216] warning messages, system

---

214 For example, this may be particularly relevant to illustrate changes impacting user journeys.

215 For instance, the specific design of the choice screen, what information is prompted to the users in the choice screen, including the consequences of making a selection; the users to which the choice screen is shown and when.

216 This applies to all types of consent required under Regulation (EU) 2022/1925, regardless of whether this is via a "form" or any other format.

updates, functionalities available, or customer journey to access functionalities[217]);

488. None.

g) any changes to (i) the remuneration flows in connection with the use of the Undertaking's core platform service (e.g. fee structure, level of the fees, revenue share for the relevant service(s), introduction of new fees, provisions and practices related to the business users' pricing policy, other remuneration flows between the Undertaking and the business users or end users, as applicable) and (ii) the other terms and conditions provided to end users and business users (or individually negotiated agreements with business and/or end users), or where applicable, changes to existing terms and conditions, required by the implementation of the measure concerned (e.g. privacy policy, conditions for access and interoperability and any other relevant clauses);

489. None.

h) any other relevant changes made in connection with the implementation of the measure concerned not covered by points e) to g) above;

490. None

i) any consultation[218] with end users, business users and/or any interested parties that has been carried out in the context of (i) the elaboration of the measure and/or (ii) the implementation of the measure, and how the input of these consulted parties has been taken into account. Provide a list of end users, business users and/or any interested parties consulted in this context and a high- level description of the topic of the consultation with those users/parties;

491. None.

j) any involvement of external consultants in the elaboration of the measure, including a description of the consultants' mission, whether they are independent from the Undertaking, a description of both their output and the methodology used to reach that output and, if applicable, an explanation of the reasons why the recommendations made by the external consultants were not followed;

492. None.

k) any alternative measures whose feasibility or implications has been assessed and the reasons for not choosing them and, in particular, where relevant (e.g., interoperability), the results of the evaluation of existing

---

217 The Undertaking must provide a click-by-click description of the end user's interaction with the user interface. The Undertaking may submit visual illustrations and/or recorded demos.

218 This information should include a description of the methodology for the consultation.

open standards and/or state of the art implementations and the reasons for not choosing them;

493. None.

l) any action taken to inform end users and/or business users of the measure, their feedback; and any changes to the measure implemented on the basis of this feedback;

494. None.

m) where applicable, the interaction with measures the Undertaking has implemented to ensure compliance with other obligations under Regulation (EU) 2022/1925;

495. None.

n) where applicable, all actions taken to protect integrity, security or privacy (e.g., data access, data retention policies) pursuant to the relevant provisions in Regulation (EU) 2022/1925 and why these measures are strictly necessary and justified and there are no less restrictive means to achieve these goals;

496. None.

o) any type of market analysis or testing (in particular A/B testing[219]), business user surveys or consumer surveys or end user consent rates,[220] that have been carried out to estimate the expected impact of the measure on the objectives of Regulation (EU) 2022/1925;[221]

497. None.

p) any type of market analysis or testing (in particular A/B testing), business user surveys or consumer surveys or end user consent rates, that have been or are expected to be carried out to evaluate the actual impact or

---

219 A/B testing is an experiment where the audience is randomly split to test a number of variations of a measure and determine which performs better. A/B testing and consumer surveys may be particularly well-suited to demonstrate: (i) compliance with obligations which include a change to an end-user interface and (ii) the absence of dark patterns, which could jeopardize the effectiveness of the proposed measure.

220 End user consent rates refer to the percentage of end users who provided consent to the data processing for which end user consent is required under Regulation (EU) 2022/1925 (for instance Articles 5(2) and 6(10)).

221 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

evolution of the impact of the measure on the objectives of Regulation (EU) 2022/1925;[222]

498. None.

q) a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the relevant obligation', as required by Article 8 of Regulation (EU) 2022/1925, including an explanation why the Undertaking considers these indicators to be the most suitable;

499. None.

r) any relevant data[223] **which can inform whether the measure is or will be effective in achieving the objectives of Regulation (EU) 2022/1925, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc. Provide an exact definition of the terms used and a detailed calculation explanation;**

500. None.

s) any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools;

501. None.

t) where applicable, when compliance requires granting third parties (e.g., business users), access to data, interfaces or other technical features of the service: describe the procedure for third parties to obtain such access (including how third parties will be informed of this possibility), the scope (including terms and conditions attached to the access), the format, and the frequency (e.g. real time) and any other relevant information (e.g. whether the shared data/interface or other technical feature can be independently audited, data access policies, data retention policies and measures to enable secure data access).

