Data Protection Impact Assessment (DPIA) – Microsoft CoPilot 365

Document Name	Data Protection Impact Assessment – CoPilot 365
Author or Owner (name and job title)	Chris Yacomine (Senior Product Owner)
Department or Team	DDAT
Document Status	Draft
Version Number	0.1
Release Date	
Approver (if applicable)	
Review Date	
Distribution	Internal

Guidance for completing this DPIA template

- If you're unsure whether you need to complete a DPIA, use the Screening assessment - do I need to do a DPIA? first to help you decide.

- **Must** and **should** are used throughout the guidance notes in this template to help you understand which things are a legislative requirement and **must** be done versus things that the ICO considers **should** be done as best practice to comply effectively with the law.

- You **must** complete this DPIA template if your screening assessment indicates a DPIA is required.

- You **should** aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you won't be able to continue with your plans without changing them, or at all.

- We recommend that you fill out each section of this template in order, as each subsequent section builds upon the last. You will not be able to complete later sections correctly if you skip ahead. You **should** read the guidance notes throughout this template to help you with each section.

- If you are struggling with completing this template the Information Management and Compliance Service is available to provide advice and support. Please keep in mind their service standards if you require help.

1. Data processing overview

1.1. Ownership

Guidance notes:

- There **must** be a clear owner for any residual risk resulting from your data processing. At the ICO our Information Asset Owners (service directors) are our senior risk owners and **must** sign off on your plans.
- We **must** understand our role in relation to the personal data being processed. Our obligations will vary depending on whether we are a controller, joint controller or processor.
- If you are procuring a new product or service from a third party, you will typically find information about data protection roles and responsibilities within the service terms and conditions, or any contract being agreed between us and the third party.

Guidance Link: Controllers and processors | ICO

Project Title:	Microsoft CoPilot 365
Project Manager:	Danielle Haslehurst (DH)
Information Asset Owner:	ICO - Director of Digital IT
Controller(s):	ICO
Data processor(s):	Microsoft

1.2. Describe your new service or process

Guidance notes:

- Provide a summary of the service or process you want to implement. Include any relevant background information and your key aims and objectives.

We are looking to activate Microsoft CoPilot for 365 across our existing 365 product suite – Teams, Outlook, Word, Excel, PowerPoint, Notes, etc. This tool effectively adds a feature to these existing products, allowing the user to use Generative AI to ask questions, summarise documents, help write content, create basic slides and presentations amongst many other things.

This DPIA is intended to cover the use of Microsoft CoPilot for 365 specifically for a pilot phase, comprising circa. 30 users with close contact and feedback from our Senior Product Owner(s) and a project team. Should the proof of concept prove viable, and our pilot show a good potential for rollout across a larger group across the organisation, this DPIA will be revisited and revised accordingly.

A brief overview of Microsoft Copilot 365 is available here: Microsoft Copilot for Microsoft 365 overview | Microsoft Learn (Appendix 2) and Microsoft have made available information about Data, Privacy and Security for Coilot for 365 (Appendix 3).

A more detailed overview, which specifically covers key GDPR considerations, is provided in Microsoft GDPR and Generative AI - A Guide for the Public Sector (see Appendix 7).

Microsoft Copilot 365 is subject to the same Product Terms, including the Privacy and Security terms (see Appendix 4) and Data Protection Addendum (see Appendix 5) as our wider use of M365, considered in detail in the previously completed Microsoft 365 DPIA.

The purpose of this assessment is to consider any new data protection impact from activating Microsoft CoPilot 365 and the Microsoft Graph that enables it.

In a very basic sense, Microsoft Graph acts like a bridge between Microsoft CoPilot 365 users and their data stored across various Microsoft services. When using Microsoft CoPilot 365, the user generates and interacts with a lot of data like user profiles and preferences, and this data is stored across various Microsoft services like Azure, Office 365, etc.

Microsoft Graph helps Microsoft CoPilot 365 to access and manage this data efficiently. For example, it can fetch user profile information when needed. Microsoft Graph ensures that Microsoft CoPilot 365 works seamlessly with other Microsoft services by managing the data flow between them. This is done while maintaining strict data privacy and security standards, since Microsoft Graph only accesses data it needs and only with the proper permissions.

We are looking to roll this out in a phased approach; we've initially done some internal testing on the tool (i.e. does it work as expected, can we activate this within our existing Azure environment, etc.) And we've now begun to explore what the use cases are and how ICO users will benefit from this and does it justify the investment.

Rollout Plan:
1. Internal Testing (May-June)
2. Internal Pilot with Business Area i.e. Communications Team (July-October)
3. Incrementally roll-out to more ICO Users & Business Areas i.e. Private Office, DDAT, etc. (October onwards)

Potential ICO use cases:

Microsoft Teams: If meeting has transcription turned on, it can review the discussion and summarise the meeting, assign owners and confirm actions. This can remove the manual effort for notetaking for PA's and meeting admins.

Microsoft Word: For communications teams, it can help with generating and forming the first draft of articles, media briefings, digital content, social media, etc.

Microsoft Word: For communications teams, it can help with reviewing documents to ensure they meet our accessibility guidelines and our ICO style guide.

Microsoft Excel: It can help to identify trends and insights in the data and generate reports and graphs from this.

Microsoft Outlook: For any user, it can help summarise the contents of a long e-mail chain. As well as drafting the first draft of replies to e-mails.

1.3. Personal data inventory

Guidance notes:

- We **must** have a clear understanding of the personal data being processed. This is **essential** for identifying and managing risks.
- Use the table below to list each category of personal data being processing. Use a new row for each data category. You can add as many rows to the table as you need.
- Categories of data may not be obvious to you from the outset e.g. tracking data (IP or location) or data collated via cookies and you need to take the time to fully understand the extent of the personal data you will process.
- Your data subjects are the individuals the personal data relates to. For example, these could be members of the public, ICO employees, our contractors etc.
- Recipients will be anyone who the data is shared with.
- UK GDPR restricts transfers of personal data outside of the UK so any overseas transfers **must** be identified.
- Personal data should be kept for no longer than is necessary. You **must** identify a retention period for the personal data you intend to process.

Guidance Link: What is personal data? | ICO

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
ICO Organisational data This is *"Customer data"* as defined in the Product Terms and Data Protection Addendum (Appendix 5). Microsoft Copilot for Microsoft 365 can generate responses from ICO organisational data, such as our user documents, emails, calendar, chats, meetings, and contacts (see Appendix 3.) It will therefore access the wide variety of categories of	ICO employees, members of the public and all stakeholders whose personal data the ICO processes as part of its routine business operations.	Microsoft and their Online Services Subprocessors (Appendix 8). ICO staff as end users of Copilot for 365.	Yes If yes, list the countries the data will be transferred to: *"Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate" See (Appendix 5).*	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained: ICO Organisational data within M365 is subject to the various retention periods detailed in our Retention and Disposal Policy.

personal data contained within the information we currently store in M365. This will likely include both special category and criminal offence data.				
User Interactions with Copilot Users enter prompts into Copilot for Microsoft 365 and data is stored about these interactions. This includes the information contained within prompts, the data they retrieve, and the generated responses. The record of interactions is the user's Copilot interaction history.	ICO staff as end users of CoPilot for 365.	M365 admins via Content Search or Microsoft Purview. ICO staff as end users of CoPilot for 365.	As above.	Other (please specify time period below) Subject to the same 7 day retention policy that applies to Teams Chat Messages. If selecting other, please specify the length of time personal data will be retained:

Usage Data This could include specific actions the user takes within the application, such as the time they log in, the feature/365 product they used, and how often they use the application.	ICO Employees	M365 Admins, Purview Administrators, and a small number of colleagues in DDaT authorised to access the usage report – currently one Senior Product Owner	As above	Other (please specify time period below) Admins can use Microsoft Purview to set retention policies for the data. Audit data is kept for 90 days, and prompts will only be retained for 7 days, as per Teams chat retention period. Usage data reports are retained in the CoPilot dashboard for 30 days.

1.4. Lawful basis for processing

Guidance notes:

- To process personal data, you **must** have a lawful basis. Select a lawful basis for processing the personal data in your inventory from the drop-down lists below.

Guidance Links: Lawful basis for processing and Lawful basis interactive guidance tool

First, select a lawful basis from Article 6 of the UK GDPR.

Article 6(1)(e) - public task

If more than one lawful basis applies to your processing, please list any additional basis here:

Guidance notes:

- If your personal data inventory includes any **special category data,** you **must** identify an additional condition for processing from Article 9 of the UK GDPR.

Guidance link: Special category data

Next, if applicable, select an additional condition for processing from Article 9 of the UK GDPR:

Article 9(2)(g) - reasons of substantial public interest

If you have selected conditions (b), (h), (i) or (j) above, you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018. Please select from the following:

N/A

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of the conditions set out in Part 2 of Schedule 1 of the DPA 2018. Please select from the following:

6. Statutory and government purposes

Guidance notes:

- If you are processing **criminal offence data,** you **must** meet one of the 28 conditions for processing criminal offence data set out in paragraphs 1 to 37 Schedule 1 of the DPA 2018.

Guidance Link: Criminal offence data

Finally, if applicable select an additional condition for processing any criminal offence data:

6. Statutory and government purposes

1.5. Necessity and proportionality

Guidance note:

- You **must** assess whether your plans to process personal data are both necessary and proportionate to you achieving your purpose. You should explain why this is the case below.
- 3 **must** take steps to minimise the personal data you process; processing only what is adequate, relevant and necessary.
- You **should** think about any personal data you can remove without affecting your objective.
- You **should** consider if there's any opportunity to anonymise or pseudonymise the data you're using.

Microsoft CoPilot 365 and Microsoft Graph can help address these concerns in the following ways:

- Necessity and Proportionality: Microsoft CoPilot 365 only processes personal data that is necessary for providing its services. For example, it might process user identification data to provide personalised experiences or usage data to improve the service. Microsoft Graph helps in this process by enabling efficient access to this data across various Microsoft services. The data processed is proportionate to the purpose, i.e. enhancing user experience and improving the service.

- Data Minimisation: Both Microsoft CoPilot 365 and Microsoft Graph adhere to the principle of data minimisation. They process only what is adequate, relevant, and necessary. Unnecessary data is not processed or stored. For instance, Microsoft CoPilot 365 doesn't process personal data that isn't relevant to its functioning, like physical location, unless it's necessary for a specific feature.

- Removing Unnecessary Data: Microsoft has policies in place for regular review and deletion of unnecessary data. If certain data is found to be not contributing to the service or user experience, it can be removed.

- Anonymisation and Pseudonymisation: Wherever possible, Microsoft employs techniques like anonymisation and pseudonymization to protect user data. For example, a unique user ID might be used instead of directly using personal identifiers like name or email. This helps in reducing the risk of data breaches.

We are also looking to create an internal usage AI policy for Microsoft CoPilot 365 and other internal AI products; ensuring that users use it for its intended uses and minimise using personal data where possible.

The SharePoint Online migration will also further help mitigate this, as we will be ensuring that documents and folders have the correct labels and access permissions. CoPilot can only access documents that users already have access to.
We are seeking to increase capacity and efficiency by using automation where possible to allow colleagues to focus their time on more high-value tasks, rather than on manual input or low-value tasks. The necessity for this work has been highlighted to help us to deliver the Enterprise Data Strategy, and the Digital AI and Automation programme, to deliver against the ICO25 objective.

1.6. Consulting with stakeholders

Guidance notes:

- You **should** consult with relevant stakeholders both internally (for example Cyber Security, Legal Services, IT etc.) and externally to help you identify any risks to your data subjects.
- Briefly outline who you will be consulting with to inform your DPIA.
- Where appropriate you **should** seek the views of your data subjects, or their representatives, on your intended processing. Where this isn't possible, you should explain why below.

We are following the new ADA (Architectural Design Authority) process, which includes oversight from a wide range of specialisms, such as: cyber-security, information management, IT and digital infrastructure, product management, architecture, and data teams. This forum will need to approve CoPilot 365 before it can proceed to the pilot phase in the ICO.

2. Personal data lifecycle

Guidance Note:

- You **must** provide a systematic description of your processing from the point that personal data is first collected through to its disposal.
- This **must** include the source of the data, how it is obtained, what technology is used to process it, who has access to it, where it is stored and how and when it is disposed of.
- If your plans involve the use of any new technology, for example a new piece of software, you **must** explain how this technology works and outline any 'privacy friendly' features that are available.
- If helpful you can use the headings provided below to help you construct your lifecycle. You can include a flow diagram if this helps your explanation.

Data source and collection:

Microsoft Copilot 365 accesses content and context through Microsoft Graph, generating responses based on organisational data like user documents, emails, calendar, chats, meetings and contacts. All of which will have been collected from a wide variety of sources.

All user prompts to Copilot and responses from Copilot are stored as a record of interactions in the user's Copilot interaction history and can be deleted by the user or admins. See Data, Privacy, and Security for Microsoft Copilot for Microsoft 365 | Microsoft Learn (Appendix 3) and Search for and delete Microsoft Copilot for Microsoft 365 data | Microsoft Learn (Appendix 9).

Technology used for the processing:

Microsoft Copilot for Microsoft 365 utilises large language models (LLMs), content in Microsoft Graph and integrates with Microsoft 365 productivity apps like Word, Excel, PowerPoint, Outlook and Teams to provide outputs to the end user. See Microsoft Copilot for Microsoft 365 overview | Microsoft Learn (Appendix 2) for a more detailed summary.

Storage location:

Microsoft Copilot 365 uses the Preferred Data Location (PDL) for users and groups to determine where to store data. If the PDL isn't set or is invalid, data is stored in the Tenant's Primary Provisioned Geography location.

Section 31

[redacted]

Section 31 [redacted]

Data Residency for Microsoft Copilot for Microsoft 365 - Microsoft 365 Enterprise | Microsoft Learn (Appendix 10) for more information.

Access controls:

Copilot only uses data that a user already has access to. If a member of staff has access to a file (e.g. they were added to a SharePoint site where a file resides) then Copilot will also have access to it when they ask it prompts. There are existing Microsoft 365 controls that offers multiple protections such as blocking harmful content, detecting protected material and preventing prompt injections. These measures should help ensure the security and integrity of our data. See Data, Privacy, and Security for Microsoft Copilot for Microsoft 365 | Microsoft Learn (Appendix 3).

Data sharing:

The information contained within prompts to Microsoft CoPilot for 365 and the data they retrieve along with the generated responses remain within our existing Microsoft 365 service boundary. As such use of the Microsoft Copilot for 365 service shouldn't see any data shared with any parties outside of the ICO, other than Microsoft and their sub processors (see Appendix 8) as per the existing M365 Online Service Terms (see Appendix 4), Data Protection Addendum (see Appendix 5).

Disposal:

All user prompts to Copilot and responses from Copilot are stored as a record of those interactions in the user's Copilot interaction history and can be deleted by the user or admins.

Microsoft Copilot 365 can retain and delete messages for compliance reasons, including user prompts to Copilot and Copilot responses to users. It is possible to discover prompts, if perhaps there is a data breach, or an investigation needs to happen, or there is a safeguarding concern (including Prevent). It is possible for administrators to use Microsoft Purview to help with investigations. Further details available at this link: Search for and delete Microsoft Copilot for Microsoft 365 data | Microsoft Learn (See Appendix 9). User prompts will be retained for 7 days, the same as Teams Chat Messages.

Retention policies and retention labels are essential for managing data lifecycle in Microsoft 365, allowing the ability to retain or delete content as needed. Retention settings can be applied to various Microsoft 365 services, including Exchange, SharePoint, OneDrive, Teams and Viva Engage. CoPilot 365 can only access data that is still available and has not been permanently deleted due to the retention policy on a specific app. For example, if a retention policy is set to delete Teams chats after a certain period, CoPilot 365 will not be able to access those chats once they have been deleted. Retention policies can be adaptive or static, and they can be applied at the container level (e.g. SharePoint sites, Exchange mailboxes) or the item level (e.g. individual files or emails). Further detail available at Learn about retention for Microsoft Copilot for Microsoft 365 | Microsoft Learn (see Appendix 10).

3. Key UK GDPR principles and requirements

Guidance notes:

- Answering the questions in this section will help you comply with essential data protection requirements.
- You may identify specific actions that are needed and you should add these to your list of DPIA outcomes in section 6.0.

3.1. Purpose and Transparency

Guidance notes:

- In most cases you will need to communicate essential information about your data processing to your data subjects. A privacy notice is the most common way of doing this.
- You **must** review the existing privacy notice on the ICO website. If your data processing involves the personal data of ICO staff, review our Staff Privacy Notice on Iris.
- You need to decide if our existing privacy notices sufficiently cover your plans. If not, you **must** get them updated or you **must** provide your data subjects with a separate, bespoke privacy notice.

Q1. How will you provide your data subjects with information about your data processing?

The existing privacy notice already covers my planned processing.

Guidance notes:

- If you identified consent as your lawful basis for processing in section 1.4 you **must** maintain appropriate records of the data subjects consent.

Guidance Link: Consent

Q2. Are you satisfied you're maintaining appropriate records of data subjects' consent?

N/A - no processing based on data subjects consent

Guidance notes:

- If you identified legitimate interests as your lawful basis for processing in section 1.4 you **should** complete a Legitimate Interests Assessment (LIA). We have a template LIA available.

Guidance Link: How do we apply legitimate interests in practice?

Q3. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

N/A - no processing based on legitimate interests lawful basis

If applicable, please provide a link to your completed assessment.

3.2. Accuracy

Guidance notes:

- All reasonable steps should be taken to ensure personal data is kept accurate and up to date. Steps **must** be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

Q4. Are you satisfied the personal data you're processing is accurate?

Yes

Q5. How will you ensure the personal data remains accurate for the duration of your processing?

Microsoft CoPilot for 365 leverages our existing organisational data and only accesses data that is still available and has not been permanently deleted. Responsibility for maintaining the accuracy of the data it utilises would remain with the existing data owners, as per their current practices.

3.3. Minimisation, Retention and Deletion

Guidance notes:

- You should only collect and hold the minimum amount of personal data you need to fulfil your purpose. Data should be retained for no longer than is needed for that purpose and then deleted without delay.

Q6. Have you done everything you can to minimise the personal data you're processing?

Yes

Q7. How will you ensure the personal data are deleted at the end of the retention period?

See section 2 above. For all personal data contained within our organisational data in M365 existing processes for the deletion of that data at the end of its retention period would be relied upon.

Q8. Will you need to update the ICO retention and disposal schedule?

Yes

3.4. Security: Confidentiality, integrity and availability

Guidance notes:

- Personal data **must** be processed in a way that ensures it is appropriately secure and protected from unauthorised access, accidental loss, destruction or damage.
- You **must** make sure access to the personal data is limited to the appropriate people and ensure you're confident the processing system being used is secure.

Guidance link: A Guide to Data Security

Q9. Where will the personal data be stored and what measures will you put in place to maintain confidentiality, integrity and availability?

See above explanation in Section 2 and relevant appendices for security assurance.

Q10. Have you confirmed there are appropriate access controls to keep the personal data secure?

Yes

Q11. Has the cyber security team completed a security assessment of your plans?

No

Q12. If yes what was the outcome of their assessment?

Section 31

[redacted]

Q13. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

When we move beyond pilot phase, we will onboard new licensees with training materials in the form of slides, which link to additional resources on Microsoft's website too. There will be information around how to contact us if there are any bugs, issues or improvements required. And we are in the process of writing an internal AI fair usage / acceptable usage policy, which will be a dependency before we go-live into BAU with the tool.
Training will be developed and delivered by the Product Owner, and will complement change readiness assessments by the Change Manager, which will highlight if there are any particular training needs which may need to be addressed in order to successfully rollout CoPilot.

3.5. Accountability and governance

Guidance notes:

- The accountability principle makes us responsible for demonstrating our compliance with the UK GDPR. We do this by clearly assigning responsibilities for compliance tasks, and by maintaining relevant records relating to our processing activities and decision making.

- Your Information Asset Owner is the risk owner for any residual risk associated with your data processing and **must** sign off this DPIA.

Q14. Is your Information Asset Owner aware of your plans?

Yes

Q15. Will you need to update our article 30 record of processing activities?

No

Q16. If you are using a data processor, have you agreed, or will you be agreeing, a written contract with them?

Yes

3.6. Individual Rights

Guidance Note:

- UK GDPR provides a number of rights to data subjects when their personal data is being processed.

- As some rights are not absolute, and only apply in limited circumstances, we may have grounds to refuse a specific request from an individual data subject. But you **must** be sure your new service or process can facilitate the exercise of these rights and it should be technically feasible for us to action a request if required.

Guidance Link: Individual rights

Q17. Is there a means of providing the data subjects with access to the personal data being processed?

Yes

Q18. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes

Q19. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes

Q20. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes

Q21. Can we extract and transmit the personal data in a structured, commonly used and machine-readable format if requested by the data subject?

Yes

Q22. Can we erase the personal data on receipt of a request from the data subject?