502. None.

---

222 The full methodology for any analysis, testing or survey shall be included in the Compliance Report.

223 Reported on a sufficiently disaggregated basis to be informative (for example, by reference to each business user) and, if applicable, per type of device.

Regarding Article 7

503. Microsoft refers to **Section 2.3** below.

2.1.3. A detailed explanation of how the Undertaking has assessed compliance with the obligation, including whether any assessment projects, such as external or internal audits have been carried out. For all such assessment projects, provide information about the identity and the role of the people involved and whether they are independent from the Undertaking, the assessment methodology and timeline for the relevant assessment project, and any output (e.g., audit reports or compliance plans).[224]

504. From 6 September 2023, Microsoft has taken steps to assess and assure compliance with the obligations and restrictions imposed by the DMA. Under Article 28 of the DMA, Microsoft established its DMA Compliance Function, and identified a senior manager as its Head of the Compliance Function. Microsoft also created a DMA Management Body, including senior corporate executives, including Microsoft's President and Vice Chair, the Executive Vice President responsible for Windows, and the Chief Executive Officer of LinkedIn, to ensure proper oversight and execution of Microsoft's obligations.

505. As authorized by the Management Body, and with the support of engineering and business teams, Microsoft's Compliance Function is implementing monitoring and oversight measures to ensure that Microsoft's designated CPSs are compliant with the DMA. Microsoft has identified and appointed Directly Responsible Individuals ("**DRIs**") for each applicable DMA obligation across both Windows and LinkedIn. The DRIs are responsible for implementing required changes to each CPS and monitoring to ensure that each CPS remains in continuous compliance with the DMA. The DRIs will be asked by the Compliance Function to attest that they have met their responsibilities on a routine basis. The Compliance Function meets regularly with all DRIs and maintains an ongoing engagement rhythm with other key stakeholders, including Microsoft's Management Body, in connection with its responsibilities under Article 28.

506. Microsoft has also created a DMA Compliance website – https://www.microsoft.com/en-us/legal/compliance/dmacompliance – with information about its DMA compliance program, which includes a link to the public version of Microsoft's compliance report and an escalation point to receive feedback from interested parties both inside and outside Microsoft. This feedback mechanism will supplement Microsoft's internal compliance efforts and, Microsoft expects, will provide valuable insight and perspective on Microsoft's compliance with the DMA.

507. Microsoft has also developed DMA-related training and Q&A sessions for Microsoft personnel, tailored to roles and responsibilities.

[224] Microsoft includes information in this submission annex for **Sections 2.1.3-2.1.5**, in line with the instructions in the Commission's compliance report template under Article 11 of the DMA. Microsoft, however, notes that these sections in particular fall under the Microsoft Compliance Function's realm and supervision.

2.1.4. A list and description of any reports prepared by the head of the compliance function for the management body of the Undertaking in relation to Regulation (EU) 2022/1925 and, in particular, on risks of non-compliance within the meaning of Article 28(4) of Regulation (EU) 2022/1925 and of the management body's replies to those reports, including a list and description of the measures taken in response to those reports.

508. The Microsoft Management Body convenes as often as is necessary, but on at least a quarterly basis, to monitor and assess Microsoft's compliance with the DMA. The Microsoft Management Body is planning to produce detailed reports updating the Management Body on Microsoft's compliance with the DMA. Whereas none such detailed report has been produced to date, Microsoft provides for completeness the following table with presentations by the Head of the Compliance Function to the Management Body, as of the date of this compliance report. These relate to both CPSs and all applicable obligations.

Table 1. Presentations By The Microsoft Compliance Function To The Management Body

24 October 2023 Management Body Meeting	
Presentation Prepared By The Head Of The DMA Compliance Function	**The Management Body's Actions**
PowerPoint Presentation The presentation explained the law's requirements to set up a DMA Compliance Function and a Management Body, the role and reporting structure of the Compliance Function, and resolutions to be adopted in the meeting. The Management Body also reviewed the planned timeline for meetings of the Management Body, and the Compliance Function's path to the creation of Microsoft's compliance report under Article 11 of the DMA. The Compliance Function also informed the Management Body about Deloitte's independent audit of Microsoft's description of its consumer profiling techniques, required by Article 15 of the DMA.	At this meeting, the Management Body: • Reviewed and discussed several proposed resolutions. • Unanimously approved and adopted the proposed resolutions. • Reviewed and discussed the Mission Letter for the Head of the Compliance Function. • Unanimously approved the Mission Letter for the Head of the Compliance Function.
Minutes of the Meeting The Compliance Function tracked each discussion and decision of the Management Body at the meeting, and produced the minutes of the meeting. The meeting minutes reflect the Management Body's review and approval of three resolutions, including the creation and empowerment of the Management Body, the creation and empowerment of the DMA Compliance Function, and the roles and	As stated below, the Management Body reviewed and approved the 24 October 2023 Meeting Minutes, during its 2 February 2024 Management Body meeting.