Yes

4. Risk assessment

Guidance Note:

- You **must** use the table below to identify and assess risks to individuals. You can add as many rows to the table as you need.
- **Remember:** we have an **Averse** risk appetite towards compliance risks (see our Risk Management Policy and Appetite Statement for more information).
- You **must** identify measures to reduce the level of risk where possible.
- In the risk description column, you can select from common risks to individuals in the drop-down list provided. Alternatively, you can enter your own risk descriptions if preferred.
- **The drop-down list is not exhaustive**, and you must identify and assess risks within the context of your planned processing.
- Mitigation measures can be existing, i.e. they're already in place and reduce the risk without any further action being needed. Or they're expected i.e. these are additional measures you intend to take before the data processing begins in order to further reduce risk.
- Use the risk scoring criteria in Appendix 1 to score your risks. You **must** score both the impact (I) and probability (P). The expected risk score total is the result of I multiplied by P.
- When considering probability, you should score based on all your mitigation measures having been implemented in order to get an *expected* risk score.

	Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
				Impact	Probability	Total

Section 31

[redacted]

	Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
			Section 31 [redacted]			

Section 31

[redacted]

	Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
			Section 31 [redacted]			

Section 31

[redacted]

	Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
			Section 31			

Section 31

	Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
	Section 31 [redacted]		Section 31 [redacted]			
Section 31 [redacted]						

	Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
			Section 31 [redacted]			

5. Consult the DPO

Guidance Note:

- Once you have completed all of the sections above you **must** submit your DPIA for consideration by the DPIA Forum who will provide you with recommendations on behalf of our Data Protection Officer (DPO). The DPIA process outlines the next steps.

- Any recommendations from the DPOs team will be recorded below and your DPIA will then be returned to you. You **must** then record your response to each recommendation, and then proceed with completing the rest of this template.

	Recommendation	Date	Project Team Response

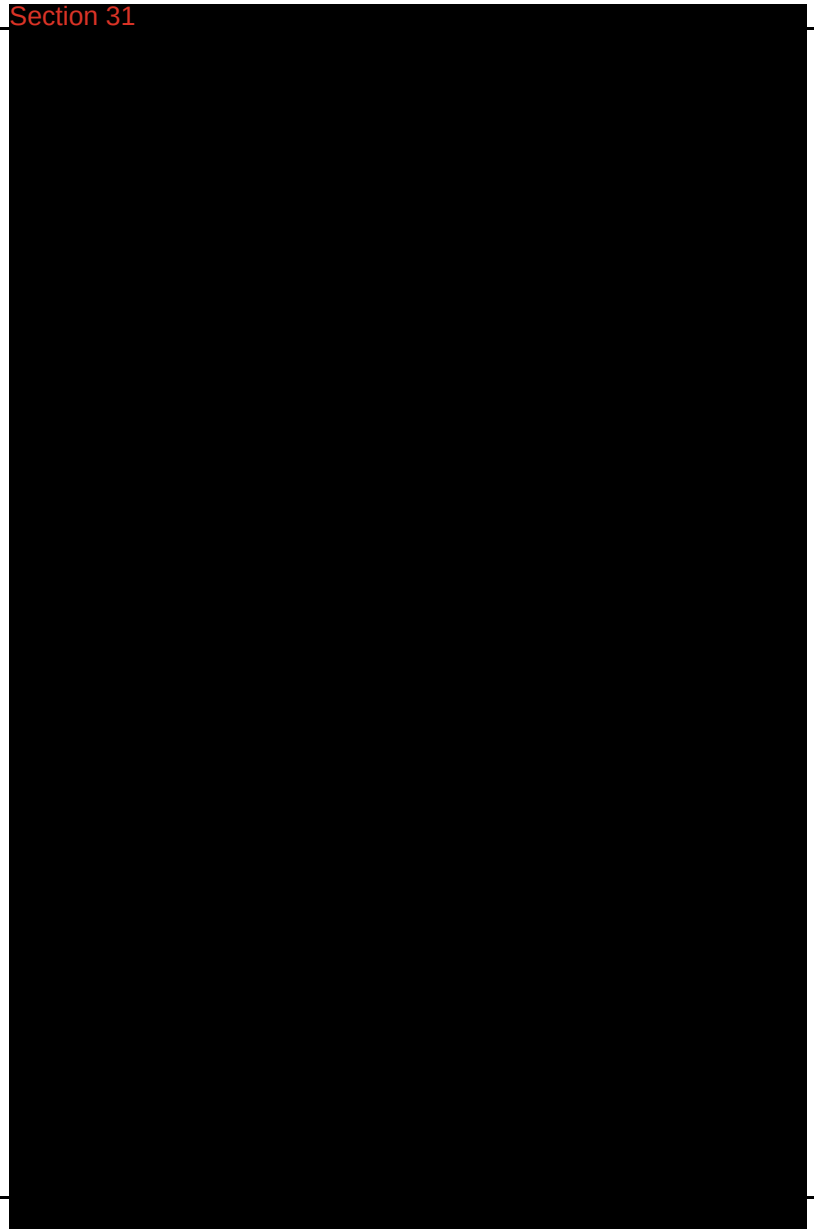
1	The DPIA is currently just a general DPIA about Microsoft CoPilot for 365 and you need to elaborate on your use cases and the ICO's purpose for using it. There are privacy choices you can make on Teams for example and more detail is needed on this. You also need to explain who is responsible for governance of Co-Pilot in general and what choices have been made about its deployment. A governance document is recommended to outline how this will be deployed at the ICO.		Accept Any comments: The functionality of MS CoPilot is continually being adapted and added to by Microsoft, meaning any list of use cases would not necessarily be up to date by the time the DPIA is drafted, completed, nor reviewed, nor is it within the gift of the ICO to be able to determine what is the current 'definitive' use case list in a static document such as this. However, a governance document will be drafted regarding deployment at the ICO, as well as acceptable use policies, and will be owned by the Product Owner. If rejecting DPO recommendations explain why:

	Recommendation	Date	Project Team Response
2	In section 1.3, in relation to usage data you've said recipients will include a small number of colleagues in DDaT. Can you clarify who this will be for example is this users with Purview Access? IT help? Product Owners?	29/08/2024	**Accept** Any comments: 1.3 additions made If rejecting DPO recommendations explain why:

	Recommendation	Date	Project Team Response
3	Section 1.5 Necessity and Proportionality - there is no real explanation of necessity. You need to explain how using CoPilot will benefit the ICO so there is some justification for your processing of personal data.	29/08/2024	**Accept** Any comments: We are seeking to increase capacity and efficiency by using automation where possible to allow colleagues to focus their time on more high-value tasks, rather than on manual input or low-value tasks. Additions made to 1.5 If rejecting DPO recommendations explain why:

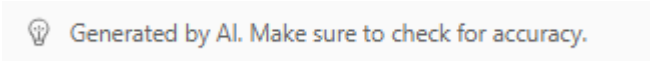
4	Access Controls Section 31 [redacted]	29/08/2024	Accept Any comments: Access permissions across M365 will be set within each of the applications and systems. Mitigations which are already in place for access controls across M365 will be respected, and data could be queried from SharePoint, Exchange, and Teams, as well as PowerBI and Viva Engage. You will only be able to access content within each area which you have express permission to, and for content which is searchable. Section 31 [redacted]

Section 31 [redacted]		If rejecting DPO recommendations explain why:


Section 31

	Recommendation	Date	Project Team Response
	Section 31 [redacted]		

	Recommendation	Date	Project Team Response
5	It's mentioned that it's possible for administrators, via Purview, to discover user prompts, if there is a data breach, or an investigation needs to happen, or there is a safeguarding concern. Please can you clarify whether the 7 day retention applies to data available via Purview and whether prompts are actually retained longer in recycle bins or similar.	29/08/2024	**Accept** Any comments: Additional information provided, including 90-day retention period for audit data via Purview, and 7-day retention period for prompts, which will respect Teams retention. If rejecting DPO recommendations explain why:

6	Accuracy There is limited assurance provided in the DPIA about the accuracy of data across M365. Predominantly the mitigation for this risk is an assumption that it is accurate and we'd suggest more evidence is needed to support this position and effectively score this risk. At present there isn't enough to achieve the current expected risk score of 6 - medium. A high level of confidence in the accuracy of CoPilot outputs is surely needed given some of the potential use cases outlined, and this extends beyond accuracy of personal data. Human review of outputs will be needed and end user guidance will be required so staff are aware of how to review and validate outputs.	29/08/2024	Accept Any comments: The tool offers a health warning when used:  Training for CoPilot 356 will include the need for accuracy as results may not be reliable. If information is pulled from a document, there will be a citation which references back to the source material where you can verify the accuracy of the data. If rejecting DPO recommendations explain why:

	Recommendation	Date	Project Team Response
7	Section 3 Q11 - A security assessment is vital and needs to be done, particularly given the risks with access highlighted.	29/08/2024	**Accept** Any comments: We now have an information security consultant available to conduct such an assessment, and this DPIA has been shared and will be reviewed with that colleague in preparation and support of their security assessment. If rejecting DPO recommendations explain why:

	Recommendation	Date	Project Team Response
8	Section 3 Q13 - it's unclear who is responsible for delivering this training - which team or individuals? It's likely more comprehensive training will be needed beyond a fair usage policy and we'd recommend training needs are given further consideration.	29/08/2024	**Accept** Any comments: This answer has been expanded to address If rejecting DPO recommendations explain why:

6. Integrate the DPIA outcomes

Guidance Note:

- Completing sections 1 to 5 of your DPIA will have helped you identify a number of key actions that you now **must** take to meet UK GDPR requirements and minimise risks to your data subjects. For example, you may now need to draft a privacy notice for your data subjects; or you could have risk mitigations that you need to go and implement.

- You **should** also consider whether any additional actions are required as a result of any recommendations you received from the DPOs team.

- Use the table below to list the actions you need to take and track your progress with implementation. Most actions will typically need to be completed **before** you can start your processing.

Action	Date for completion	Responsibility for Action	Completed Date
Update Retention Schedule	Before processing begins	IM&C Service / Chris Yacomine	
Engage Cyber Security for a security assessment	Before processing begins	Chris Yacomine	
Complete AI fair usage / acceptable usage policy	Ongoing monitoring and assessment	Chris Yacomine	

Action	Date for completion	Responsibility for Action	Completed Date
Use developed tool to produce a report on permissions across SharePoint sites and task site owners with reviewing the permissions on their site.	Ongoing monitoring and assessment	Chris Yacomine	

Action	Date for completion	Responsibility for Action	Completed Date
Deployment of further Retention Labels post EDRM migration	Before processing begins	IM&C	

7. Expected residual risk and sign off by the IAO

Guidance note:

- Summarise the expected residual risk below for the benefit of your IAO. This is any remaining risk **after** you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank.

- If the expected residual risk remains high (i.e. red on the traffic light scoring in the Appendix) then you **must** consult the ICO as the regulator by following the process used by external organisations.

We are keeping initial numbers of trial participants low in order to maintain and monitor strict controls; however, this is new technology for the ICO. We are essentially learning, although we are drawing upon learning from colleagues in Government and other public sector bodies also.

Section 31

[redacted]

7.1 IAO sign off

Guidance Note:

- Your IAO owns the risks associated with your processing and they have final sign off on your plans. You **must** get your IAO to review the expected residual risk and confirm their acceptance of this risk before you proceed.
- Once your DPIA has been signed off it is complete. You should review it periodically or when there are any changes to your data processing.

IAO (name and role)	**Date of sign off**

8. DPIA change history

Guidance note:

- You should track all significant changes to your DPIA by updating the table below.

Version	Date	Author	Change description
V0.1	22/08/2024	Chris Yacomine / Steven Johnston	First Draft
V0.2	30/08/2024	Steven Johnston	DPIA forum recommendations added to section 5 and actions to section 6.
V0.3	23/10/2024	Danielle Haslehurst	Confirmation of scope added, and residual risk explained

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions,

Impact	Scoring criteria
	property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (e.g. does the threat require insider knowledge or significant technical resources to exploit any vulnerability).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur

Probability	Scoring criteria
	For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted, and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: Microsoft CoPilot for Microsoft 365 overview [captured 12/07/2024]

Microsoft Copilot for Microsoft 365 overview

- Article
- 21/06/2024
- 6 contributors

Feedback

In this article

Microsoft Copilot for Microsoft 365 is an AI-powered productivity tool that coordinates large language models (LLMs), content in Microsoft Graph, and the Microsoft 365 productivity apps that you use every day, such as Word, Excel, PowerPoint, Outlook, Teams, and others. This integration

provides real-time intelligent assistance, enabling users to enhance their creativity, productivity, and skills.

Copilot for Microsoft 365 uses a combination of LLMs, a type of artificial intelligence (AI) algorithm that uses deep learning techniques and vast data sets to understand, summarize, predict, and generate content. These LLMs include pre-trained models, such as Generative Pre-Trained Transformers (GPT) like GPT-4, designed to excel in these tasks.

Copilot integration with Graph and Microsoft 365 Apps

Microsoft Copilot for Microsoft 365 is a sophisticated processing and orchestration engine that provides AI-powered productivity capabilities by coordinating the following components:

- Large language models (LLMs)
- Content in Microsoft Graph, such as emails, chats, and documents that you have permission to access.
- The Microsoft 365 productivity apps that you use every day, such as Word and PowerPoint.

Microsoft 365 productivity apps (such as Word, Excel, PowerPoint, Outlook, Teams, loop, and more) operate with Copilot to support users in the context of their work. Some of these features are detailed in the following table:

Expand table

Microsoft 365 App	Feature	Description
Word	Draft with Copilot	Generate text with and without formatting in new or existing documents. Word files can also be used for grounding data
	Chat	Create content, summarize, ask questions about your document, and do light commanding via Chat.
PowerPoint	Draft with Copilot	Create a new presentation from a prompt or Word file, leveraging enterprise templates. PowerPoint files can also be used for grounding data
	Chat	Summary and Q&A
	Light commanding	Add slides, pictures, or make deck-wide formatting changes.

Microsoft 365 App	Feature	Description
Excel	Draft with Copilot	Get suggestions for formulas, chart types, and insights about data in your spreadsheet.
Loop	Collaborative content creation	Create content that can be collaboratively improved through direct editing or refinement by Copilot.
Outlook	Coaching tips	Get coaching tips and suggestions on clarity, sentiment, and tone, along with an overall message assessment and suggestions for improvement.
	Summarize	Summarize an email thread to help the user quickly understand the discussion.
	Draft with Copilot	Pull from other emails or content across Microsoft 365 that the user already has access to.
Teams	Chat	Users can invoke Copilot in any chat. Copilot can summarize up to 30 days of the chat content prior to the last message in a given chat. Copilot uses only the single chat thread as source content for responses and can't reference other chats or data types (for example, meeting transcripts, emails, and files). Users can interact with Copilot by selecting pre-written prompts or writing their own questions. Responses include clickable citations that direct users to the relevant source content that was used. Conversations with Copilot take place in a side panel that allows users to copy and paste. Copilot conversations will disappear after the side panel is closed.
	Meetings	Users can invoke Copilot in meetings or calls within the same tenant. Copilot will use the transcript in real-time to answer questions from the user. It only uses the transcript and knows the name of the user typing the question. The user can type any question or use pre-determined prompts; however, Copilot will only answer questions related to the meeting conversation from the transcript. The user can copy/paste an answer and access Copilot after the meeting ends on the Recap page.
	Copilot	Allows users to access data across their Microsoft 365 Graph and leverage LLM functionality. Copilot can be accessed in Teams and when signed-in to Bing with an active directory account.
	Calls	Copilot in Teams Phone uses the power of AI to empower you to work more flexibly and intelligently, automating important

Microsoft 365 App	Feature	Description
		administrative tasks of a call, such as capturing key points, task owners, and next steps, so you can stay focused on the discussion. Copilot in Teams Phone supports both voice over Internet Protocol (VoIP) and public switched telephone network (PSTN) calls.
	Whiteboard	Makes meetings and brainstorm sessions more creative and effective. Use natural language to ask Copilot to generate ideas, organize ideas into themes, create designs that bring ideas to life and summarize whiteboard content.
OneNote	Draft with Copilot	Use prompts to draft plans, generate ideas, create lists, and organize information to help you easily find what you need.
Forms	Draft with Copilot	Use prompts to draft questions and suggestions that help you create surveys, polls, and other forms with ease.

To learn more about what's possible with Microsoft 365 Apps and Copilot, check out Microsoft 365 AI help and learning.

How does Microsoft Copilot for Microsoft 365 work?

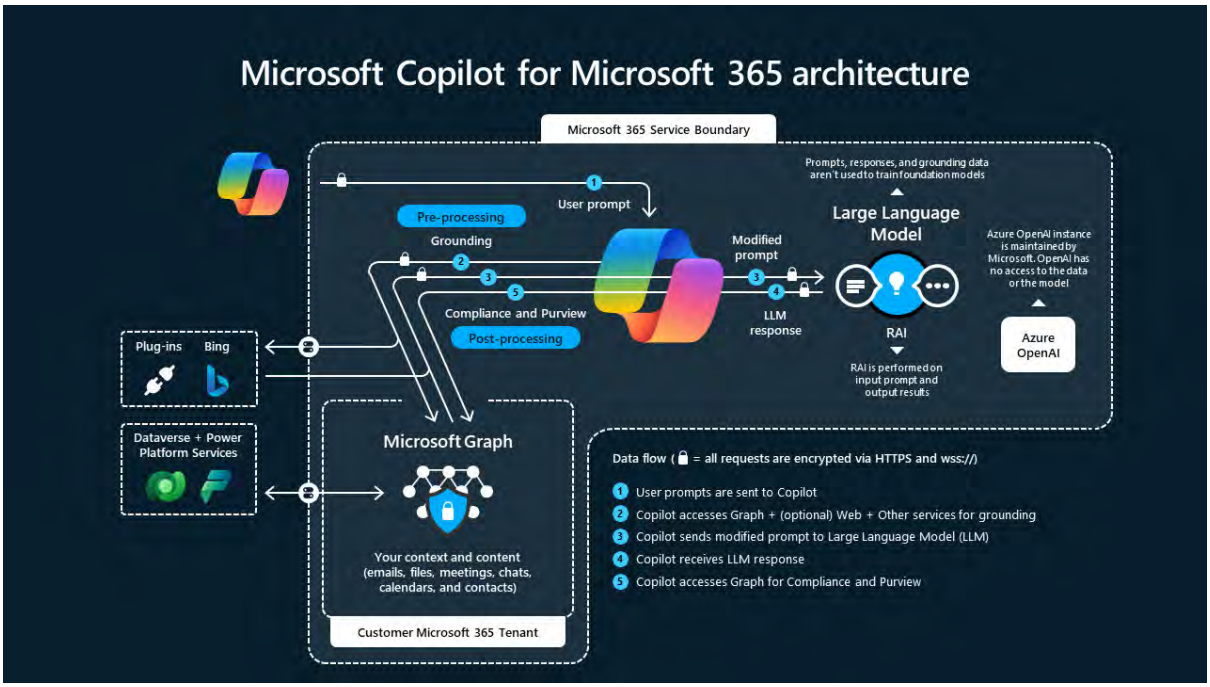
Microsoft Copilot for Microsoft 365 capabilities that users see in Microsoft 365 Apps and other surfaces appear as intelligent features, functionality, and prompting capability. Our foundation LLMs and proprietary Microsoft technologies work together in an underlying system that helps you securely access, use, and manage your organizational data.

- **Microsoft 365 Apps** (such as Word, Excel, PowerPoint, Outlook, Teams, and Loop) operate with Copilot for Microsoft 365 to support users in the context of their work. For example, Copilot in Word is designed to assist users specifically in the process of creating, understanding, and editing documents. In a similar way, Copilot in the other apps helps users in the context of their work within those apps.
- **Microsoft Copilot with Graph-grounded chat** enables you to bring your work content and context to Microsoft Copilot's chat capabilities. With Graph-grounded chat, you can draft content, catch up on what you missed, and get answers to questions via open-ended prompts— all securely grounded in your work data. Use Graph-grounded Copilot at many surfaces, including within Microsoft Teams, at Microsoft365.com, and at copilot.microsoft.com.
- **Microsoft Graph** has long been fundamental to Microsoft 365. It includes information about the relationships between users, activities, and your organization's data. The Microsoft Graph API brings more context from customer signals into the prompt, such as

information from emails, chats, documents, and meetings. For more information, see Overview of Microsoft Graph and Major services and features in Microsoft Graph.

- **Semantic Index** for Copilot uses multiple LLMs that sit on top of Microsoft Graph to interpret user queries and produce sophisticated, meaningful, and multilingual responses that help you to be more productive. It allows you to search quickly through billions of vectors (mathematical representations of features or attributes) to help connect you with relevant and actionable information in your organization. For more information, see the Semantic Index for Copilot article

The following diagram provides a visual representation of how Microsoft Copilot for Microsoft 365 works.



Here's an explanation of how Microsoft Copilot for Microsoft 365 works:

- Copilot receives an input prompt from a user in an app, such as Word or PowerPoint.
- Copilot then pre-processes the input prompt through an approach called grounding, which improves the specificity of the prompt, to help you get answers that are relevant and actionable to your specific task. The prompt can include text from input files or other content discovered by Copilot, and Copilot sends this prompt to the LLM for processing. Copilot only accesses data that an individual user has existing access to, based on, for example, existing Microsoft 365 role-based access controls.
- Copilot takes the response from the LLM and post-processes it. This post-processing includes other grounding calls to Microsoft Graph, responsible AI checks, security, compliance and privacy reviews, and command generation.
- Copilot returns the response to the app, where the user can review and assess the response.

We refer to the user's prompt and Copilot's response to that prompt as the "content of interactions" and the record of those interactions is the user's Copilot interaction history.

Microsoft Copilot for Microsoft 365 iteratively processes and orchestrates these sophisticated services to help produce results that are relevant to your organization because they're contextually based on your organizational data.

Semantic Index

Through enhanced interactions with your individual and company data via the Microsoft Graph, and the creation of a new index, the semantic index is an improvement to Microsoft 365 search that lays the foundation for the next generation of Search and Copilot experiences. The semantic index respects security and policies in the Microsoft Graph so that when a user issues a query either directly via search or in Microsoft Copilot, it's always in the security context of the user, and only content that a user has access to is returned.

To learn more, see Semantic Index for Copilot.

Availability

Copilot for Microsoft 365 is available as an add-on plan with one of the following licensing prerequisites:

For Business and Enterprise:

- **Microsoft 365 plans:**
  - Microsoft 365 E5
  - Microsoft 365 E3
  - Microsoft 365 F1
  - Microsoft 365 F3
  - Microsoft 365 Business Basic
  - Microsoft 365 Business Premium
  - Microsoft 365 Business Standard
  - Microsoft 365 Apps for business
  - Microsoft 365 Apps for enterprise
- **Office 365 plans:**
  - Office 365 E5
  - Office 365 E3
  - Office 365 E1
  - Office 365 F3
- **Microsoft Teams plans:**
  - Microsoft Teams Essentials
  - Microsoft Teams Enterprise

    - Microsoft Teams EEA (European Economic Area)
- **Exchange plans:**
    - Exchange Kiosk
    - Exchange Plan 1
    - Exchange Plan 2
- **SharePoint plans:**
    - SharePoint Plan 1
    - SharePoint Plan 2
- **OneDrive for Business plans:**
    - OneDrive for Business Plan 1
    - OneDrive for Business Plan 2
- **Planner and Project plans:**
    - Microsoft Planner Plan 1 (formerly Project Plan 1)
    - Microsoft Project Plan 3
    - Microsoft Project Plan 5
    - Project Online Essentials
- **Visio plans:**
    - Visio Plan 1
    - Visio Plan 2
- **Other plans:**
    - Microsoft ClipChamp

For Education Faculty and Higher Education Students Aged 18+:

- Microsoft 365 A1*
- Microsoft 365 A3*
- Microsoft 365 A5*
- Office 365 A1*
- Office 365 A3*
- Office 365 A5*

*Available via Enrollment for Education Solutions (EES) or Cloud Solution Provider (CSP) only.

You can use the Microsoft Copilot for Microsoft 365 setup guide in the Microsoft 365 admin center to assign the required licenses to users. For more information, see Assign licenses to users in the Microsoft 365 admin center and Microsoft Copilot for Microsoft 365 requirements.

Additional resources

You can learn more about Microsoft Copilot for Microsoft 365 by reviewing these resources:

- Data, Privacy, and Security for Microsoft Copilot for Microsoft 365
- The Copilot System: Explained by Microsoft
- Semantic Index for Copilot: Explained by Microsoft

- How Microsoft Copilot for Microsoft 365 works
- How to get ready for Microsoft Copilot for Microsoft 365
- Microsoft 365 AI help and learning

You can also stay up to date on the latest Copilot features, changes, and announcements using the Message center in the Microsoft 365 admin center.

Appendix 3 – Data, Privacy and Security for Microsoft Copilot for Microsoft 365

Data, Privacy, and Security for Microsoft Copilot for Microsoft 365

- Article
- 20/06/2024
- 5 contributors

Feedback

In this article

Microsoft Copilot for Microsoft 365 is a sophisticated processing and orchestration engine that provides AI-powered productivity capabilities by coordinating the following components:

- Large language models (LLMs)
- Content in Microsoft Graph, such as emails, chats, and documents that you have permission to access.
- The Microsoft 365 productivity apps that you use every day, such as Word and PowerPoint.

For an overview of how these three components work together, see Microsoft Copilot for Microsoft 365 overview. For links to other content related to Microsoft Copilot for Microsoft 365, see Microsoft Copilot for Microsoft 365 documentation.

Important

- Microsoft Copilot for Microsoft 365 is compliant with our existing privacy, security, and compliance commitments to Microsoft 365 commercial customers, including the General Data Protection Regulation (GDPR) and European Union (EU) Data Boundary.
- Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs, including those used by Microsoft Copilot for Microsoft 365.

- Microsoft Copilot for Microsoft 365 operates with multiple protections, which include, but are not limited to, **blocking harmful content**, **detecting protected material**, and **blocking prompt injections (jailbreak attacks)**.

The information in this article is intended to help provide answers to the following questions:

- How does Microsoft Copilot for Microsoft 365 use your proprietary organizational data?
- How does Microsoft Copilot for Microsoft 365 protect organizational information and data?
- What data is stored about user interactions with Microsoft Copilot for Microsoft 365?
- What data residency commitments does Microsoft Copilot make?
- What extensibility options are available for Microsoft Copilot for Microsoft 365
- How does Microsoft Copilot for Microsoft 365 meet regulatory compliance requirements?
- Do controls for connected experiences in Microsoft 365 Apps apply to Microsoft Copilot for Microsoft 365?
- Can I trust the content that Microsoft Copilot for Microsoft 365 creates? Who owns that content?
- What are Microsoft's commitments to using AI responsibly?

Note

Microsoft Copilot for Microsoft 365 will continue to evolve over time with new capabilities. To keep up to date on Microsoft Copilot for Microsoft 365 or ask questions, visit the **Microsoft 365 Copilot community** on the Microsoft Tech Community.

How does Microsoft Copilot for Microsoft 365 use your proprietary organizational data?

Microsoft Copilot for Microsoft 365 provides value by connecting LLMs to your organizational data. Microsoft Copilot for Microsoft 365 accesses content and context through Microsoft Graph. It can generate responses anchored in your organizational data, such as user documents, emails, calendar, chats, meetings, and contacts. Microsoft Copilot for Microsoft 365 combines this content with the user's working context, such as the meeting a user is in now, the email exchanges the user had on a topic, or the chat conversations the user had last week. Microsoft Copilot for Microsoft 365 uses this combination of content and context to help provide accurate, relevant, and contextual responses.

Important

Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs, including those used by Microsoft Copilot for Microsoft 365.

Microsoft Copilot for Microsoft 365 only surfaces organizational data to which individual users have at least view permissions. It's important that you're using the permission models available in Microsoft 365 services, such as SharePoint, to help ensure the right users or groups have the right access to the right content within your organization. This includes permissions you give to users outside your organization through inter-tenant collaboration solutions, such as shared channels in Microsoft Teams.

When you enter prompts using Microsoft Copilot for Microsoft 365, the information contained within your prompts, the data they retrieve, and the generated responses remain within the Microsoft 365 service boundary, in keeping with our current privacy, security, and compliance commitments. Microsoft Copilot for Microsoft 365 uses Azure OpenAI services for processing, not OpenAI's publicly available services. Azure OpenAI doesn't cache customer content and Copilot modified prompts for Copilot for Microsoft 365.

Note

- When you're using plugins to help Copilot for Microsoft 365 to provide more relevant information, check the privacy statement and terms of use of the plugin to determine how it will handle your organization's data. For more information, see **Extensibility of Microsoft Copilot for Microsoft 365**.
- When you're using the web content plugin, Copilot for Microsoft 365 parses the user's prompt and identifies terms where web grounding would improve the quality of the response. Based on these terms, Copilot generates a search query that it sends to the Bing Search service. For more information, **Data, privacy, and security for web queries in Copilot for Microsoft 365**.

Abuse monitoring for Microsoft Copilot for Microsoft 365 occurs in real-time, without providing Microsoft any standing access to customer data, either for human or for automated review. While abuse moderation, which includes human review of content, is available in Azure OpenAI, Microsoft Copilot for Microsoft 365 services have opted out of it. Microsoft 365 data isn't collected or stored by Azure OpenAI.

Note

We may use customer feedback, which is optional, to improve Microsoft Copilot for Microsoft 365, just like we use customer feedback to improve other Microsoft 365 services and Microsoft 365 productivity apps. We don't use this feedback to train the foundation LLMs used by Microsoft Copilot for Microsoft 365. Customers can manage feedback through admin controls. For more information, see **Manage Microsoft feedback for your organization** and **Providing feedback about Microsoft Copilot for Microsoft 365**.

Data stored about user interactions with Microsoft Copilot for Microsoft 365

When a user interacts with Microsoft Copilot for Microsoft 365 (using apps such as Word, PowerPoint, Excel, OneNote, Loop, or Whiteboard), we store data about these interactions. The stored data includes the user's prompt and Copilot's response, including citations to any information used to ground Copilot's response. We refer to the user's prompt and Copilot's response to that prompt as the "content of interactions" and the record of those interactions is the user's Copilot interaction history. For example, this stored data provides users with Copilot interaction history in Microsoft Copilot with Graph-grounded chat and meetings in Microsoft Teams. This data is processed and stored in alignment with contractual commitments with your organization's other content in Microsoft

365. The data is encrypted while it's stored and isn't used to train foundation LLMs, including those used by Microsoft Copilot for Microsoft 365.

To view and manage this stored data, admins can use Content search or Microsoft Purview. Admins can also use Microsoft Purview to set retention policies for the data related to chat interactions with Copilot. For more information, see the following articles:

- Overview of Content search
- Microsoft Purview data security and compliance protections for generative AI apps
- Learn about retention for Copilot for Microsoft 365

For Microsoft Teams chats with Copilot, admins can also use Microsoft Teams Export APIs to view the stored data.

Deleting the history of user interactions with Microsoft Copilot for Microsoft 365

Your users can delete their Copilot interaction history, which includes their prompts and the responses Copilot returns, by going to the My Account portal. For more information, see Delete your Microsoft Copilot interaction history.

Microsoft Copilot for Microsoft 365 and the EU Data Boundary

Microsoft Copilot for Microsoft 365 calls to the LLM are routed to the closest data centers in the region, but also can call into other regions where capacity is available during high utilization periods.

For European Union (EU) users, we have additional safeguards to comply with the EU Data Boundary. EU traffic stays within the EU Data Boundary while worldwide traffic can be sent to the EU and other countries or regions for LLM processing.

Microsoft Copilot for Microsoft 365 and data residency

Copilot for Microsoft 365 is upholding data residency commitments as outlined in the Microsoft Product Terms and Data Protection Addendum. Copilot for Microsoft 365 was added as a covered workload in the data residency commitments in Microsoft Product Terms on March 1, 2024.

Microsoft Advanced Data Residency (ADR) and Multi-Geo Capabilities offerings include data residency commitments for Copilot for Microsoft 365 customers as of March 1, 2024. For EU customers, Copilot for Microsoft 365 is an EU Data Boundary service. Customers outside the EU may have their queries processed in the US, EU, or other regions.

Extensibility of Microsoft Copilot for Microsoft 365

While Microsoft Copilot for Microsoft 365 is already able to use the apps and data within the Microsoft 365 ecosystem, many organizations still depend on various external tools and services for work management and collaboration. Microsoft Copilot for Microsoft 365 experiences can reference third-party tools and services when responding to a user's request by using Microsoft Graph connectors or plugins. Data from Graph connectors can be returned in Microsoft Copilot for Microsoft 365 responses if the user has permission to access that information.

When plugins are enabled, Microsoft Copilot for Microsoft 365 determines whether it needs to use a specific plugin to help provide a relevant response to the user. If a plugin is needed, Microsoft Copilot for Microsoft 365 generates a search query to send to the plugin on the user's behalf. The query is based on the user's prompt, Copilot interaction history, and data the user has access to in Microsoft 365.

In the **Integrated apps** section of the Microsoft 365 admin center, admins can view the permissions and data access required by a plugin as well as the plugin's terms of use and privacy statement. Admins have full control to select which plugins are allowed in their organization. A user can only access the plugins that their admin allows and that the user installed or is assigned. Microsoft Copilot for Microsoft 365 only uses plugins that are turned on by the user.

Note

The policy settings that control the use of optional connected experiences in Microsoft 365 Apps don't apply to plugins.

For more information, see the following articles:

- Manage Plugins for Copilot in Integrated Apps
- Extend Microsoft Copilot for Microsoft 365
- How Microsoft Copilot for Microsoft 365 can work with your external data

How does Microsoft Copilot for Microsoft 365 protect organizational data?

The permissions model within your Microsoft 365 tenant can help ensure that data won't unintentionally leak between users, groups, and tenants. Microsoft Copilot for Microsoft 365 presents only data that each individual can access using the same underlying controls for data access used in other Microsoft 365 services. Semantic Index honors the user identity-based access boundary so that the grounding process only accesses content that the current user is authorized to access. For more information, see Microsoft's privacy policy and service documentation.

When you have data that's encrypted by Microsoft Purview Information Protection, Microsoft Copilot for Microsoft 365 honors the usage rights granted to the user. This encryption can be applied

by sensitivity labels or by restricted permissions in apps in Microsoft 365 by using Information Rights Management (IRM). For more information about using Microsoft Purview with Microsoft Copilot for Microsoft 365, see Microsoft Purview data security and compliance protections for generative AI apps.

We already implement multiple forms of protection to help prevent customers from compromising Microsoft 365 services and applications or gaining unauthorized access to other tenants or the Microsoft 365 system itself. Here are some examples of those forms of protection:

- Logical isolation of customer content within each tenant for Microsoft 365 services is achieved through Microsoft Entra authorization and role-based access control. For more information, see Microsoft 365 isolation controls.
- Microsoft uses rigorous physical security, background screening, and a multi-layered encryption strategy to protect the confidentiality and integrity of customer content.
- Microsoft 365 uses service-side technologies that encrypt customer content at rest and in transit, including BitLocker, per-file encryption, Transport Layer Security (TLS) and Internet Protocol Security (IPsec). For specific details about encryption in Microsoft 365, see Encryption in the Microsoft Cloud.
- Your control over your data is reinforced by Microsoft's commitment to comply with broadly applicable privacy laws, such as the GDPR, and privacy standards, such as ISO/IEC 27018, the world's first international code of practice for cloud privacy.
- For content accessed through Microsoft Copilot for Microsoft 365 plug-ins, encryption can exclude programmatic access, thus limiting the plug-in from accessing the content. For more information, see Configure usage rights for Azure Information Protection.

Meeting regulatory compliance requirements

As regulation in the AI space evolves, Microsoft will continue to adapt and respond to fulfill future regulatory requirements.

Microsoft Copilot for Microsoft 365 is built on top of Microsoft's current commitments to data security and privacy in the enterprise. There's no change to these commitments. Microsoft Copilot for Microsoft 365 is integrated into Microsoft 365 and adheres to all existing privacy, security, and compliance commitments to Microsoft 365 commercial customers. For more information, see Microsoft Compliance.

Beyond adhering to regulations, we prioritize an open dialogue with our customers, partners, and regulatory authorities to better understand and address concerns, thereby fostering an environment of trust and cooperation. We acknowledge that privacy, security, and transparency aren't just features, but prerequisites in the AI-driven landscape at Microsoft.

Additional information

Microsoft Copilot for Microsoft 365 and policy settings for connected experiences

If you turn off connected experiences that analyze content for Microsoft 365 Apps on Windows or Mac devices in your organization, Microsoft Copilot for Microsoft 365 features won't be available to your users in the following apps:

- Excel
- PowerPoint
- OneNote
- Word

Similarly, Microsoft Copilot for Microsoft 365 features in those apps on Windows or Mac devices won't be available if you turn off the use of connected experiences for Microsoft 365 Apps.

For more information about these policy settings, see the following articles:

- Use policy settings to manage privacy controls for Microsoft 365 Apps for enterprise *(for Windows)*
- Use preferences to manage privacy controls for Office for Mac

About the content that Microsoft Copilot for Microsoft 365 creates

The responses that generative AI produces aren't guaranteed to be 100% factual. While we continue to improve responses, users should still use their judgment when reviewing the output before sending them to others. Our Microsoft Copilot for Microsoft 365 capabilities provide useful drafts and summaries to help you achieve more while giving you a chance to review the generated AI rather than fully automating these tasks.

We continue to improve algorithms to proactively address issues, such as misinformation and disinformation, content blocking, data safety, and preventing the promotion of harmful or discriminatory content in line with our responsible AI principles.

Microsoft doesn't claim ownership of the output of the service. That said, we don't make a determination on whether a customer's output is copyright protected or enforceable against other users. This is because generative AI systems may produce similar responses to similar prompts or queries from multiple customers. Consequently, multiple customers may have or claim rights in content that is the same or substantially similar.

If a third party sues a commercial customer for copyright infringement for using Microsoft's Copilots or the output they generate, we'll defend the customer and pay the amount of any adverse judgments or settlements that result from the lawsuit, as long as the customer used the guardrails

and content filters we have built into our products. For more information, see Microsoft announces new Copilot Copyright Commitment for customers.

How does Copilot block harmful content?

Azure OpenAI Service includes a content filtering system that works alongside core models. The content filtering models for the Hate & Fairness, Sexual, Violence, and Self-harm categories have been specifically trained and tested in various languages. This system works by running both the input prompt and the response through classification models that are designed to identify and block the output of harmful content.

Hate and fairness-related harms refer to any content that uses pejorative or discriminatory language based on attributes like race, ethnicity, nationality, gender identity and expression, sexual orientation, religion, immigration status, ability status, personal appearance, and body size. Fairness is concerned with making sure that AI systems treat all groups of people equitably without contributing to existing societal inequities. Sexual content involves discussions about human reproductive organs, romantic relationships, acts portrayed in erotic or affectionate terms, pregnancy, physical sexual acts, including those portrayed as an assault or a forced act of sexual violence, prostitution, pornography, and abuse. Violence describes language related to physical actions that are intended to harm or kill, including actions, weapons, and related entities. Self-harm language refers to deliberate actions that are intended to injure or kill oneself.

Learn more about Azure OpenAI content filtering.

Does Copilot provide protected material detection?

Yes, Copilot for Microsoft 365 provides detection for protected materials, which includes text subject to copyright and code subject to licensing restrictions. Not all of these mitigations are relevant for all Copilot for Microsoft 365 scenarios.

Does Copilot block prompt injections (jailbreak attacks)?

Jailbreak attacks are user prompts that are designed to provoke the generative AI model into behaving in ways it was trained not to or breaking the rules it's been told to follow. Microsoft Copilot for Microsoft 365 is designed to protect against prompt injection attacks. Learn more about jailbreak attacks and how to use Azure AI Content Safety to detect them.

Committed to responsible AI

As AI is poised to transform our lives, we must collectively define new rules, norms, and practices for the use and impact of this technology. Microsoft has been on a Responsible AI journey since 2017,

when we defined our principles and approach to ensuring this technology is used in a way that is driven by ethical principles that put people first.

At Microsoft, we're guided by our AI principles, our Responsible AI Standard, and decades of research on AI, grounding, and privacy-preserving machine learning. A multidisciplinary team of researchers, engineers, and policy experts reviews our AI systems for potential harms and mitigations — refining training data, filtering to limit harmful content, query- and result-blocking sensitive topics, and applying Microsoft technologies like InterpretML and Fairlearn to help detect and correct data bias. We make it clear how the system makes decisions by noting limitations, linking to sources, and prompting users to review, fact-check, and adjust content based on subject-matter expertise. For more information, see Governing AI: A Blueprint for the Future.

We aim to help our customers use our AI products responsibly, sharing our learnings, and building trust-based partnerships. For these new services, we want to provide our customers with information about the intended uses, capabilities, and limitations of our AI platform service, so they have the knowledge necessary to make responsible deployment choices. We also share resources and templates with developers inside organizations and with independent software vendors (ISVs), to help them build effective, safe, and transparent AI solutions.

Related articles

- Microsoft Copilot for Microsoft 365 requirements
- Get started with Microsoft Copilot for Microsoft 365
- Microsoft Copilot adoption site

Appendix 4 – Privacy and Security Terms

Microsoft Product Terms

[Captured 12/07/2024]

Privacy & Security Terms

General | Core Online Services | EU Data Boundary Services

General

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

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

Online Services excluded from the DPA

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

Software Products excluded from the DPA

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

Non-Microsoft Products

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

DPA Terms Geography Exclusions

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

Core Online Services

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

Online Services	
Microsoft Dynamics 365 Core Services	The following services, each as a standalone service or as included in a Dynamics 365 branded plan or application: Dynamics 365 Customer Service, Dynamics 365 Customer Insights, Dynamics 365 Field Service, Dynamics 365 Business Central, Dynamics 365 Supply Chain Management, Dynamics 365 Intelligent Order Management, Dynamics 365 Finance, Dynamics 365 Commerce, Dynamics 365 Human Resources, Dynamics 365 Project Operations, and Dynamics 365 Sales.

Online Services	
	Dynamics 365 Core Services do not include (1) Dynamics 365 Services for supported devices or software, which includes but is not limited to Dynamics 365 for apps, tablets, phones, or any of these; (2) LinkedIn Sales Navigator; or (3) except as expressly defined in the licensing terms for the corresponding service, any other separately-branded service made available with or connected to Dynamics 365 Core Services.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365 or Microsoft 365-branded plan or suite: Customer Lockbox, Exchange Online Archiving, Exchange Online Protection, Exchange Online, Microsoft Bookings, Microsoft Forms, Microsoft Planner, Microsoft Stream (Classic), Microsoft Teams, Microsoft To-Do, Microsoft Defender for Office 365, Office for the web, OneDrive for Business, Project, SharePoint, Sway, Viva Insights, Whiteboard, Viva Engage, and Microsoft Copilot for Microsoft 365. Office 365 Services do not include Microsoft 365 Apps for enterprise, any portion of a PSTN service that operates outside of Microsoft's control, any client software, or any separately branded service made available with an Office 365 or Microsoft 365-branded plan or suite, such as a Bing or a service branded "for Office 365."
Microsoft 365 Compliance Services	The following services, each as a standalone service or as included in a Microsoft 365-branded plan or suite: Microsoft Purview Customer Lockbox, Microsoft Purview Data Loss Prevention, Microsoft Purview Customer Key, Microsoft Purview Data Lifecycle Management, Microsoft Purview Information Barriers, Microsoft Purview Privileged Access Management, Microsoft Purview Compliance Manager, Microsoft Purview Information Protection, Microsoft Information Governance, Microsoft Purview-Insider Risk Management, Microsoft Purview Communication Compliance, Microsoft Purview Records Management, Microsoft Purview eDiscovery, and Microsoft Purview Audit, Microsoft Priva Privacy Risk Management, and Microsoft Priva Subject Rights Request.
Microsoft Azure Core Services	Azure AI, Azure AI Content Safety, Azure Active Directory B2C, Anomaly Detector, API Management, App Service (API Apps, Logic Apps, Mobile Apps, WebJobs, Functions), Lab Services, Application Gateway, Azure Monitor, Automation, Azure API for FHIR, Azure App Configuration, Azure Bastion, Azure AI Bot Service, Azure Cache for Redis, Azure AI Search, Azure Communication Services, Azure Container Apps, Azure Container Instances, Azure Container Registry (ACR), Azure Cosmos DB, Azure Data Explorer, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Databricks, Azure DDOS Protection, Azure DevOps, Azure DNS, Microsoft Entra ID, Azure Event Grid, Microsoft Fabric, Azure Firewall, Azure AI Document Intelligence, Azure Health Data Services, Azure AI Immersive Reader, Azure Kubernetes Service, Azure Managed Grafana, Azure Machine Learning, Azure AI Metrics Advisor, Azure NetApp Files, Azure OpenAI Service, Azure Red Hat OpenShift, Azure VMware Solution, Microsoft Purview Data Map, Microsoft Purview Data Catalog, Microsoft Purview Data Estate Insights, Microsoft Purview Data Policies, Microsoft Purview Data Sharing, Azure Resource

Online Services	
	Manager, Azure Spring Apps, Azure Time Series Insights, Azure AI Video Indexers, Azure Web PubSub, Backup, Batch, Cloud Services, Computer Vision, Content Moderator, Azure AI Custom Vision, Data Factory, Data Lake Analytics, Data Lake Store, Event Hubs, Express Route, Face, HDInsight, Import/Export, IoT Hub, Key Vault, Language Understanding, Load Balancer, Azure Machine Learning Studio (classic), Media Services, Microsoft Azure Portal, Notification Hubs, Azure AI Personalizer, Power BI Embedded, QnA Maker, Microsoft Defender for Cloud, Service Bus, Service Connector, Service Fabric, Azure SignalR Service, Site Recovery, Speech Services, SQL Database, SQL Managed Instance, SQL Server Stretch Database, Storage, StorSimple, Stream Analytics, Synapse Analytics, Text Analytics, Traffic Manager, Azure AI Translator, Virtual Machines, Virtual Machine Scale Sets, Virtual Network, and VPN Gateway.
Microsoft Defender for Cloud Apps	The cloud service portion of Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security).
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune.
Microsoft Power Platform Core Services	The following services, each as a standalone service or as included in an Office 365 or Microsoft Dynamics 365 branded plan or suite: Microsoft Power BI, Microsoft Power Apps, Microsoft Power Automate, Microsoft Power Pages, and Microsoft Copilot Studio. Microsoft Power Platform Core Services do not include any client software, including but not limited to Power BI Report Server, the Power BI, PowerApps or Microsoft Power Automate mobile applications, Power BI Desktop, or Power Apps Studio.
Microsoft Defender for Endpoint Services	The cloud services portion of Microsoft Defender for Endpoint.
Microsoft Defender for Identity	The cloud services portion of Microsoft Defender for Identity.
Microsoft Defender XDR	The cloud service portion of Microsoft Defender XDR.
Microsoft Sentinel	The cloud service portion of Microsoft Sentinel.

Online Services	
Windows 365	The cloud service portion of Windows 365, excluding the Windows operating system running on Windows 365 Cloud PCs.

Security Practices and Policies for Core Online Services

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

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

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

Location of Customer Data at Rest for Core Online Services

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

- **Office 365 Services.** If Customer provisions its tenant in Australia, Brazil, Canada, the European Union, France, Germany, India, Japan, Norway, Qatar, South Africa, South Korea, Sweden, Switzerland, the United Kingdom, the United Arab Emirates, or the United States, Microsoft will store the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, (3) files uploaded to OneDrive for Business, (4) Microsoft Teams chat messages (including private messages, channel messages, meeting messages and images used in chats), and for customers using Microsoft Stream (Classic) (on SharePoint) meeting recordings, and (5) any stored content of interactions with Microsoft Copilot for Microsoft 365 to the extent not included in the preceding commitments. If Customer purchases an Advanced Data Residency subscription, then Microsoft will store certain Customer Data at rest in the applicable Geo in accordance with this section and the "Advanced Data Residency Commitments" section of the product documentation at https://aka.ms/adroverview.
- **Microsoft Intune Online Services**. When Customer provisions a Microsoft Intune tenant account to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft Intune Trust Center.
- **Microsoft Power Platform Core Services**. When Customer provisions a Power Platform Core Service to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo, except as described in the Microsoft Power Platform Trust Center.
- **Microsoft Azure Core Services**. If Customer configures a particular service to be deployed within a Geo then, for that service, Microsoft will store Customer Data at rest within the specified Geo. Certain services may not enable Customer to configure deployment in a particular Geo or outside the United States and may store backups in other locations. Refer to the Microsoft Trust Center (which Microsoft may update from time to time, but Microsoft will not add exceptions for existing Services in general release) for more details.
- **Microsoft Defender for Cloud Apps**. If Customer provisions its tenant in the European Union or the United States, Microsoft will store Customer Data at rest only within that Geo, except as described in the Microsoft Defender for Cloud Apps Trust Center.
- **Microsoft Dynamics 365 Core Services**. When Customer provisions a Dynamics 365 Core Service to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo, except as described in the Microsoft Dynamics 365 Trust Center.
- **Microsoft Defender for Endpoint Services**. When Customer provisions a Microsoft Defender for Endpoint tenant to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft Defender for Endpoint Trust Center.
- **Microsoft Defender for Identity.** When Customer provisions a Microsoft Defender for Identity tenant to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft Defender for Identity Trust Center.

- **Microsoft Defender XDR**. When Customer provisions a Microsoft Defender XDR tenant to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft Defender XDR Trust Center.
- **Windows 365**. When a Windows 365 tenant is deployed within an available Geo, then, for that tenant, Microsoft will store Customer Data at rest within that specified Geo. If Customer provisions Windows 365 Cloud PCs within the same tenant to different available Geos, then, for each Cloud PC, Microsoft will store Cloud PC Customer Data at rest within that specified Geo.

EU Data Boundary Services

The term "EU Data Boundary" means the Microsoft computers, computing environment, and physical data centers located solely in the European Union (EU) and the European Free Trade Association (EFTA). The term "EU Data Boundary Services" applies only to the Online Services in the table below, excluding any Previews.

EU Data Boundary Services	
Azure	Azure services that enable deployment in a region within the EU Data Boundary and the following non-regional services: Azure Active Directory B2C, Azure Advisor, Azure Bot Service, Cloud Shell, Azure Communication Services, Azure Data Box, Azure DNS, Microsoft Entra ID, Microsoft Fabric, Azure Kubernetes Service on Azure Stack HCI, Azure Lighthouse, Azure Migrate, Azure Monitor, Azure Resource Mover, Azure Service Health, Azure Sphere, Azure Stack Edge, Azure Stack HCI, Azure Stack Hub, Azure Virtual Desktop, Azure VM Image Builder, Power BI Embedded, Traffic Manager, Translator
Dynamics 365	Dynamics 365 Business Central, Dynamics 365 Commerce, Dynamics 365 Customer Insights, Dynamics 365 Customer Service, Dynamics 365 Customer Voice, Dynamics 365 Field Service, Dynamics 365 Finance, Dynamics 365 Guides, Dynamics 365 Intelligent Order Management, Dynamics 365 Project Operations, Dynamics 365 Remote Assist, Dynamics 365 Sales, Dynamics 365 Supply Chain Management
Microsoft 365	Customer Lockbox, Exchange Online, Exchange Online Archiving for Exchange Online, Microsoft Bookings, Microsoft Forms, Microsoft MyAnalytics, Microsoft Planner, Microsoft StaffHub, Microsoft Stream (Classic) (on SharePoint), Microsoft Teams, Microsoft To-Do, Office for the web, Online Services provided as part of Microsoft 365 Apps, OneDrive for Business, SharePoint Online, Sway, Whiteboard, Viva Engage, Microsoft Copilot for Microsoft 365, Communications Compliance, eDiscovery and Audit, Insider Risk Management, Information Barriers, Microsoft Purview Data Loss Prevention, Microsoft Intune, Priva Privacy Risk Management, Priva Subject Rights Management, Microsoft Viva Answers, Microsoft Viva Connections, Microsoft Viva Engage, Microsoft Viva Glint, Microsoft Viva Goals, Microsoft Viva Insights, Microsoft Viva Learning, Microsoft Viva Pulse, Microsoft Copilot for Sales, and Microsoft Viva Topics
Power Platform	Microsoft Power Apps, Microsoft Power Automate, Microsoft Power BI, Microsoft Power Pages, Microsoft Copilot Studio

Location of Customer Data for EU Data Boundary Services

For EU Data Boundary Services, Microsoft will store and process Customer Data and Personal Data within the EU Data Boundary as detailed below.

Customer must configure EU Data Boundary Services as follows:

- For **Azure**, Customer must deploy the service into an Azure region located within the EU Data Boundary. See Data Residency in Azure (https://azure.microsoft.com/explore/global-infrastructure/data-residency) for more information. For services that do not enable deployment into a specified Azure region, Customer must follow the instructions at Configuring Azure non-regional services for the EU Data Boundary (https://learn.microsoft.com/privacy/eudb/eu-data-boundary-configure-azure-nonregional-services).
- For **Dynamics 365 and Power Platform**, if Customer provisions a tenant with a billing address in the EU or EFTA, that tenant will be in-scope for the EU Data Boundary if Customer also creates all of its environments within a Geo inside the EU Data Boundary.
- For **Microsoft 365**, if Customer provisions a tenant in the EU or EFTA, that tenant will be in-scope for the EU Data Boundary, except for those tenants where Customer has also purchased the Microsoft 365 Multi-Geo Capabilities add-on that enables customers to expand Microsoft 365 tenant presence to multiple geographic regions or countries (https://learn.microsoft.com/microsoft-365/enterprise/microsoft-365-multi-geo?view=o365-worldwide).

Use of EU Data Boundary Services may result in limited transfers of Customer Data or Personal Data outside the EU Data Boundary, as set forth below and further detailed in transparency documentation for the EU Data Boundary located at https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn or successor location. Any such transfers will be conducted in accordance with the Data Protection Addendum and the Product Terms.

- **Remote Access**. Microsoft personnel located outside the EU Data Boundary may remotely access data processing systems in the EU Data Boundary as necessary to operate, troubleshoot, and secure the EU Data Boundary Services.
- **Customer-Initiated Transfers**. Customers may initiate transfers outside the EU Data Boundary, such as by accessing EU Data Boundary Services from locations outside the EU Data Boundary, sending an email to a recipient located outside the EU Data Boundary, or use of EU Data Boundary Services in combination with other services not in the EU Data Boundary.
- **Protecting Customers**. Microsoft transfers limited data outside of the EU Data Boundary as necessary to detect and protect Customers against security threats.
- **Directory Data**. Microsoft may replicate limited Microsoft Entra directory data from Microsoft Entra ID (including username and email address) outside the EU Data Boundary to provide the service.

- **Network Transit**. To reduce routing latency and to maintain routing resiliency, Microsoft uses variable network paths that may occasionally result in transit of data outside the EU Data Boundary.
- **Service and Platform Quality and Management**. When required to monitor and maintain service quality or to ensure accuracy of statistical measures of service use or performance, pseudonymized Personal Data may be transferred outside of the EU Data Boundary.
- **Service-Specific Transfers**. See transparency documentation referenced above for information about transfers applicable to specific EU Data Boundary Services.

Appendix 5 – Microsoft products and services Data Protection Addendum

Licensing Documents (microsoft.com)

[Captured 12/07/2024]

Volume Licensing

Microsoft Products and Services Data Protection Addendum

Last updated January 2, 2024

Published in English on January 2, 2024. Translations will be published by Microsoft when available. These commitments are binding on Microsoft as of January 2, 2024.

Table of Contents

Introduction

The parties agree that this Microsoft Products and Services Data Protection Addendum ("DPA") sets forth their obligations with respect to the processing and security of Customer Data, Professional Services Data, and Personal Data in connection with the Products and Services. The DPA is incorporated by reference into the Product Terms and other Microsoft agreements. The parties also agree that, unless a separate Professional Services agreement exists, this DPA governs the processing and security of Professional Services Data. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in Customer's volume licensing agreement or other applicable agreements in connection with the Products and Services ("Customer's agreement"), the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Professional Services Data, or Personal Data, as defined herein.

Microsoft makes the commitments in this DPA to all Customers with an existing Customer's agreement. These commitments are binding on Microsoft with regard to Customer regardless of (1) the Product Terms that are otherwise applicable to any given Product subscription or license, or (2) any other agreement that references the Product Terms.

Applicable DPA Terms and Updates

Limits on Updates

When Customer renews or purchases a new subscription to a Product or enters into a work order for a Professional Service, the then-current DPA Terms will apply and will not change during Customer's subscription for that Product or term for that Professional Service. When Customer obtains a perpetual license to Software, the then-current DPA Terms will apply (following the same provision for determining the applicable then-current Product Terms for that Software in Customer's agreement) and will not change during Customer's license for that Software.

New Features, Supplements, or Related Software

Notwithstanding the foregoing limits on updates, when Microsoft introduces features, offerings, supplements or related software that are new (i.e., that were not previously included with the Products or Services), Microsoft may provide terms or make updates to the DPA that apply to Customer's use of those new features, offerings, supplements or related software. If those terms include any material adverse changes to the DPA Terms, Microsoft will provide Customer a choice to use the new features, offerings, supplements, or related software, without loss of existing functionality of a generally available Product or Professional Service. If Customer does not install or use the new features, offerings, supplements, or related software, the corresponding new terms will not apply.

Government Regulation and Requirements

Notwithstanding the foregoing limits on updates, Microsoft may modify or terminate a Product or Professional Service in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects Microsoft to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for Microsoft to continue operating the Product or offering the Professional Service without modification, and/or (3) causes Microsoft to believe the DPA Terms or the Product or Professional Service may conflict with any such requirement or obligation.

Electronic Notices

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

Prior Versions

The DPA Terms provide terms for Products and Services that are currently available. For earlier versions of the DPA Terms, Customer may refer to https://aka.ms/licensingdocs or contact its reseller or Microsoft Account Manager.

Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in Customer's agreement. The following defined terms are used in this DPA:

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

"Data Protection Requirements" means the GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"DPA Terms" means the terms in the DPA and any Product-specific terms in the Product Terms that specifically supplement or modify the privacy and security terms in the DPA for a specific Product (or feature of a Product). In the event of any conflict or inconsistency between the DPA and such Product-specific terms, the Product-specific terms shall prevail as to the applicable Product (or feature of that Product).

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

"Local EU/EEA Data Protection Laws" means any subordinate legislation and regulation implementing the GDPR.

"GDPR Terms" means the terms in Attachment 1, under which Microsoft makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

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

"Product" has the meaning provided in the volume license agreement. For ease of reference, "Product" includes Online Services and Software, each as defined in the volume license agreement.

"Products and Services" means Products and Professional Services. Product and Professional Service availability may vary by region and applicability of this DPA to specific Products and Professional Services is subject to the limitations in the Scope section in this DPA.

"Professional Services" means the following services: (a) Microsoft's consulting services, consisting of planning, advice, guidance, data migration, deployment and solution/software development services provided under a Microsoft Enterprise Services Work Order or, when agreed to in the Project Description, under a Cloud Workload Acceleration Agreement that incorporates this DPA by reference; and (b) technical support services provided by Microsoft that help customers identify and resolve issues affecting Products, including technical support provided as part of Microsoft Unified Support or Premier Support Services, and any other commercial technical support services. The Professional Services do not include the Products or, for purposes of the DPA only, Supplemental Professional Services.

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

"2021 Standard Contractual Clauses" means the standard data protection clauses (processor-to-processor module) between Microsoft Ireland Operations Limited and Microsoft Corporation for the transfer of personal data from processors in the EEA to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission in decision 2021/914/EC, dated 4 June 2021.

"Subprocessor" means other processors used by Microsoft to process Customer Data, Professional Services Data, and Personal Data, as described in Article 28 of the GDPR.

"Supplemental Professional Services" means support requests escalated from support to a Product engineering team for resolution and other consulting and support from Microsoft provided in connection with Products or a volume license agreement that are not included in the definition of Professional Services.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies.

General Terms

Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its providing the Products and Services, including security breach notification law and Data Protection Requirements. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Microsoft does not determine whether Customer's data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Products and Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Products and Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Products and Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of Products and Services, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Data Protection Terms

This section of the DPA includes the following subsections:

- Scope
- Nature of Data Processing; Ownership
- Disclosure of Processed Data
- Processing of Personal Data; GDPR
- Data Security
- Security Incident Notification
- Data Transfers and Location
- Data Retention and Deletion
- Processor Confidentiality Commitment
- Notice and Controls on use of Subprocessors
- Educational Institutions
- CJIS Customer Agreement
- HIPAA Business Associate
- Telecommunication Data
- California Consumer Privacy Act (CCPA)
- Biometric Data
- Supplemental Professional Services
- How to Contact Microsoft
- Appendix A – Security Measures
- Appendix B – Data Subjects and Categories of Personal Data
- Appendix C – Additional Safeguards Addendum.

Scope

The DPA Terms apply to all Products and Services except as described in this section.

The DPA Terms will not apply to any Products or Professional Services specifically identified as excluded, or to the extent identified as excluded, in the Product Terms or applicable work order, which are governed by the privacy and security terms in the applicable Product-specific or work order specific terms.

For clarity, the DPA Terms apply only to the processing of data in environments controlled by Microsoft and Microsoft's subprocessors. This includes data sent to Microsoft by Products and Services but does not include data that remains on Customer's premises or in any Customer selected third party operating environments.

For Supplemental Professional Services, Microsoft only makes the commitments in the Supplemental Professional Services section below.

Previews may employ lesser or different privacy and security measures than those typically present in the Products and Services. Unless otherwise noted, Customer should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements. For Products, the following terms in this DPA do not apply to Previews: Processing of Personal Data; GDPR, Data Security, and HIPAA Business Associate. For Professional Services, offerings designated as Previews or Limited Release only meet the terms of the Supplemental Professional Services.

Nature of Data Processing; Ownership

Microsoft will use and otherwise process Customer Data, Professional Services Data, and Personal Data only as described and subject to the limitations provided below (a) to provide Customer the Products and Services in accordance with Customer's documented instructions and (b) for business operations incident to providing the Products and Services to Customer. As between the parties, Customer retains all right, title and interest in and to Customer Data and Professional Services Data. Microsoft acquires no rights in Customer Data or Professional Services Data, other than the rights Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Processing to Provide Customer the Products and Services

For purposes of this DPA, "to provide" a Product consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security.

For purposes of this DPA, "to provide" Professional Services consists of:

- Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services); and
- Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including fixing software defects and otherwise keeping Products and Services up to date and performant.

In each case, providing the Products and Services is conducted in view of security obligations under Data Protection Requirements.

When providing Products and Services, Microsoft will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.

Processing for Business Operations Incident to Providing the Products and Services to Customer

For purposes of this DPA, "business operations" means the processing operations authorized by customer in this section.

Customer authorizes Microsoft:

(i.) to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and

(ii.) to calculate statistics related to Customer Data or Professional Services Data

in each case without accessing or analyzing the content of Customer Data or Professional Services Data and limited to achieving the purposes below, each as incident to providing the Products and Services to Customer.

Those purposes are:

- billing and account management;
- compensation such as calculating employee commissions and partner incentives;
- internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and
- financial reporting.

When processing for these business operations, Microsoft will apply principles of data minimization and will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section. In addition, as with all processing under this DPA, processing for business operations remains subject to Microsoft's confidentiality obligations and commitments under Disclosure of Processed Data.

Disclosure of Processed Data

Microsoft will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Professional Services Data; (c) Personal Data; and (d) any other data processed by Microsoft in connection with the Products and Services that is Customer's confidential information under Customer's agreement. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under Customer's agreement.

Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

Microsoft will only disclose or provide access to any Processed Data as required by law provided that the laws and practices respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society and, as applicable, to safeguard one of the objectives listed in Article 23(1) of GDPR.

Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.

Processing of Personal Data; GDPR

All Personal Data processed by Microsoft in connection with providing the Products and Services is obtained as part of either (a) Customer Data, (b) Professional Services Data, or (c) data generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by Microsoft from locally installed software. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Professional Services is also Professional Services Data. Pseudonymized identifiers may be included in data processed by Microsoft in connection with providing the Products and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in Attachment 1 govern, and the language in the sub-section ("Processing of Personal Data; GDPR") shall be deemed supplemental:

Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in the Product-specific terms or this DPA. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that Customer's agreement (including the DPA Terms and any applicable updates), along with the product documentation and Customer's use and configuration of features in the Products, are Customer's complete documented instructions to Microsoft for the processing of Personal Data, or the Professional Services documentation and Customer's use of the Professional Services. Information on use and configuration of the Products can be found at https://docs.microsoft.com (or a successor location) or other agreement incorporating this DPA. Any additional or alternate instructions must be agreed to according to the process for amending Customer's agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Microsoft that Customer's instructions, including appointment of Microsoft as a processor or subprocessor, have been authorized by the relevant controller.

To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR for business operations incident to providing the Products and Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use. Microsoft is accepting the added responsibilities of a data "controller" under GDPR for such processing to: (a) act consistent with regulatory requirements, to the extent required under GDPR; and (b) provide increased transparency to Customers and confirm Microsoft's accountability for such processing. Microsoft employs safeguards to protect Customer Data, Professional Services Data, and Personal Data in such processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR. With respect to processing of Personal Data under this paragraph, Microsoft makes the commitments set forth in the Additional Safeguards section; for those purposes, (i) any Microsoft disclosure of Personal Data, as described in the Additional Safeguards section, that has been transferred in connection with business operations is deemed a "Relevant Disclosure" and (ii) the commitments in the Additional Safeguards section apply to such Personal Data.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled "Nature of Data Processing; Ownership" above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Products and Services pursuant to Customer's agreement and for business operations incident to providing the Products and Services to Customer (as further described in the section of this DPA entitled "Nature of Data Processing; Ownership" above).
- **Categories of Data.** The types of Personal Data processed by Microsoft when providing the Products and Services include: (i) Personal Data that Customer elects to include in Customer Data and Professional Services Data; and (ii) those expressly identified in Article 4 of the GDPR that may be generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by Microsoft from locally installed software. The types of Personal Data that Customer elects to include in Customer Data and Professional Services Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Appendix B.

- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix B.

Data Subject Rights; Assistance with Requests

Microsoft will make available to Customer, in a manner consistent with the functionality of the Products and Services and Microsoft's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Microsoft receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with the Products and Services for which Microsoft is a data processor or subprocessor, Microsoft will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Products and Services. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires Microsoft to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Microsoft and keep it accurate and up-to-date. Microsoft may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data, Professional Services Data, and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. A description of the security controls for these requirements is available to Customers.

Each Core Online Service also complies with the control standards and frameworks shown in the table in the Product Terms. Each Core Online Service and Professional Service implements and maintains the security measures set forth in Appendix A for the protection of Customer Data and Professional Services Data.

Microsoft implements and maintains the security measures set forth in Annex II of the 2021 Standard Contractual Clauses for the protection of Personal Data within the scope of the GDPR.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate ISO 27001, ISO 27002, ISO 27018 or any standard or framework in the table for Core Online Services in the Product Terms, unless it is no longer used in the industry and it is replaced with a successor (if any).

Data Encryption

Customer Data and Professional Services Data (each including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default.

Microsoft also encrypts Customer Data stored at rest in Online Services and Professional Services Data stored at rest. In the case of Online Services on which Customer or a third-party acting on Customer's behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties.

Data Access

Microsoft employs least privilege access mechanisms to control access to Customer Data and Professional Services Data (including any Personal Data therein). Role-based access controls are employed to ensure that access to Customer Data and Professional Services Data required for service operations is for an appropriate purpose and approved with management oversight. For Core Online Services and Professional Services, Microsoft maintains Access Control mechanisms described in the table entitled "Security Measures" in Appendix A; and there is no standing access by Microsoft personnel to Customer Data, and any required access is for a limited time.

Customer Responsibilities

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for Products and Services meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by

Microsoft provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer's virtual machine or application).

Auditing Compliance

Microsoft will conduct audits of the security of the computers, computing environment, and physical data centers that it uses in processing Customer Data, Professional Service Data, and Personal Data, as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at https://servicetrust.microsoft.com/ or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor. If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

To the extent Customer's audit requirements under the Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, Microsoft will promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and Microsoft will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Microsoft to unreasonably delay performance of the audit. To the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data, Professional Services Data, and Personal Data by Microsoft, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Microsoft, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Microsoft's other customers or to Microsoft systems or facilities not involved in providing the applicable Products and Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Microsoft expends for any such audit, in addition to the rates for services performed by Microsoft. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material non-compliance.

Nothing in this section of the DPA varies or modifies the GDPR Terms or affects any supervisory authority's or data subject's rights under the Data Protection Requirements. Microsoft Corporation is an intended third-party beneficiary of this section.

Security Incident Notification

If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, Professional Services Data, or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to Customer by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer maintains accurate contact information with Microsoft for each applicable Product and Professional Service. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Microsoft's notification of or response to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Products and Services.

Data Transfers and Location

Data Transfers

Customer Data, Professional Services Data, and Personal Data that Microsoft processes on Customer's behalf may not be transferred to, or stored and processed in a geographic location except in accordance with the DPA Terms and the safeguards provided below in this section.

Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms.

All transfers of Customer Data, Professional Services Data, and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Products and Services are subject to the terms of the 2021 Standard Contractual Clauses implemented by Microsoft. In addition, transfers from the United Kingdom are subject to the terms of the IDTA implemented by Microsoft. For purposes of this DPA, the "IDTA" means the International data transfer addendum to the European Commission's standard contractual clauses for international data transfers issued by the UK Information Commissioner's Office under S119A(1) of the UK Data Protection Act 2018. Microsoft will abide by the requirements of European Economic Area, United Kingdom, and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, Microsoft is certified to the EU-U.S. and Swiss-U.S. Data Privacy Frameworks, the UK Extension to the EU-U.S. Data Privacy Framework and the commitments they entail. Microsoft agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the principles of the Data Privacy Frameworks.

Location of Customer Data

For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as set forth in the Product Terms.

For EU Data Boundary Online Services, Microsoft will store and process Customer Data and Personal Data within the European Union as set forth in the Product Terms.

Microsoft does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

Data Retention and Deletion

At all times during the term of Customer's subscription or the applicable Professional Services engagement, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service and Professional Services Data.

Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless authorized under this DPA to retain such data.

For Personal Data in connection with the Software and for Professional Services Data, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon Customer's request, unless authorized under this DPA to retain such data.

The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data, Professional Services Data, or Personal Data as described in this section.

Processor Confidentiality Commitment

Microsoft will ensure that its personnel engaged in the processing of Customer Data, Professional Services Data, and Personal Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Customer Data, Professional Services Data, and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors

Microsoft may hire Subprocessors to provide certain limited or ancillary services on its behalf. Customer consents to this engagement and to Microsoft Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Microsoft of the processing of Customer Data, Professional Services Data, and Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Microsoft is responsible for its Subprocessors' compliance with Microsoft's obligations in this DPA. Microsoft makes available information about Subprocessors on a Microsoft website. When engaging any Subprocessor, Microsoft will ensure via a written contract that the Subprocessor may access and use Customer Data, Professional Services Data, or Personal Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Customer Data, Professional Services Data, or Personal Data for any other purpose. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the

DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice and, as applicable, update the website and provide Customer with a mechanism to obtain notice of that update of any new Subprocessor at least 6 months in advance of providing that Subprocessor with access to Customer Data. Additionally, Microsoft will give Customer notice and, as applicable, update the website and provide Customer with a mechanism to obtain notice of that update of any new Subprocessor at least 30 days in advance of providing that Subprocessor with access to Professional Services Data or Personal Data other than that which is contained in Customer Data. If Microsoft engages a new Subprocessor for a new Product or Professional Service that processes Customer Data, Professional Services Data, or Personal Data, Microsoft will give Customer notice prior to availability of that Product or Professional Service.

If Customer does not approve of a new Subprocessor for an Online Service or Professional Services, then Customer may terminate any subscription for the affected Online Service or the applicable Statements of Service for the applicable Professional Service, respectively, without penalty or termination fee by providing, before the end of the relevant notice period, written notice of termination. If Customer does not approve of a new Subprocessor for Software, and Customer cannot reasonably avoid use of the Subprocessor by restricting Microsoft from processing data as set forth in the documentation or this DPA, then Customer may terminate any license for the affected software product without penalty by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Microsoft to re-evaluate any such new Subprocessor based on the applicable concerns. If the affected Product is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for any subscriptions or other applicable unpaid work for the terminated Products or Services from subsequent invoices to Customer or its reseller.

Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Microsoft acknowledges that for the purposes of the DPA, Microsoft is a "school official" with "legitimate educational interests" in the Customer Data and Professional Services Data, as those terms have been defined under FERPA and its implementing regulations, and Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that Microsoft may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Products and Services that may be required by applicable law and to convey notification on behalf of Microsoft to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data and Professional Services Data in Microsoft's possession as may be required under applicable law.

CJIS Customer Agreement

Microsoft provides certain government cloud services ("Covered Services") in accordance with the FBI Criminal Justice Information Services ("CJIS") Security Policy ("CJIS Policy"). The CJIS Policy governs the use and transmission of criminal justice information. All Microsoft CJIS Covered Services shall be governed by the terms and conditions in the CJIS Management Agreement.

HIPAA Business Associate

If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data or Professional Services Data, as those terms are defined under the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations promulgated thereunder (collectively, "HIPAA"), execution of Customer's agreement includes execution of the HIPAA Business Associate Agreement ("BAA").The full text of the BAA identifies the Online Services or Professional Services to which it applies and is available at http://aka.ms/BAA. Customer may opt out of the BAA by sending the following information to Microsoft in a written notice (under the terms of the Customer's agreement):

- the full legal name of the Customer and any Affiliate that is opting out; and
- if Customer has multiple agreements, Customer's agreement to which the opt out applies.

Telecommunication Data

To the extent Microsoft is processing traffic, content and other Personal Data in the provision of Products and Services that qualify as telecommunication services under applicable law, specific statutory obligations may apply. Microsoft will comply with all telecommunication specific laws and regulations applicable to its providing the Products and Services, including security breach notification, Data Protection Requirements, and telecommunication secrecy.

California Consumer Privacy Act (CCPA)

If Microsoft is processing Personal Data within the scope of the CCPA, Microsoft makes the following additional commitments to Customer. Microsoft will process Customer Data, Professional Services Data, and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any "sale"

exemption. In no event will Microsoft sell any such data. These CCPA terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the DPA Terms, Product Terms, or other agreement between Microsoft and Customer.

Biometric Data

If Customer uses Products and Services to process Biometric Data, Customer is responsible for: (i) providing notice to data subjects, including with respect to retention periods and destruction; (ii) obtaining consent from data subjects; and (iii) deleting the Biometric Data, all as appropriate and required under applicable Data Protection Requirements. Microsoft will process that Biometric Data following Customer's documented instructions (as described in the "Processor and Controller Roles and Responsibilities" section above) and protect that Biometric Data in accordance with the data security and protection terms under this DPA. For purposes of this section, "Biometric Data" will have the meaning set forth in Article 4 of the GDPR and, if applicable, equivalent terms in other Data Protection Requirements.

Supplemental Professional Services

When used in the sections listed below, the defined term "Professional Services" includes Supplemental Professional Services, and the defined term "Professional Services Data" includes data obtained for Supplemental Professional Services.

For Supplemental Professional Services, the following sections of the DPA apply in the same manner as they apply to Professional Services: "Introduction", "Compliance with Laws", "Nature of Processing; Ownership", "Disclosure of Processed Data", "Processing of Personal Data; GDPR", the first paragraph of "Security Practices and Policies", "Customer Responsibilities", "Security Incident Notification", "Data Transfer" (including the terms regarding the 2021 Standard Contractual Clauses), the third paragraph of "Data Retention and Deletion", "Processor Confidentiality Commitment", "Notice and Controls on use of Subprocessors", "HIPAA Business Associate" (to the extent applicable in the BAA), "California Consumer Privacy Act (CCPA)", "Biometric Data", "How to Contact Microsoft", "Appendix B – Data Subjects and Categories of Personal Data", and "Appendix C – Additional Safeguards Addendum".

How to Contact Microsoft

If Customer believes that Microsoft is not adhering to its privacy or security commitments, Customer may contact customer support or use Microsoft's Privacy web form, located at http://go.microsoft.com/?linkid=9846224. Microsoft's mailing address is:

Microsoft Enterprise Service Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. The privacy representative of Microsoft Ireland Operations Limited can be reached at the following address:

Microsoft Ireland Operations, Ltd.
Attn: Data Protection
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

Appendix A – Security Measures

Microsoft has implemented and will maintain for Customer Data in the Core Online Services and Professional Services Data the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms), are Microsoft's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership**. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. Microsoft personnel with access to Customer Data or Professional Services Data are subject to confidentiality obligations. **Risk Management Program**. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service and before processing Professional Service Data or launching the Professional Services. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory**. Microsoft maintains an inventory of all media on which Customer Data or Professional Services Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling** - Microsoft classifies Customer Data and Professional Services Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and Professional Services Data and has procedures for disposing of printed materials that contain such data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data or Professional Services Data on portable devices, remotely accessing such data, or processing such data outside Microsoft's facilities.
Human Resources Security	**Security Training**. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. Microsoft limits access to facilities where information systems that process Customer Data or Professional Services Data are located to identified authorized individuals. **Physical Access to Components**. Microsoft maintains records of the incoming and outgoing media containing Customer Data or Professional Services Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such data they contain. **Protection from Disruptions**. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. Microsoft uses industry standard processes to delete Customer Data and Professional Services Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data or Professional Services Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Microsoft maintains multiple copies of Customer Data and Professional Services Data from which such data can be recovered. - Microsoft stores copies of Customer Data and Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Professional Services Data are located. - Microsoft has specific procedures in place governing access to copies of Customer Data and Professional Services Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Professional Services and for Azure Government Services, which are reviewed every twelve months.

Domain	Practices
	- Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data and Professional Services Data, including malicious software originating from public networks. **Data Beyond Boundaries** - Microsoft encrypts, or enables Customer to encrypt, Customer Data and Professional Services Data that is transmitted over public networks. - Microsoft restricts access to Customer Data and Professional Services Data in media leaving its facilities. **Event Logging**. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data or Professional Services Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Customer Data or Professional Services Data. **Access Authorization** - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data or Professional Services Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Customer Data or Professional Services Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data and Professional Services Data when needed. - Microsoft restricts access to Customer Data and Professional Services Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data or Professional Services Data they are not authorized to access.

Domain	Practices
Information Security Incident Management	**Incident Response Process** - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data and Professional Services Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data or Professional Services Data are located. - Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data and Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed.

Appendix B – Data Subjects and Categories of Personal Data

Data subjects: Data subjects include the Customer's representatives and end-users including employees, contractors, collaborators, and customers of the Customer. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by Microsoft. Microsoft acknowledges that, depending on Customer's use of the Products and Services, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors and temporary workers (current, former, prospective) of Customer;
- Dependents of the above;
- Customer's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of Customer's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the Customer and/or use communication tools such as apps and websites provided by the Customer;
- Stakeholders or individuals who passively interact with Customer (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the Customer);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of data: The personal data that is included in e-mail, documents and other data in an electronic form in the context of the Products and Services. Microsoft acknowledges that, depending on Customer's use of the Products and Services, Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);

- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified in Article 4 of the GDPR.

Appendix C – Additional Safeguards Addendum

By this Additional Safeguards Addendum to the DPA (this "Addendum"), Microsoft provides additional safeguards to Customer for the processing of personal data, within the scope of the GDPR, by Microsoft on behalf of Customer and additional redress to the data subjects to whom that personal data relates.

This Addendum supplements and is made part of, but is not in variation or modification of, the DPA.

1. **Challenges to Orders**. In the event Microsoft receives an order from any third party for compelled disclosure of any personal data processed under this DPA, Microsoft shall:

   a. use every reasonable effort to redirect the third party to request data directly from Customer;

   b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and

   c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with applicable law of the European Union or applicable Member State law.

If, after the steps described in a. through c. above, Microsoft or any of its affiliates remains compelled to disclose personal data, Microsoft will disclose only the minimum amount of that data necessary to satisfy the order for compelled disclosure.

For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2. **Indemnification of Data Subjects**. Subject to Sections 3 and 4, Microsoft shall indemnify a data subject for any material or non-material damage to the data subject caused by Microsoft's disclosure of personal data of the data subject that has been transferred in response to an order from a non-EU/EEA government body or law enforcement agency in violation of Microsoft's obligations under Chapter V of the GDPR (a "Relevant Disclosure"). Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under this Section 2 to the extent the data subject has already received compensation for the same damage, whether from Microsoft or otherwise.

3. **Conditions of Indemnification**. Indemnification under Section 2 is conditional upon the data subject establishing, to Microsoft's reasonable satisfaction, that:

   a. Microsoft engaged in a Relevant Disclosure;

   b. the Relevant Disclosure was the basis of an official proceeding by the non-EU/EEA government body or law enforcement agency against the data subject; and

   c. the Relevant Disclosure directly caused the data subject to suffer material or non-material damage.

The data subject bears the burden of proof with respect to conditions a. though c.

Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under Section 2 if Microsoft establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

4. **Scope of Damages**. Indemnification under Section 2 is limited to material and non material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Microsoft's infringement of the GDPR.

5. **Exercise of Rights**. Rights granted to data subjects under this Addendum may be enforced by the data subject against Microsoft irrespective of any restriction in Clauses 3 or 6 of the Standard Contractual Clauses. The data subject may only bring a claim under this Addendum on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Addendum are personal to the data subject and may not be assigned.

6. **Notice of Change**. Microsoft agrees and warrants that it has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the Customer and its obligations under this Addendum or the 2021 Standard Contractual Clauses and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum or the Standard Contractual Clauses, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract.

Attachment 1 – European Union General Data Protection Regulation Terms

Microsoft makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon Microsoft with regard to Customer regardless of (1) the version of the Product Terms and DPA that is otherwise applicable to any given Product subscription or license, or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Microsoft on behalf of Customer. These GDPR Terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the Product Terms or other agreement between Microsoft and Customer. These GDPR Terms do not apply where Microsoft is a controller of Personal Data.

Relevant GDPR Obligations: Articles 5, 28, 32, and 33

1. Microsoft supports Customer's accountability obligations via this DPA and the product documentation provided to Customer, and will continue to do so during the term of the term of Customer's subscription or the applicable Professional Services engagement pursuant to subsection 3(h) below. (Article 5(2))

2. Microsoft shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, Microsoft shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))

3. Processing by Microsoft shall be governed by these GDPR Terms under European Union (hereafter "Union") or Member State law and are binding on Microsoft with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer's licensing agreement, including these GDPR Terms. In particular, Microsoft shall:

(a) process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Microsoft is subject; in such a case, Microsoft shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) take all measures required pursuant to Article 32 of the GDPR;

(d) respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;

(e) taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

(f) assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Microsoft;

(g) at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;

(h) make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Microsoft shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

4. Where Microsoft engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Microsoft shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))

5. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and Microsoft shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))

6. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Article 32(2))

7. Customer and Microsoft shall take steps to ensure that any natural person acting under the authority of Customer or Microsoft who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4))

8. Microsoft shall notify Customer without undue delay after becoming aware of a Personal Data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Microsoft.

Table of Contents / General Terms

Appendix 6 – Microsoft Privacy Statement (extracts)

Microsoft Privacy Statement – Microsoft privacy

[Captured 12/07/2024]

Products provided by your organisation – notice to end users

If you use a Microsoft product with an account provided by an organisation you are affiliated with, such as your work or school account, that organisation can:

- Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.
- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

If you lose access to your work or school account (in event of change of employment, for example), you may lose access to products and the content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such products.

Many Microsoft products are intended for use by organisations, such as schools and businesses. Please see the Enterprise and developer products section of this privacy statement. If your organisation provides you with access to Microsoft products, your use of the Microsoft products is subject to your organisation's policies, if any. You should direct your privacy enquiries, including any requests to exercise your data protection rights, to your organisation's administrator. When you use social features in Microsoft products, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation or help content specific to the Microsoft product. Microsoft is not responsible for the privacy or security practices of our customers, which may differ from those set forth in this privacy statement.

When you use a Microsoft product provided by your organisation, Microsoft's processing of your personal data in connection with that product is governed by a contract between Microsoft and your organisation. Microsoft processes your personal data to provide the product to your organisation and you, and in some cases for Microsoft's business operations related to providing the product as described in the Enterprise and developer products section. As mentioned above, if you have questions about Microsoft's processing of your personal data in connection with providing products to your organisation, please contact your organisation. If you have questions about Microsoft's business operations in connection with providing products to your organisation as provided in the Product Terms, please contact Microsoft as described in the How to contact us section. For more information on our business operations, please see the Enterprise and developer products section.

For Microsoft products provided by your K-12 school, including Microsoft 365 Education, Microsoft will:

- not collect or use student personal data beyond that needed for authorised educational or school purposes;
- not sell or rent student personal data;
- not use or share student personal data for advertising or similar commercial purposes, such as behavioural targeting of advertisements to students;
- not build a personal profile of a student, other than for supporting authorised educational or school purposes or as authorised by the parent, guardian or student of appropriate age; and
- require that our vendors with whom student personal data is shared to deliver the educational service, if any, are obligated to implement these same commitments for student personal data.

Artificial Intelligence and Microsoft Copilot capabilities

Microsoft leverages the power of artificial intelligence (AI) in many of our products and services, including by incorporating generative AI features such as Microsoft Copilot capabilities. Microsoft's deployment and use of AI is subject to Microsoft's AI Principles and Microsoft's Responsible AI Standard, and Microsoft's collection and use of personal data in developing and deploying AI features is consistent with commitments outlined in this privacy statement. Product-specific details provide additional relevant information. You can find out more about how Microsoft uses AI here.

Microsoft Copilot capabilities. Microsoft Copilot is Microsoft's everyday AI companion, and is designed to help you achieve more through a single experience that runs across devices, understanding relevant context on the web, on your PC, and across apps to bring you the right skills at the right time. With the help of Copilot, users can start a draft of a new Word document, generate a PowerPoint presentation, quickly find the answers to complex search queries online, find relevant documents or other personal content, or be inspired to create new songs, stories, images or other content, among other tasks. Copilot is a family of services, and Microsoft's collection and use of data may differ depending on the service and the intended functionality in a given scenario.

The Copilot website and app (available on iOS and Android) is the core of the consumer Copilot experience. Within this core experience, users can search the web, create text, images, songs, or other outputs, or engage with other features, such as plugins. On the website and in the app, users enter "prompts" that provide instructions to Copilot (e.g. "Give me recommendations for a restaurant that accommodates parties of 10 near me"). In order to provide a relevant response, Copilot will use this prompt, along with the user's location, language and similar settings, to formulate a helpful response. In some markets, authenticated users can choose to allow Copilot to have access to prior prompt

history to better personalise the product. The consumer Copilot product uses the data collected to provide and improve the Copilot services, including to provide relevant advertising. Users who are signed-in to their account can manage their prompt history in product and on the Microsoft Privacy Dashboard, and can adjust their location, language, and other settings in the product.

Copilot also appears as an assistant within other Microsoft consumer products, such as Bing and Microsoft Edge. In those situations, data processing activities generally align with those products' primary uses. For example, Copilot in Bing's use and collection of personal data is consistent with Bing's core web search offering as described in the Search and Browse section of this privacy statement. More information about Copilot in Bing is available at Copilot in Bing: Our approach to Responsible AI. In Microsoft Edge, Copilot appears in the sidebar experience and can help the user complete tasks related to the webpages they visit (e.g. "summarise this page"). This data is used consistent with the Microsoft Edge section of this privacy statement.

Copilot Pro is another consumer Copilot offering, and offers subscribers priority access to the very latest models, improved image creation abilities and access to Copilot in Microsoft Word, PowerPoint, OneNote, Excel and Outlook. The main Copilot Pro website and app has similar data collection, use and controls as consumer Copilot, as described above. When Copilot is integrated with Microsoft 365 products, Copilot data collection is consistent with how data collection and use is described in the Productivity and Communications section of this privacy statement.

There are also Copilot offerings designed for enterprise users. When enabled by an eligible enterprise, users logged in with their Entra ID who want to access consumer Copilot services are offered Copilot with Commercial Data Protection, which minimises data collection and use consistent with the expectations of enterprise users. More information on Copilot with Commercial Data Protection is available here.

Microsoft Copilot for Microsoft 365 enterprise offers enterprise-grade data protection along with access to the corporate graph, Copilot within Microsoft 365 and Teams, and additional customisation features. Data collection and use in Copilot for Microsoft 365 enterprise is consistent with the practices described in the Enterprise and Developer Products section of this privacy statement.

Top of page

Enterprise and developer products

Enterprise and Developer Products are Microsoft products and related software offered to and designed primarily for use by organisations and developers. They include:

- Cloud services, referred to as Online Services in the Product Terms, such as Microsoft 365 and Office 365, Microsoft Azure, Microsoft Dynamics365 and Microsoft Intune for which an organisation (our customer) contracts with Microsoft for the services ("Enterprise Online Services").
- Other enterprise and developer tools and cloud-based services, such as Azure PlayFab Services (to learn more see Azure PlayFab Terms of Service).
- Server, developer and hybrid cloud platform products, such as Windows Server, SQL Server, Visual Studio, System Centre, Azure Stack and open source software like Bot Framework solutions ("Enterprise and Developer Software").
- Appliances and hardware used for storage infrastructure, such as StorSimple ("Enterprise Appliances").
- Professional services referred to in the Product Terms that are available with Enterprise Online Services, such as onboarding services, data migration services, data science services, or services to supplement existing features in the Enterprise Online Services.

In the event of a conflict between this Microsoft privacy statement and the terms of any agreement(s) between a customer and Microsoft for Enterprise and Developer Products, the terms of those agreement(s) will control.

You can also learn more about our Enterprise and Developer Products' features and settings, including choices that impact your privacy or your end users' privacy, in product documentation.

If any of the terms below are not defined in this Privacy Statement or the Product Terms, they have the definitions below.

General. When a customer tries, purchases, uses, or subscribes to Enterprise and Developer Products, or obtains support for or professional services with such products, Microsoft receives data from you and collects and generates data to provide the service (including improving, securing, and updating the service), conduct our business operations, and communicate with the customer. For example:

- When a customer engages with a Microsoft sales representative, we collect the customer's name and contact data, along with information about the customer's organisation, to support that engagement.
- When a customer interacts with a Microsoft support professional, we collect device and usage data or error reports to diagnose and resolve problems.
- When a customer pays for products, we collect contact and payment data to process the payment.
- When Microsoft sends communications to a customer, we use data to personalise the content of the communication.
- When a customer engages with Microsoft for professional services, we collect the name and contact data of the customer's designated point of contact and use information provided by the customer to perform the services that the customer has requested.

The Enterprise and Developer Products enable you to purchase, subscribe to, or use other products and online services from Microsoft or third parties with different privacy practices, and those other products and online services are governed by their respective privacy statements and policies.

View Summary

Top of page

Enterprise online services

To provide the Enterprise Online Services, Microsoft uses data you provide (including Customer Data, Personal Data, Administrator Data, Payment Data, and Support Data) and data Microsoft collects or generates associated with your use of the Enterprise Online Services. We process data as described in the Product Terms, Microsoft Products and Services Data Protection Addendum (Products and Services DPA), and the Microsoft Trust Centre.

Personal Data. Customer is the controller of Personal Data and Microsoft is the processor of such data, except when (a) Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor or (b) as stated otherwise in the standard Products and Services DPA. In addition, as provided in the standard Products and Services DPA, Microsoft has taken on the added responsibilities of a data controller under GDPR when processing Personal Data in connection with its business operations incident to providing its services to Microsoft's commercial customers, such as billing and account management, compensation, internal reporting and business modelling, and financial reporting. We use Personal Data in the least identifiable form that will support processing necessary for these business operations. We rely on statistical data and aggregate pseudonymized Personal Data before using it for our business operations, removing the ability to identify specific individuals.

Administrator Data. Administrator Data is the information provided to Microsoft during sign-up, purchase, or administration of Enterprise Online Services. We use Administrator Data to provide the Enterprise Online Services, complete transactions, service the account, detect and prevent fraud, and comply with our legal obligations. Administrator Data includes the name, address, phone number, and email address you provide, as well as aggregated usage data related to your account, such as the controls you select. Administrator Data also includes contact information of your colleagues and friends if you agree to provide it to Microsoft for the limited purpose of sending them an invitation to use the Enterprise Online Services; we contact those individuals with communications that include information about you, such as your name and profile photo.

As needed, we use Administrator Data to contact you to provide information about your account, subscriptions, billing, and updates to the Enterprise Online Services, including information about new features, security, or other technical issues. We also contact you regarding third-party enquiries we receive regarding use of the Enterprise Online Services, as described in your agreement. You cannot unsubscribe from these non-promotional communications. We may also contact you regarding information and offers about other products and services, or share your contact information with Microsoft's partners. When such a partner has specific services or solutions to meet your needs, or to

optimise your use of the Enterprise Online Services, we may share limited, aggregated information about your organisation's account with the partner. Microsoft will not share your confidential information or contact information with the authorised partner unless we have sufficient rights to do so. You can manage your contact preferences or update your information in your account profile.

Payment Data. We use payment data to complete transactions, as well as to detect and prevent fraud.

Support Data. Customers provide or authorise Microsoft to collect data in connection with obtaining technical support for the Enterprise Online Services. We process Support Data to provide technical support and as described in the Products and Services DPA.

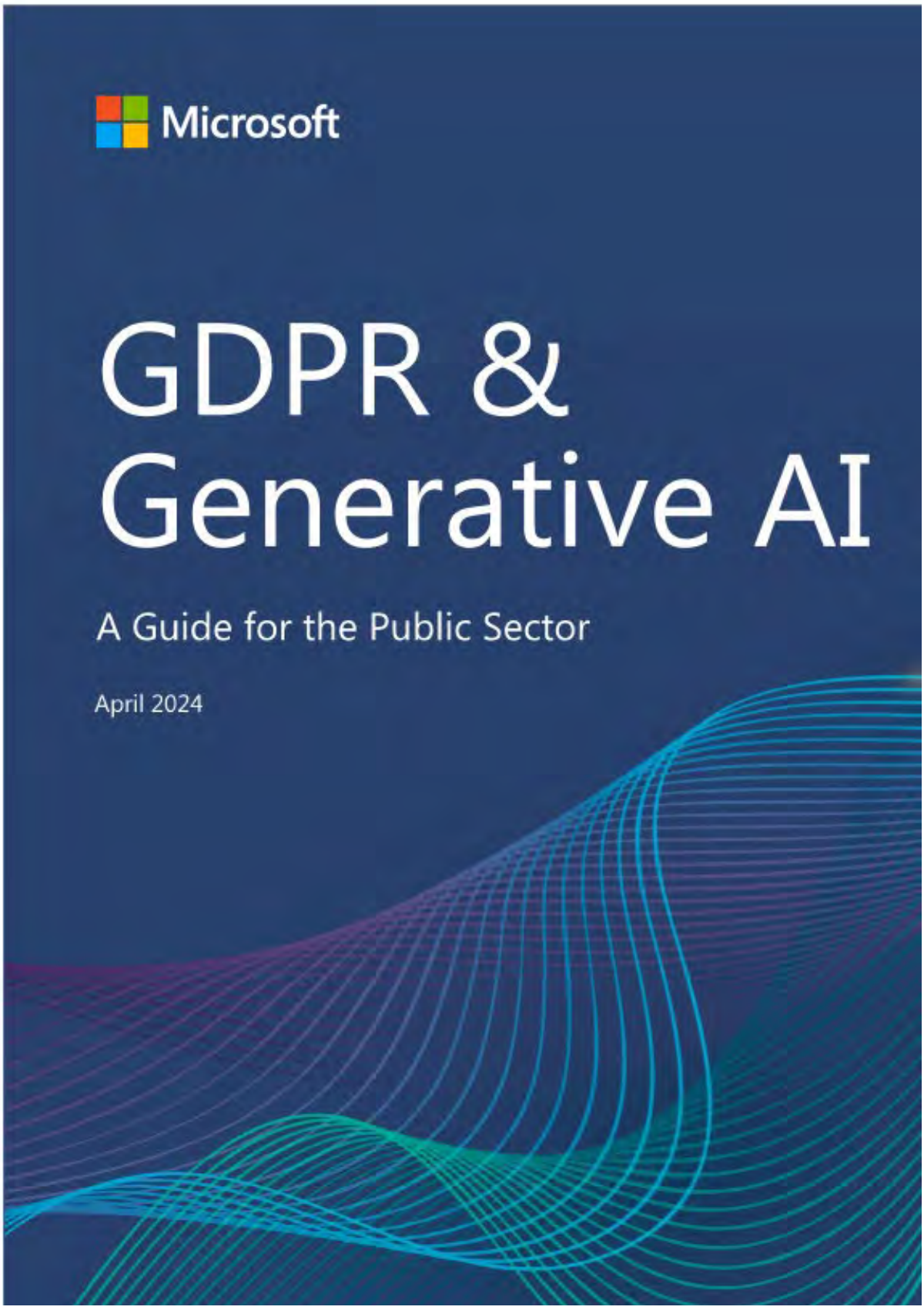
Local Software and Diagnostic Data. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications). The local software may collect Diagnostic Data (as defined in the Products and Services DPA) about the use and performance of that software. That data may be transmitted to Microsoft and used for the purposes described in the Products and Services DPA.

Bing Search Services Data. Bing Search Services, as defined in the Product Terms, use data such as search queries as described in the Bing section of this privacy statement.

Appendix 7 – GDPR and Generative AI, A Guide for the Public Sector

GDPR-and-Generative-AI-A-Guide-for-the-Public-Sector-FINAL.pdf (microsoft.com)

[Captured 12/07/2024


Microsoft
GDPR &
Generative AI
A Guide for the Public Sector
April 2024

Contents

Executive Summary

- The use cases for generative AI in the public sector present an exciting opportunity to improve the quality and efficiency of public services. At Microsoft we want to empower our customers to harness the full potential of new technologies like generative artificial intelligence (generative AI), while complying with their obligations under the General Data Protection Regulation (GDPR).

- Microsoft is committed to ensuring its AI systems are developed responsibly and in a way that is worthy of people's trust. We drive this commitment according to six key principles which align closely with public sector priorities and the fundamental principles set out in Article 5 of the GDPR.

- When considering GDPR compliance in the context of the procurement and use of generative AI services, the fundamental principles of the GDPR apply in the same manner as they do for processing personal data in any other context (e.g. the use of cloud services). So, while AI technology may be new, the principles and accordingly the processes for risk assessment and compliance with the GDPR remain the same. Hence, to ensure GDPR compliance, public sector organizations should be confident to approach Microsoft's AI services in the same way as they have approached procuring other cloud services.

- Microsoft's existing privacy commitments including those provided in Microsoft's Data Protection Addendum extend to our AI commercial products. Public sector customers can rest assured that the privacy commitments they have long relied on when using our enterprise cloud products also apply to Copilot for Microsoft 365 and

- There are a number of key the GDPR which public sec need to consider when pro AI services. In this paper w details of these obligation associated support and re Microsoft can offer includi to international transfers o transparency, data subject obligations, technical and security measures, and DP

- Our customers' data belon customers. Microsoft does ownership of any custome output content created by generative AI solutions. In Customer Data (including content) is used to train fo without customer permissi

- As the regulatory landscap we innovate to provide ne solutions, Microsoft will co industry-leading tools, res to demonstrate our enduri to meeting the needs and European public sector cu journey.

Introduction

As technologies evolve, so too do the ways in which public sector organizations can embrace digital transformation technologies to help deliver on their responsibilities. It is clear that governments need to accelerate their digital and technological capabilities to meet citizen demands, while operating with often constrained budgets. Citizens increasingly expect faster, more personalised services, with an experience similar to those made available by the private sector. In response, government departments are motivated to take advantage of the efficiencies seen in other industries that have been realized by harnessing the potential of digital transformation technologies.

Effective public service delivery is both a responsibility and an opportunity for governments. Ultimately it means working efficiently with the resources available, delivering great outcomes for society, while safeguarding people's privacy and wellbeing. Getting this balance "right", requires an understanding of the

At Microsoft we want to empowe
harness the full potential of new t
generative AI, while complying wi
under the GDPR to ensure the pri
citizens' and public institutions' d

We have a long-standing practice
customers' information. Our appr
AI is built on a foundation of priv
dedicated to upholding core valu
and safety in all our generative AI
solutions. As the use of AI solutio
customers can be confident that t
is safeguarded by industry-leadin
and privacy practices in one of th
on the market today. Public secto
assured that the privacy commitm
relied on when using our enterpri
also apply to our enterprise gene
that are backed by the Microsoft's

This paper is set out as follows:

Part 1

Examines the meaning of responsible AI in the public sector context, the six key principles and our approach to responsible AI that guides Microsoft's development of AI products, and demonstrates the tools and resources Microsoft offers to assist your AI deployment.

Part 2

Shifts focus to the structure and requirements of the GDPR and how Microsoft can support public sector customers to embrace our AI solutions while continuing to meet their compliance obligations under the GDPR.

Parts 3 and 4

Are dedicated to an in-depth exploration of Copilot for Microsoft 365 and the Azure OpenAI Service, and how these services can be utilized in compliance with the GDPR.

Part 5

Concludes the paper, reflecting o
and the future trajectory of AI for

Appendix 1

Showcases some of the exciting o
generative AI presents for the pul

Appendix 2

Addresses some frequently asked
that public sector organizations h
embracing AI in a GDPR-compliar

Appendix 3

Provides links to additional resou
sector customers can reference to
expand their understanding of th
provided in this paper.

Part 1:

Responsibly using AI in the Public Sector -
Microsoft's AI journey and leveraging our tools and resources

Responsible AI in the Public Sector

AI has the potential to transform the public sector, from improving healthcare and education to enhancing public safety and transportation. The growing interest in generative AI is clear. However, with this 'great power comes great responsibility', and it is therefore essential that AI is developed and deployed responsibly. Microsoft has taken a principled role in this area with the development of comprehensive AI responsibility policies and tools, grounded on work we have been doing for many years.

The responsible use of AI is, of course, a topic which public sector organizations around the world have actively addressed in recent years. Through leading discussions, developing approaches and strategies, and implementing these in their operations, the use of AI to responsibly deliver more effective and inclusive public services is on the rise.

Learn more about Governing AI

At Microsoft, we are committed to making sure AI systems are developed responsibly and in a way that is worthy of people's trust. We drive this commitment according to **six key principles** which align closely with public sector priorities and the fundamental principles set out in **Article 5 of the GDPR:**

- **Fairness:** AI systems should be designed to treat all individuals fairly, without bias or discrimination.
- **Reliability and safety:** AI systems should be reliable and safe, with built-in mechanisms to prevent errors and minimize harm.

These principles can be used by p
organizations to evaluate AI syste
in use or under consideration in t
GDPR, as explored in Part 2 below
we have established our Office of
which sets AI governance policies
company, advises our senior lead
issues, enables engineering and c
across the company to build acco
AI principles, all while ensuring th
we are continuing to examine and
stance as new capabilities and ch

Learn more about Microsoft's prin
to Responsible AI

In June 2022, we published our in
Responsible AI Standard for prod
share what we've learned so far in
and actionable guidelines. We bel
academia, civil society, and gover
collaborate to advance the state-
from one another.

Public sector organizations shoul
governed by responsible AI strate
strategies should incorporate prin
tools, and governance to enable t
organization to assess, adopt, and
of AI.

When potential risks are understo
managed, the public sector can re
of AI. Forward-looking leaders wil
commitment to responsible AI is
but is baked into their organizatio
pipeline. This allows the public se

Tools, Commitments, and Resources to Assist your AI Deployment

To support our customers and empower their compliant use of AI, Microsoft offers a range of solutions, tooling, and resources to assist in their AI deployment. From comprehensive transparency documentation to a suite of tools for data governance, risk, and compliance assessment. Dedicated programs such as our industry-leading AI Assurance Program and AI Customer Commitments further broaden the support we offer public sector customers in addressing their needs.

Microsoft's AI Assurance Program helps customers ensure that the AI applications they deploy on our platforms meet the legal and regulatory requirements for responsible AI. The program includes support for regulatory engagement and advocacy, risk framework implementation and the creation of a customer council.

For decades we've defended our
intellectual property claims relatir
Building on our previous AI Custo
Microsoft announced our Custom
Commitment, which extends our
indemnity support to both Copilo
and our Azure OpenAI Service. N
a customer for copyright infringe
for Microsoft 365 or the Azure Op
the output they generate, we will
and pay the amount of any adver
settlements that result from the la
customer has used the guardrails
have built into our products.

Microsoft has also developed a ra
support our customers with data
Microsoft Purview. You can find fu
Microsoft Purview can support co
in Part 2.

Part 2:

The GDPR Compliance Framework in the Context of AI

What is the GDPR and who does it apply to?

The General Data Protection Regulation also known as the "GDPR"[1] sets an important bar globally for privacy rights, information security, and compliance. At Microsoft, we value privacy as a fundamental right, and we believe that the GDPR plays an important role in protecting and enabling the privacy rights of individuals.

Microsoft is committed to its own compliance with the GDPR, and providing an array of products, features, documentation, and resources to support our customers in meeting their compliance obligations under the GDPR.

The GDPR is in force in the UK and all EU countries and imposes a set of data protection rules on the processing of personal data, with the goal to protect the fundamental rights of data subjects and create a level playing field for the processing of personal data and further the internal market.

Any public sector organization that processes the personal data of data subjects residing in Europe is subject to the GDPR.[2] The national laws also incorporate data protection rules and guidelines. These are generally adapted to meet and/or exceed the requirements of the GDPR.

Leverage established principles to comply with regulatory frameworks when using AI solutions

When we think about the GDPR in the context of

including when using the cloud. S
technology may be new, the princ
the processes for risk assessment
the GDPR remain the same

It is also helpful to recognize that
drafted to be technology-agnosti
not prevent public sector organiz
embracing opportunities to use g

As such, applying established GDI
processes is a great way for publi
to harness the revolutionary pote
deliver great outcomes for society
people's privacy and wellbeing. M
standing history of collaborating
public sector organizations in pur
transformation priorities while co
requirements of the GDPR, includ
transition from on-premises to cl
Public sector organizations can ap
generative AI solutions by leverag
they have used in procuring our c

Cloud computing is essential for a
potentially groundbreaking AI tec
hyper-scale cloud is, therefore, th
deploying AI. Azure's enterprise-g
which form part of Copilot for Mi
Azure OpenAI Service provide a s
upon which public sector custom
data privacy, security, and compli
confidently scale AI while managi
compliance with the GDPR.

Who is responsible for GDPR compliance when using AI and cloud services?

Under the GDPR, there are two key parties each with a separate set of compliance responsibilities:

- **The Data Controller:** The data controller decides why and how personal data is processed and is the entity that is the principal subject of the obligations imposed by the GDPR. Many of these obligations apply from the moment this entity starts to collect personal data about individuals.
- **The Data Processor:** In contrast, under the GDPR, the data processor is essentially a subcontractor to the data controller, processing personal data on behalf of and upon instruction from the data controller.

Public sector organizations can act as data controllers and data processors in the GDPR context. When using Microsoft's generative AI services, Microsoft's Product Terms indicate whether Microsoft is providing an Online Service as a data processor or a data controller. Most of the Online Services, including generative AI services, are provided by Microsoft as a data processor and are governed by the Data Protection Addendum. For further details on specific products and services consult the Microsoft Product Terms.

Compliance with the GDPR is a shared responsibility

GDPR compliance is a shared responsibility. Microsoft is committed to complying with all laws and regulations which are applicable to Microsoft and its generative AI tools and services including the GDPR.

As a public sector organization, you will need to determine how these tools and services will be used

How does Microsoft su customers with their GI compliance obligations

As more public sector organizatio generative AI, many are looking t as a service provider, but as a trus journey to helping them to meet obligations under the GDPR.

The first step towards compliance how Microsoft's generative AI ser how they process personal data. transparency documentation and you understand how our AI tools choices our customers can make performance and behavior.

In Part 3 and Part 4 of this paper information and links to additiona you can use to help enhance your these products and services.

Jump to Part 3 to find out more a Microsoft 365

Jump to Part 4 to find out more a OpenAI Service

This knowledge provides the four compliance with a number of key the GDPR. We will explore these k the associated support that Micro later in this Part 2 but first we will core privacy commitments which customers in the AI era.

Protecting the data of our public sector customers - Microsoft's privacy commitments in the AI era

Microsoft's existing privacy commitments extend to our AI commercial products, as explained in a blog post from our Chief Privacy Officer Julie Brill. You can rest assured that the privacy commitments you have long relied on when using our enterprise cloud products also apply to our enterprise generative AI solutions that are backed by Microsoft's Data Protection Addendum, including Copilot for Microsoft 365 and Azure OpenAI Service.

The following seven commitments apply to "Customer Data", which is defined in Microsoft's Product Terms as all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, our customers through use of an online service. All inputs (including prompts)[3] and output content[4] are Customer Data. In accordance with Microsoft's Data Protection Addendum the customer "retains all right, title and interest in and to Customer Data".

1. We will keep your organization's data private.

Your data remains private when using Copilot for Microsoft 365 and Azure OpenAI Service and is governed by our applicable privacy and contractual commitments, including the commitments we make in Microsoft's Data Protection Addendum and Microsoft's Product Terms.

2. You are in control of your organization's data.

Your data is not used in undisclosed ways or without your permission. You may choose to customize your use of Copilot for Microsoft 365 or Azure OpenAI Service, opting to use your data to fine tune models for your organization's own use. If you do use your organization's data to fine tune, any fine-tuned AI solutions created with your organization's data will be available only to you.

3. Your access control and enterprise policies are maintained.

4. Your organization's data is nc

Microsoft does not share your dat without your permission. Your dat generated through your organiza for Microsoft 365 or Azure OpenA prompts and responses – are kep disclosed to third parties.

5. Your organization's data priv are protected by design.

Security and privacy are incorpora phases of design and implementa Microsoft 365 and Azure OpenAI our products, we provide a strong baseline and make available addit you can choose to enable. As exte we will continue to advance our s to ensure world-class privacy and for Microsoft 365 and Azure Oper will continue to be transparent ab

6. Your organization's data is nc foundation models.

Microsoft's generative AI solution Copilot for Microsoft 365 and Azu capabilities, do not use Customer foundation models without your data is never available to OpenAI OpenAI models.

7. Our products and solutions c data protection regulations.

The Microsoft AI products and sol are compliant with today's global privacy regulations. As we continu future of AI together, including th the EU AI Act and other global law be certain that Microsoft will be t privacy, safety, and security practi with global laws that govern AI, a promises with clear contractual c

You can find additional details ab privacy commitments apply to Az

Key obligations under the GDPR in the context of the procurement and use of generative AI services

There are a number of obligations under the GDPR which public sector organizations need to consider when procuring generative AI services. This section considers some of the key obligations and what associated support and resources Microsoft can offer to your organization to help you comply.

Articles 12 to 14 of the GDPR (Transparency)

Articles 12 to 14 of the GDPR require data controllers to provide data subjects with certain key information about how their personal data will be used. This information must be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. This information is often provided in the form of a privacy notice. If you deploy a new technology (such as Copilot for Microsoft 365 or Azure OpenAI Service) and intend to use such technology in a way that is not reflected in your existing privacy notices, then you will need to update your privacy notices to reflect these new processing activities.

How we help you comply: The information set out in this paper and available in our transparency resources noted below is intended to assist your understanding of how Copilot for Microsoft 365 and Azure OpenAI Service process data and the extent to which additional information (if any) needs to be communicated to data subjects. Additional product-specific information is available at Data, Privacy and Security for Azure OpenAI Service; Data, Privacy, and Security for Microsoft Copilot for Microsoft 365; Copilot in Dynamics 365 and Power Platform; and FAQs for Copilot data security and privacy for Dynamics 365 and Power Platform.

Articles 15 to 21 of t (Data Subject Rights)

Under the GDPR, data control they are in a position to comp obligation to respond to requ subjects relating to the exerci under Articles 15 to 21 of the appropriate assistance from d where necessary.

How we help you comply: In Subjects Rights; Assistance wi section of Microsoft's Data Pr Addendum, Microsoft commit available to customers (in a m with the functionality of the se Microsoft's role as a data proc to fulfil requests from data su their rights under the GDPR.

If Microsoft receives such a re from a data subject in situatio processing personal data on b organization, it will redirect th submit its request to your org You are responsible for respor such requests, but Microsoft w reasonable assistance request

Microsoft has developed addi to assist its customers when r data subject rights requests, s Purview and Purview eDiscov of these products empower o proactively govern their AI us to evolving regulatory require be valuable for instance to im in responding to and actionin relation to the "right to access and the "right to be forgotten Articles 15 and 17 of the GDP

Learn more about Microsoft P features and how these tools the deployment of Microsoft's

Article 28 of the GDPR (Processor Obligations)

The GDPR requires that where a public sector organization acts as a data controller that they only use data processors to process personal data on their behalf where they provide sufficient guarantees to meet key requirements of the GDPR. These key requirements are described in Article 28 of the GDPR and include that data processors commit to:

- only use subprocessors with the consent of the data controller and remain liable for subprocessors;
- process personal data only on instructions from the data controller, including with regard to transfers;
- ensure that persons who process personal data are committed to confidentiality;
- implement appropriate technical and organizational measures to ensure a level of personal data security appropriate to the risk;
- assist the data controller in its obligations to respond to data subjects' requests to exercise their GDPR rights;
- meet the GDPR's breach notification and assistance requirements;
- assist the data controller with data protection impact assessments and consultation with supervisory authorities;
- delete or return personal data at the end of provision of services; and
- support the data controller with evidence of compliance with the

In this context, it is important
the GDPR does not require da
create and use their own data
with their data processors. Th
Protection Board (EDPB) itself
is compliant to use a cloud pr
terms, subject to their compli
GDPR, and Article 28.[5]

A hyperscale cloud provider s
customers uniformly. The con
must accurately reflect how th
services operate and protect
Uniformity is standard in clou
makes cloud services more m
scalable, secure, and affordab
site solutions. In a multi-tenar
change imposed by one custo
all customers using the servic
problematic if customers have
mutually exclusive requiremer
introducing different security
or standards for different cust

Article 32 of the GDPR (Technical and Organizational Security Measures)

Article 32 of the GDPR requires data controllers and data processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk taking into account the nature, scope, context and purposes of the processing of personal data. These measures should address the risks associated with accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

How we help you comply: In the "Data Security" section of the Microsoft's Data Protection Addendum, Microsoft contractually commits to implement and maintain appropriate technical and organizational measures to protect "Customer Data" and "Personal Data" against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, such data transmitted, stored or otherwise processed.

Those technical measures are
Microsoft's Security Policy and
27001, ISO 27002 and ISO 27
contractually commits to encr
Data' (including any 'Personal
therein), in transit (including b
data centers) and at rest. App
Measures to Microsoft's Data
Addendum also contains com
commitments from Microsoft
the security of 'Customer Data
relation to the Organization o
Security, Asset Management,
Security, Physical and Environ
Communications and Operati
Information Security, Incident
Business Continuity Managem

The technical, organizational,
measures described above ap
Customer Data that customer
create when using Copilot for
and Azure OpenAI Service. Yo
information set out above to
commitment and measures ta
to protect Customer Data (inc
data).

Jump to Part 3 to find out mo
for Copilot for Microsoft 365

Jump to Part 4 to find out mo
for Azure OpenAI Service

Article 35 of the GDPR (Data Protection Impact Assessments)

Article 35 of the GDPR requires data controllers to undertake a data privacy impact assessment (DPIA) when processing personal data is likely to result in a high risk to the rights and freedoms of data subjects (particularly when this involves using new technologies).

When assessing whether a DPIA is required data controllers need to take into account the nature, scope, content and purposes of the processing. Therefore, whether a DPIA is required for the use of Copilot for Microsoft 365 and Azure OpenAI Service will depend on the particular use case and type of personal data which you wish to process using these services.

Learn more about when a DPIA must be completed

Even if it is not legally required, a DPIA is good practice and can help you work through the specific data protection risks associated with the implementation of Copilot for Microsoft 365 and/or Azure OpenAI Service for a specific use case. Preparing a DPIA may also assist you in meeting your accountability obligations under Article 5(2) of the GDPR.

A DPIA must contain at leas

(a) a systematic descript
envisaged processing op
the purposes of the proc

(b) an assessment of the
and proportionality of th
operations in relation to
purposes;

(c) an assessment of the
rights and freedoms of c
and

(d) the measures envisa
to address the risks, incl
safeguards, security mea
mechanisms to ensure th
of personal data and to
compliance with the GD
into account the rights a
interests of data subject
persons concerned.

Learn more about the content

How we help you comply: Th
contained in this paper and th
resources to which it refers ca
completing a DPIA. In particul
in:

- **Part 3 and Part 4** relati
Copilot for Microsoft 36
OpenAI Service process
assist with completing th
described in (a) above; a

- the sections on technica
organizational measures
Copilot for Microsoft 36
OpenAI Service will assi
completing the element
in (d) above.

The assessments described in
vary on a case-by-case basis c

Articles 44 to 50 of the GDPR (Transfers of Personal Data to Third Countries)

The GDPR permits personal data to be transferred to a third country outside of the EU or EEA (including the US) where certain conditions have been satisfied. These conditions include where there has been an adequacy decision by the European Commission or where appropriate additional safeguards (such as the EU Standard Contractual Clauses) have been put in place.

For public sector customers in the UK, the UK GDPR permits personal data to be transferred to a third country outside of the UK (including the US) where certain conditions have been satisfied. These conditions include where there has been an adequacy decision by the UK Secretary of State or where appropriate additional safeguards (such as the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK Addendum") have been put in place.

How we help you comply: All transfers of personal data by Microsoft outside of the UK, EU or EEA will be subject to a valid transfer mechanism under the GDPR, including transfers to the US.

The EU Commission and the UK Secretary of State have announced adequacy decisions finding that (for the purpose of Article 45 of the GDPR) the US ensures an appropriate level of protection for personal data transferred from the UK or EU to organizations in the US that are certified to the EU-U.S. Data Privacy Framework. Microsoft is certified under the EU-U.S. Data Privacy Framework and the commitments they entail. Microsoft is committed to embracing the framework and will go beyond it by meeting or exceeding all the requirements this framework outlines for our customers.

commitments to store and pr
data within the EU as specifie
Data Protection Addendum a
Product Terms, reducing trans
data to third countries thereb
GDPR compliance for transfer
countries. Both Copilot for Mi
Azure OpenAI Services are EU
services.

The EU Data Boundary is a ge
defined boundary (consisting
in the EU and the European Fr
Association) within which Mic
committed to store and proce
Data (including any personal
certain enterprise online servi
Data Boundary uses or may u
datacenters announced or cu
in Austria, Belgium, Denmark,
France, Germany, Greece, Irela
Netherlands, Norway, Poland,
and Switzerland. In the future,
establish datacenters in additi
located in the EU or EFTA to p
Boundary Services.

There are limited exceptions t
Data Boundary that may resul
processing Customer Data (in
data) outside of the EU Data B
this is the case, Microsoft relie
data transfer mechanisms as s
GDPR. Further details relating
circumstances can be found i
Product Terms.

Learn more about the EU Data

Jump to Part 3 to find out mo
Data Residency for Copilot fo

Jump to Part 4 to find out mo
Data Residency for Azure Ope

How does the GDPR interact with the AI Act ?

The GDPR and the AI Act are intended to be complementary and operate alongside each other providing a regulatory framework for AI products and services. The GDPR, which regulates the processing of personal data by controllers and data processors, focuses on data privacy and aims to give individuals control over their personal data.

The AI Act, which applies to providers, importers, distributers, users, and others involved in the AI lifecycle, aims to ensure that AI systems that are used in the EU respect fundamental rights, safety, and ethical principles, as well as address certain risks related to the most highly capable general-purpose AI models.

Find out more about the AI Act and its interaction with the GDPR in the Appendix 2: Frequently Asked Questions (FAQs).

Our continued compli
data protection regulat
dialogue with key regul
Europe and across the

As privacy and data protection la
and requirements evolve in Europ
globe; you can be certain that Mi
transparent about our privacy, saf
practices. We will comply with law
globally that govern AI, and back
clear contractual commitments.

Beyond adhering to the GDPR an
requirements applicable to us, Mi
an open dialogue with its custom
regulatory authorities to better u
address evolving privacy and data

We continue to work closely with
authorities and privacy regulators
to share information about how o
work thereby fostering an enviro
cooperation.

Part 3:

Copilot for Microsoft 365

Understanding the potential of generative AI services and how these products and services operate and use personal data is the foundation for compliance with a number of obligations under the GDPR. This Part 3 provides information and links to various external resources which can help you understand how Copilot for Microsoft 365 operates and provides key information about the product and its features which can be used to assist with completion of a DPIA or other data protection assessment/analysis.

What is Copilot for Microsoft 365 and how does it work?

Copilot for Microsoft 365 is an AI-powered productivity tool that uses "Large Language Models (LLMs)" to work alongside popular Microsoft 365 apps such as Word, Excel, PowerPoint, Outlook, Teams, and more. Copilot for Microsoft 365 provides real-time, intelligent assistance which enables users to enhance their creativity, productivity, and skills.

Copilot for Microsoft 365 is built on top of the same cloud infrastructure as its Microsoft 365 applications, and applies the same principles of confidentiality and privacy to Customer Data that Microsoft has leveraged for years. Copilot for Microsoft 365 adheres to all existing privacy, security, and compliance commitments that apply to Microsoft 365 including Microsoft's GDPR commitments as set out in Microsoft's Data Protection Addendum and in relation to the EU Data Boundary.

Copilot for Microsoft 365 uses the organizational content in your Microsoft 365 tenant, including users' calendars, emails, chats, documents, meetings, contacts, and more only in accordance with existing

transforming. Think about promp
a conversation, using plain but cl
providing context like you would

When Copilot for Microsoft 365 u
organization's Microsoft 365 tena
user's prompt and enrich the resp
above, this is called "grounding",
to training. No Customer Data is
the LLM. In fact, the LLM is statele
it retains no information about th
submitted to it, nor any Customer
to ground it, nor any responses it

Copilot for Microsoft 365 leverag
a foundation LLM hosted in Azure
for Microsoft 365 does not intera
operated by OpenAI (e.g. ChatGP
API). OpenAI is not a sub-process
Customer Data - including the da
your organization's use of Copilot
such as prompts and responses –
third parties without your permiss

To get the best responses and the
for Microsoft 365, it's important t
prompts and avoid certain comm
more about the skill of prompting
of prompting (the ingredients of
prompting do's and don'ts.

Copilot for Microsoft 365 is

- **Built** on Microsoft's com
  approach to security, con
  privacy.

Copilot and your privacy

Copilot in Windows

Learn more about how Copilot uses your data to assist you on your Windows device.

Copilot Pro (home users)

Learn more about how Copilot uses your data in Microsoft 365 apps at home.

Copilot for Microsoft

Learn more about ho and protected when

How does Copilot for Microsoft 365 use personal data?

Copilot for Microsoft 365 provides value by connecting Microsoft's LLMs to your organizational data. Copilot for Microsoft 365 accesses content and context to generate responses anchored in your organizational data, such as user documents, emails, calendar, chats, meetings, and contacts. Copilot for Microsoft 365 combines this content with the user's working context, such as the meeting a user is currently attending, email exchanges the user had on a topic, or chat conversations the user had in a given period. Copilot for Microsoft 365 uses this combination of content and context to help provide accurate, relevant, and contextual responses to the user's prompts.
Copilot for Microsoft 365 can reference web content from the Bing search index to ground user prompts and responses. Based on the user's prompt, Copilot for Microsoft 365 determines whether it needs to use Bing to query web content to help provide a relevant response to the user. Controls are available to manage the use of web content for admins.

Abuse monitoring for Copilot for Microsoft 365 occurs in real-time, without providing Microsoft any standing access to Customer Data, either for human or for automated review. While abuse moderation, which

Microsoft will collect and store da interactions with Copilot for Micr include the user's prompt, how C and the information used to grou ("Content Interactions"). Custome manage, and search your organiz Interactions. It may be necessary privacy notices for your organizat it appropriately captures any proc data by admins in this context. Se details of the transparency obliga GDPR.

It is important for Microsoft that belongs to our customers. Micros ownership of the content created Microsoft 365. All Content Interac prompts and any output data/cor "Customer Data" in our Product T Data Protection Addendum.

All Customer Data processed by 365 is processed and stored in ali contractual commitments with yo other content in Microsoft 365.

Copilot for Microsoft 365 does nc to train foundation models witho permission.

Security for Copilot for Microsoft 365

As noted in Part 2, the GDPR requires data controllers and data processors to implement appropriate technical and organizational measures to ensure a level of security for any personal data which they process.

The same security and compliance terms apply, by default, to Copilot for Microsoft 365 as already apply for your organization's use of Microsoft 365. Copilot for Microsoft 365 is hosted in Azure infrastructure and protected by some of the most comprehensive enterprise compliance and security controls in the industry. Copilot for Microsoft 365 was built to take advantage of the security and compliance features that are already well-established in Microsoft's hyperscale cloud. This includes prioritization of reliability, redundancy, availability, and scalability, all of which are designed into our cloud services by default.

Copilot for Microsoft 365 also respects each user's access permissions to any content that it retrieves. This is important because Copilot for Microsoft 365 will only generate responses based on information the particular user has permission to access.

Microsoft already implements multiple forms of protection to help prevent customers from compromising Microsoft 365 services and applications or gaining unauthorized access to other tenants or the Microsoft 365 system itself.

Below are a few examples of those forms of protection:

- Logical isolation of Customer Data within each tenant for Microsoft 365 services is achieved through Microsoft Entra authorization and role-based access control. Learn more about Microsoft 365 isolation controls.
- Microsoft uses rigorous physical security, background screening, and a multi-layered encryption strategy to protect the confidentiality and integrity of Customer
- Your control over your o is reinforced by Microsof to comply with broadly a laws including the GDPR standards, such as ISO/IE world's first international for cloud privacy.
- For content accessed thr for Microsoft 365 plug-in can exclude programmat limiting the plug-in from content. Learn more abo usage rights for Azure In Protection.
- As generative AI systems software systems, all eler Security Development Li from threat modeling to secure build and operati strong cryptography, ide and more.
- We've also added new st Security Development Li prepare for AI threat vect updating the Threat Mod requirement to account f machine learning-specifi our AI products through to look for vulnerabilities we have proper mitigatio place.

Learn more about Data, Privacy, a Copilot for Microsoft 365

EU Data Boundary and D

As we explained in Part 2 of this p Microsoft 365 is an EU Data Boun

Learn more about the EU Data Bo

Part 4:

Azure OpenAI Service

Understanding how generative AI products and services operate and use personal data is the foundation for compliance with a number of obligations under the GDPR. This Part 4 provides information and links to various external resources which can help you understand how Azure OpenAI Service operates and provides key information about the service and its features which can be used to assist with completion of a DPIA or other data protection assessment/analysis.

What is Azure OpenAI Service and how does it work?

Azure OpenAI Service is a cloud-based platform that enables customers to build and deploy their own generative AI applications leveraging the power of AI models. Azure OpenAI Service provides customers with access to a set of LLMs for the development of generative AI experiences.

From generating realistic images and videos to enhancing customer experiences, generative AI has proven to be a versatile tool across various industries. The models underlying Azure OpenAI Service can be easily adapted to your specific task including: content design, creation and generation; summarization; semantic search; natural language to code translation; accelerated automation; personalised marketing; chatbots and virtual assistants; product and service innovation; language translation and natural language processing; fraud detection and cybersecurity; predictive analytics and forecasting; creative writing; and medical research and diagnosis.

Azure OpenAI Service is fully controlled by Microsoft. Microsoft hosts the OpenAI/Chat GPT models in

OpenAI/ChatGPT is not a sub-pro
and customer data - including the
through your organization's use o
Service– such as prompts and res
private and are not shared with th
your permission.

Learn more about the underlying
that power the Azure OpenAI Ser

Azure OpenAI Service can be used in the following ways:

- **Prompt engineering:** Prompt engineering is a technique that involves designing prompts for LLMs. Prompts are submitted by the user, and content is generated by the service, via the completions, chat completions, images, and embeddings operations. This process improves the accuracy and relevance of responses, optimizing the performance of the model.

  Learn more about prompt engineering

- **Azure OpenAI On Your Data:** When using the "on your data" feature, the service retrieves relevant data from a configured Customer Data store and augments the prompt to produce generations that are grounded with your data.

  Azure OpenAI "on your data" enables you to run supported LLMs on your organization's data without needing to train or fine-tune models. Running models on Customer Data enables you to analyze your data with greater accuracy and speed. By doing so, you can unlock valuable insights that can help you make better decisions, identify trends and patterns, and optimize your operations.

  One of the key benefits of Azure OpenAI "on your data" is its ability to tailor the content of conversational AI. The model within Azure OpenAI Service has access to and can reference specific sources to support responses, answers are not only based on its pre-trained knowledge but also on the latest information available in the designated data source. This grounding data also helps the model to avoid generating responses based on outdated or incorrect information.

  Learn more about Azure OpenAI On Your Data

- **Azure OpenAI fine-tuning:** You can provide your own training data consisting of prompt-completion pairs for the purposes of fine-tuning an OpenAI model. This

Training data and fine-tune

1. Are available exclusively f your organization.
2. Are stored within the sam as the Azure OpenAI reso
3. Can be deleted by the cu at any time

When you upload custom da results of the LLM, both the C the results of the fine-tuned m in a protected area of the clo tenant – accessible only by yo and separated by robust cont other access. The Customer D additionally be encrypted by managed or customer-manag in a Bring Your Own Key form chooses.

In most instances, Microsoft c troubleshoot any problems w without needing access to an (such as the data that was up tuning). In the rare cases whe Customer Data is required, w response to a customer-initia a problem identified by Micro control over access to that da Lockbox for Microsoft Azure. gives customers the ability to any access request to their C

Learn more about Azure Ope

Whether content is used to groun "on your own data" feature, or wh to build a fine-tuning model, the being used to train the foundatio LLM is stateless, meaning that it n about the prompt that was submi Customer Data that was used to g responses it provided. The LLM is not learn at any point during this the same foundational model eve

Preventing abuse and harmful content generation

To reduce the risk of harmful use of Azure OpenAI Service, both content filtering and abuse monitoring features are included.

Content filtering is the process by which responses are synchronously examined by automated means to determine if they should be filtered before being returned to a user. This examination happens without the need to store any data, and with no human review of the prompts (i.e. the text provided by users as requests) or the responses (i.e. the data delivered back to the user.)

Learn more about content filtering

Abuse monitoring is conducted by a separate process. This data may be accessed only by authorized Microsoft personnel to assist with debugging, and

This human review may create a c
sector customers, who need to st
between the safety of the system
external access – even under cont
accommodate that balance, Micr
access features that allow for app
use cases to opt out of these hum
logging processes.

Some customers may want to use
Service for a use case that involve
sensitive, highly confidential, or le
data but where the likelihood of h
or misuse is low. These customers
they do not want or do not have t
Microsoft to process such data fo
as described above, due to their i
applicable law. To address these c
allows customers who meet addit
Access eligibility criteria and attes
cases to apply to disable the Azur
management features by complet

How does the Azure OpenAI Service use personal data?

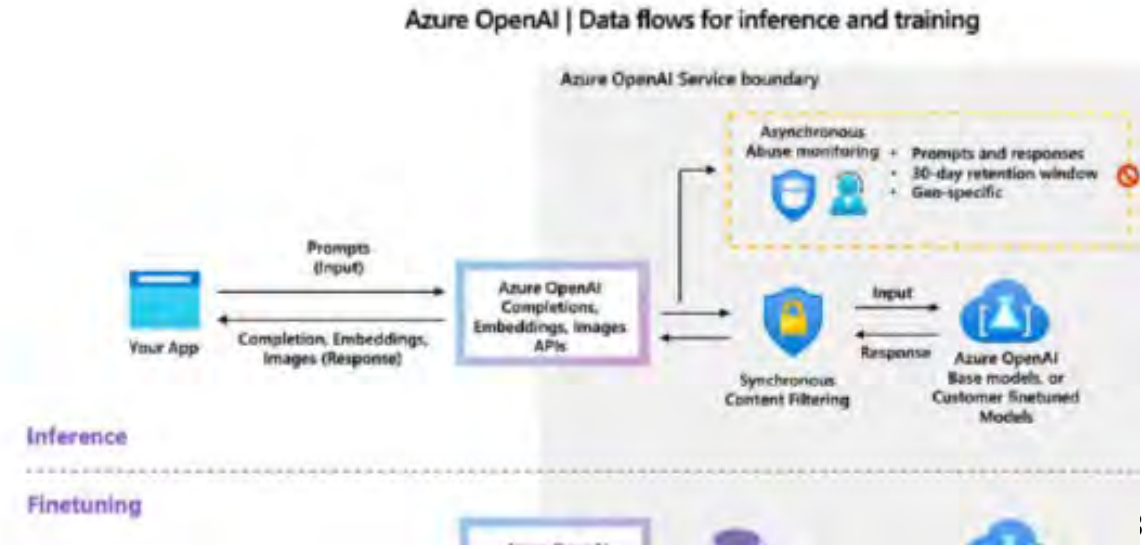
The diagram below illustrates how your organization's data is processed by Azure OpenAI Service. This diagram covers three different types of processing:

1. How Azure OpenAI Service processes your prompts to **generate content** (including when additional data from a connected data source is added to a prompt using Azure OpenAI "On Your Data").
2. How Azure OpenAI Service **creates a fine-tuned (custom) model** with your training data.
3. How Azure OpenAI Service and Microsoft personnel **analyze** prompts, completions, and images for harmful content and for patterns suggesting the use of the service in a manner that violates the Code of Conduct or other applicable product terms.

Customer prompts (inputs) and c
(outputs), embeddings, and traini

- are NOT available **to oth**
- are NOT available **to Ope**
- are NOT used **to train fo**
  models without the cust
  permission.
- are NOT used **to improv**
  or 3rd party products o
- are NOT used **for autom**
  improving Azure Open
  your use in your resource
  stateless unless you expli
  models with your training

Customer fine-tuned Azure Open
available exclusively for your orga



Security for Azure OpenAI

As noted in Part 2 of this paper, the GDPR requires data controllers and data processors to implement appropriate technical and organizational measures to ensure a level of security for any personal data which they process.

Security is built-in throughout the development lifecycle of all of our enterprise services (including those that include generative AI technology), from inception to deployment.

Azure OpenAI Service is hosted in Azure infrastructure and protected by some of the most comprehensive enterprise compliance and security controls in the industry. These services were built to take advantage of the security and compliance features that are already well-established in Microsoft's hyperscale cloud. This includes prioritization of reliability, redundancy, availability, and scalability, all of which are designed into our cloud services by default.

As generative AI systems are also software systems, all elements of our Security Development Lifecycle apply: from threat modelling to static analysis, secure build and operations, use of strong cryptography, identity standards, and more.

We've also added new steps to our Security Development Lifecycle to prepare for AI threat vectors, including updating the Threat Modelling SDL requirement to account for AI and machine learning-specific threats. We put our AI products through AI red teaming to look for vulnerabilities and confirm we have proper mitigation strategies in place.

Learn more about data, privacy and security for Azure OpenAI Service

EU Data Boundary and Residency

Azure OpenAI Service is an EU Da
For the purpose of interpreting th
Services" section of the Product T
service is an Azure service that en
a region within the EU Data Boun

Learn more about the EU Data Bo

In relation to:

- **Azure OpenAI on your l**
  Any data sources you pro
  the generated results ren
  in the data source and lo
  designate. No data is cop
  OpenAI service.

- **Training data and fine-t**
  LLMs: These are stored w
  region as Azure OpenAI r
  customer's Azure tenant.

- **Abuse monitoring for c**
  use Azure OpenAI Servi
  This review is conducted
  Microsoft employees in t
  Economic Area. The data
  prompts and completion
  logically separated by cus
  (each request includes th
  the customer's Azure Ope
  A separate data store is l
  region in which Azure Op
  is available, and a custom
  and generated content a
  Azure region where the c
  OpenAI service resource
  within the Azure OpenAI
  boundary.

Part 5:

Conclusion

Microsoft runs on trust. We are committed to security, privacy, and compliance across everything we do, and our approach to generative AI is no different. As an industry leader in the provision of generative AI solutions we are trusted by public sector customers across the world and adhere to the strictest privacy and security standards in the industry. We provide superior products and services to our public sector customers, thereby facilitating continued progress towards national digital transformation goals.

Furthermore, we have been intentional about signalling to our public sector customers our willingness and commitment to get our data protection and privacy settings right to ensure compliance with the GDPR. We demonstrate this commitment through our contracts, extensive technical documentation (providing details about our data processes and activities), and the implementation of technical and organizational safeguards to mitigate residual privacy and security risks. This is backed by consistent engagement with regulatory and industry stakeholders whom we partner with on our journey towards responsibility, accountability, and integrity in the delivery of generative AI solutions at scale.

As the regulatory landscape evolves and we innovate to provide new kinds of AI solutions, we are keenly aware that public sector organizations will continue to look to us to help decipher and operationalize the requirements of new and existing data protection frameworks. Microsoft will continue to offer industry-leading tools, transparency resources and support and we look forward to the opportunity to continue to demonstrate our enduring commitment to meeting the needs and demands of our European public sector customers in their AI journey.

Appendix 1:

Opportunities arising from generative AI in the Public Sector

The availability of generative AI solutions has served as an accelerator to the consideration of public sector generative AI use cases. This Appendix sets out several relevant areas of impact for consideration by public sector organizations.

- **Citizen Services:** Generative AI can help governments and public sector organizations provide enhanced service experiences that make government more accessible and less time-consuming by acting as an "Information Assistant" – answering frequently asked questions, recommending services based on inputs, and even handling simple transactions.

  Many governments have already experimented with chatbots to help answer simple questions about COVID vaccinations, provide support during tax time, and offer answers to common inquiries. Generative AI helps chatbots handle more open domain questions over more sophisticated and complex materials, including rapid responses to a broader range of questions at anytime from anywhere, increasing accessibility for citizens while simultaneously increasing government efficiency and reducing administrative burden.

  Citizens can even provide a narrative of their current circumstances and discover service options they previously did not know existed. These tools also free up public sector workers to focus on strategic projects instead of being tied down to mundane, repetitive functions such as responding to common questions.

- **Internal Efficiency:** Government can be complex even for government employees! Providing public sector workers with the capacity to

connections between topics
can help to spur the analytic

Insightful and succinct summ
amounts of media coverage
can be generated in seconds
helps to objectively challeng
wisdom – raising new angles,
counterarguments that may
screened by the bias of the a
approach ultimately yields st
comprehensive output.

- **Creative Aid:** No more write
AI can provide helpful initial
outlines, speeches, simple co
memos, frequently asked qu
and citizen guides. While offi
should always require a hum
to verify accuracy, apply hum
ensure that the information i
misleading, generative AI as
can accelerate the process dr
light the creative spark while
completion for common writ

- **Enhance Security:** Generativ
cybersecurity teams and prot
organization from threats. Ge
can be trained to review appl
for weaknesses using a dyna
evolves to keep pace with th
be used to review and deplo
quickly by automating vulne
which will help security profe
workloads by freeing them u
tasks.

Appendix 2:

Frequently Asked Questions (FAQs)

How is my organization's data protected when I use Microsoft's Generative AI Services?

Microsoft runs on trust. We are committed to security, privacy, and compliance across everything we do, and our approach to generative AI is no different.

Privacy is built into our approach to Responsible AI and we will continue to uphold our core values of privacy, security, fairness, accountability, transparency, reliability, inclusiveness and safety in our AI products and solutions.

In Part 2 of this paper, we outline seven commitments that demonstrate our continued commitment to protecting our customers' data when they use our Generative AI services:

- We will keep your organization's data private.
- You are in control of your organization's data.
- Your access control and enterprise policies are maintained.
- Your organization's data is not shared without your permission.
- Your organization's data privacy and security are protected by design.
- Your organization's data is not used to train foundation models without your

What is generative AI a the different types of A Microsoft uses?

Generative AI is a type of artificial create new things, like pictures, te are similar to examples it has seer by learning from a set of example patterns and rules that make them using those patterns and rules to that are similar to the ones it lean different from other types of AI b new things, instead of just recogn things it has seen before.

Microsoft's Azure OpenAI service Microsoft 365 allow customers to models, including GPT-3, GPT-4, a Microsoft environment. These mo referred to as "foundation models understood to be large-scale AI m trained on vast quantities of prim at scale (usually by self-supervise be adapted with minimal fine-tun different downstream tasks.

What are the differences between procuring cloud and generative AI services from a GDPR perspective?

The obligations under the GDPR which apply to procuring and using cloud computing services are the same as those which apply to procuring and using generative AI services. The GDPR requires a risk-based approach to be taken towards the implementation and use of any new technologies.

The level of risk involved will depend on the nature, scope, content, and purpose for which personal data will be used. When procuring cloud services and/or generative AI services, a public sector organization will need to consider what technical and organizational measures are in place to protect and safeguard the use of personal data and ensure that it has appropriate contractual commitments and operational processes to ensure it can comply with its obligations under the GDPR.

Find out more about how Microsoft can assist public sector customers in undertaking this assessment when they are looking to use Copilot for Microsoft 365 and/or Azure OpenAI Service in Part 2 of this paper.

What are the key obliga the GDPR that apply to generative AI systems?

The obligations under the GDPR v a generative AI system uses or otl personal data.

Key obligations which public sect should consider when procuring a generative AI systems include:

- consider whether you ne your privacy notices to re processing activity or to ((Articles 12 to 14 of the G
- ensure you have processe enable you to comply wit rights requests (Articles 1 GDPR);
- ensure that any agreeme a data processor complie 28 of the GDPR including to security measures and transfers;
- consider whether you ne a data protection impact (DPIA) (Article 35 of the G
- ensure that all transfers o of the UK, EU or EEA are a valid transfer mechanis to 50).

Learn more about how Microsoft customers in meeting these oblig this paper.

How does the GDPR interact with the AI Act?

The AI Act is a new law currently being put in place in the EU to regulate AI systems. It will apply to providers, importers, distributers, users, and others involved in the AI lifecycle, aiming to ensure that AI systems that are used in the EU respect fundamental rights, safety, and ethical principles, as well as address certain risks related to the most highly capable general-purpose AI models.

The GDPR and the AI Act are intended to be complementary and operate alongside each other providing a regulatory framework for AI products and services.

The GDPR, which regulates the processing of personal data by data controllers and data processors, focuses on data privacy and aims to give individuals control over their personal data. Under the AI Act most of the regulatory burden will fall on providers of high-risk AI systems and general-purpose AI (GPAI) models.

Although the GDPR and the AI Act are different in their scope and purpose, they interact with each other in several ways. For example:

- The GDPR requires data controllers to conduct a DPIA in certain circumstances. The AI Act refers to this obligation and requires users of high-risk AI systems to use certain mandatory user-facing information to comply with their DPIA-obligations under the GDPR.
- The GDPR applies where personal data is processed to train an AI system or where an AI system is being used to process personal data.

Adopting the measures outlined in this paper for GDPR compliance is therefore complementary to the AI Act and the associated obligations that will apply under this new legislation.

How does Microsoft co applicable law?

Microsoft's AI products and soluti built for compliance with applicat and privacy laws today, including

Microsoft's approach to protectin underpinned by a commitment tc existing and emerging regulatory globally. We will continue to supp privacy and AI regulation, and bel way to make rapid progress on ne AI is to lean in to existing legal pr and regulatory tools that could b protecting privacy and safety in th

Does Microsoft share C with OpenAI/ChatGPT?

No. Your organization's Customer prompts (inputs) and completion embeddings, and any training dat to the Microsoft Online Services a OpenAI.

Azure OpenAI Service is fully cont Microsoft hosts the OpenAI mode Azure environment and Azure Op not interact with any services ope (e.g., ChatGPT, or the OpenAI API) sub-processor to Microsoft.

Learn more about the underlying that power Azure OpenAI Service.

Can I share confidential with Microsoft's Genera services?

Yes. When using Azure OpenAI or Microsoft 365, customers may co confidential information. The four are accessed via Azure OpenAI Se Microsoft 365 do not use Custom

How does Microsoft protect security in this new era of AI?

Security is built-in throughout the development lifecycle of all of our enterprise services (including those that include generative AI technology), from inception to deployment.

Azure OpenAI Service and Copilot for Microsoft 365 are hosted in Azure infrastructure and protected by some of the most comprehensive enterprise compliance and security controls in the industry. These services were built to take advantage of the security and compliance features that are already well-established in Microsoft's hyperscale cloud. This includes prioritization of reliability, redundancy, availability, and scalability, all of which are designed into our cloud services by default.

Because generative AI systems are also software systems, all elements of our Security Development Lifecycle apply: from threat modeling to static analysis, secure build and operations, use of strong cryptography, identity standards, and more. We've also added new steps to our Security Development Lifecycle to prepare for AI threat vectors, including updating the Threat Modeling SDL requirement to account for AI and machine learning-specific threats. We put our AI products through AI red teaming to look for vulnerabilities and ensure we have proper mitigation strategies in place.

Learn more about Security for Copilot for Microsoft 365 in Part 3 of this paper, and about Security for Azure OpenAI Service in Part 4 of this paper.

Are data transfers to countries outside of the UK, EU or EEA allowed under the GDPR?

Yes, personal data can be transferred to countries outside the UK, EU or EEA where certain conditions are met including where: (a) there is an adequacy decision by the European Commission or the UK Secretary of State (Article 45 of the GDPR); or (b) the transfer is subject to additional safeguards which include the EU

Where will my data be s processed?

Your data residency choices will b you use Microsoft's Generative AI services that offer local storage ar capabilities.

Azure OpenAI Service and Copilo will process and store your data w Data Boundary (EUDB) customers Product Terms and the EU Data Bo Documentation.

Do public sector organi need to develop a custo protection addendum (

No, the GDPR does not require th controller has a customized data p with their data processors. Micros Addendum is compliant with the Article 28 of the GDPR.

It is not viable for hyperscale clou different terms for different custo uniformity of the services which n more manageable, scalable, secur on-site solutions. In addition, intro security measures or standards fo could undermine the security of M as a whole. It is therefore not feas change its operational processes contractual commitments and/or for every customer.

Find out more about Microsoft's c obligations in Part 2 of this paper.

How can public sector customers set up their procurement of generative AI services to be compliant with the GDPR?

The GDPR requires data controllers to consider data protection issues at every stage of their processing activities, from the initial design (including during the procurement phase) to final implementation.

The risks associated with the use of generative AI in the public sector will vary depending on the specific use case and related nature, sensitivity, and volume of personal data that will be used in connection with that use case.

One way you can demonstrate compliance with the GDPR is to complete a data protection impact assessment (DPIA) relating to specific use cases for generative AI solutions. A DPIA helps organizations identify and reduce the data protection risks. A DPIA is legally required where the processing activity is likely to result in a high risk to the rights and freedoms of data subjects. Even if it is not legally required, a DPIA is good