responsibilities of the Head of the Compliance Function and the DMA Compliance Officers.	
2 February 2024 Management Body Meeting	
Presentation Prepared By The Head Of The DMA Compliance Function	**The Management Body's Actions**
PowerPoint Presentation In this presentation, the 24 October 2023 Meeting Minutes were presented for the Management Body's review and consideration. The presentation also provided an update on Microsoft's DMA compliance status and progress, as well as Microsoft's readiness for the March 2024 compliance report under Article 11 of the DMA. The Management Body was also presented with Microsoft's strategies and policies for taking up, managing, and monitoring compliance with the DMA, as required by DMA Article 28(8). After a discussion of these strategies, the Management Body considered a resolution to approve these strategies, which included the: • Establishment of Microsoft's DMA Compliance Function; • Identification of DRIs; • Creation of DMA Compliance reporting and feedback intake mechanisms; • Changes of and additions to, where necessary, terms and conditions in agreements related to each CPS; • DMA Compliance related modifications of Windows and LinkedIn; • Development of DMA-related training; • Establishment of engagement rhythm requirement with key stakeholders; and • Planning for additional mechanisms to ensure ongoing compliance after the compliance deadline.	At this meeting, the Management Body: • Reviewed, approved, and adopted the Meeting Minutes from the 24 October 2023 Management Body Meeting; • Reviewed and discussed Microsoft's DMA compliance progress and readiness for the March 2024 compliance report under Article 11 of the DMA; • Reviewed and discussed Microsoft's strategies and policies for taking up, managing, and monitoring compliance with the DMA, as required by DMA Article 28(8); • Unanimously approved and adopted Microsoft's strategies and policies, as well as the accompanying resolution, to take up, manage, and monitor compliance with the DMA.
Minutes of the Meeting The Meeting Minutes for the 2 February 2024 Management Body Meeting have not been created or approved as of the compliance deadline. The Meeting Minutes will be prepared before the next meeting of the Management	None to date.

Body, and will be presented to the Management Body for its review, comment, and potential approval at that next meeting.	

Source: Microsoft

2.1.5. A list and a summary of any feedback (e.g., complaints) of the Undertaking's business users established in the Union or end users established or located in the Union concerning the Undertaking's compliance with the obligations. Where this feedback exceeds ten (10) instances, please group them to the extent possible (e.g., per topic). Please also provide an explanation of any action that the Undertaking has taken based on this feedback.[225]

509. Microsoft has not received feedback responsive to this section concerning either Windows' or LinkedIn's compliance with the DMA obligations in the reporting period between 6 September 2023 and the compliance deadline, reflecting the fact that Microsoft was not required to comply with the DMA before the compliance deadline.

2.2. A list of the Undertaking's core platform service's top fifteen (15) business users per core platform service based on revenues established in the EEA for the last year, as defined in Article 2, point (21) of and in the Annex to Regulation (EU) 2022/1925, and, for these business users provide: the name, address, telephone number and e-mail address of the head of their legal department (or other person exercising similar functions; and in cases where there is no such person, the chief executive officer).[226] If revenues are not available or do not represent a suitable measure, please provide a list of top business users based on an alternative relevant proxy and explain why it is the most relevant one to assess the importance of business users for the specific core platform service.

510. Business users are developers of applications for Windows. Windows is an open platform. Business users can distribute their applications on Windows for free and without notifying Microsoft, and the most popular applications on Windows do so. Microsoft allows, but does not require, business users to distribute their applications through the Microsoft Store, and Microsoft makes revenue from those business users. The most used applications on Windows, however, and those likely to have the most revenue associated with them, are not distributed through the Microsoft Store.

511. Microsoft has identified the requested top fifteen business users based on the highest number of applications installed on Windows PCs in the EEA as of January 2024. Microsoft provides contact details for these business users at confidential **Annex – Windows – 1**. This list includes unique third-party business users. Microsoft does not have access to their non-public revenue information.

---

225 The Undertaking should ask about and respect the decision of the company submitting feedback to preserve the anonymity of its submission or to keep certain parts confidential. The Undertaking should inform the Commission of any such anonymity or confidentiality requests. In any case, the Undertaking should describe any actions taken based on the relevant feedback in a non-confidential form.

226 Please use the "eRFI contact details template" on the DMA website: https://digital-markets-act.ec.europa.eu/about-dma/practical-information_en#templates.

512. Because applications can distribute on Windows without providing any contact information, Microsoft does not have an official contact internally. Microsoft obtained contact information for these business users from public sources.

2.3. If applicable, the reasons why the Undertaking considers that a specific obligation laid down in Articles 5 to 7 of Regulation (EU) 2022/1925 cannot by nature apply to the Undertaking's relevant core platform service (i.e., because it is clear from the text of Regulation (EU) 2022/1925 that a specific obligation does not apply to a core platform service). For the avoidance of doubt, this section does not cover situations governed by Articles 9 or 10 of Regulation (EU) 2022/1925.

513. Microsoft sets out below the DMA obligations that, by nature, do not apply to operating systems and thus to Windows. As a result, Windows is not subject to the obligations in Articles 5(3), 5(9), 5(10), 6(5), 6(8), 6(11), 6(12), and 7 of the DMA.

514. **Article 5(3)** is a provision that applies to online intermediation services, which are defined by Article 2(2) of Regulation 2019/1150 as:[227]

> "services which meet all of the following requirements:
>
> *(a) they constitute information society services within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (12);*
>
> *(b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers."*[228]

515. Windows is not an online intermediation service, and therefore this provision does not apply to Windows.

516. **Article 5(9)** requires reports to advertisers to which Microsoft provides online advertising services. Microsoft does not provide online advertising services through Windows, and therefore this provision does not apply to Windows.

517. **Article 5(10)** requires reports to publishers to which Microsoft provides online advertising services. Microsoft does not provide online advertising services through Windows, and therefore this provision does not apply to Windows.

518. **Article 6(5)** relates to "ranking" of the gatekeeper's first-party services and products to similar third-party services and products. "Ranking" is defined by Article 2(22) of the DMA as "*the relative prominence given to goods or services offered through online*

---

227 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services; OJ L 186, 11 July 2019, pp. 57–79.

228 For the purposes of this definition, Article 1(1)(b) of Directive (EU) 2015/1535 defines information society services as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.*"

intermediation services, online social networking services, video-sharing platform services or virtual assistants, or the relevance given to search results by on line search engines as presented organized or communicated by the undertaking providing online intermediation services, online social networking services, video-sharing platform services, virtual assistants or online search engines, irrespective of the technology means used for such presentation, organization or communication and irrespective of whether only one results is presented or communicated."

519. Windows is an operating system and not an online intermediation service, online social networking service, video-sharing platform service, or online search engine and so it does not engage in "ranking" as defined by the DMA. Therefore, Article 6(5) does not apply to Windows.

520. **Article 6(8)** requires that Microsoft provide advertisers and publishers with certain performance measuring tools and certain data. Windows is not a platform for advertisers and publishers. Therefore, Article 6(8) does not apply to Windows.

521. **Article 6(11)** applies to online search engines. Article 2(6) of the DMA defines online search engines by reference to Article 2(5) of Regulation (EU) 2019/1150[229] that defines an online search engine as "*a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found*."

522. Windows is not an online search engine but an operating system. Therefore, Article 6(11) does not apply to Windows.

523. **Article 6(12)** applies to software application stores,[230] online search engines, and online social networking services.

524. Windows is not a software application store, online search engine, or online social networking service. Therefore, Article 6(12) does not apply to Windows.

525. **Article 7** applies to number-independent interpersonal communication services. Windows is not a number-independent interpersonal communication service but an operating system. Therefore, Article 7 does not apply to Windows.

---

229 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services; OJ L 186, 11 July 2019, pp. 57–79.

230 Article 2(14) DMA defines "software application stores" as "*a type of online intermediation services, which is focused on software applications as the intermediated product or service.*"

Declaration

Microsoft, as a gatekeeper, declares that, to the best of its knowledge and belief, the information given in this submission is true, correct, and complete, that all estimates are identified as such and are its best estimates of the underlying facts, and that all the opinions expressed are sincere.

Name: Christopher Nelson

Organisation: Microsoft Corporation

Position: Associate General Counsel / Head of DMA Compliance Function

Address: One Redmond Way, Redmond, WA 98052, United States of America

Phone number: +1 425-882-8080

E-mail: [CONFIDENTIAL]

Date: 05 March 2024

Signature: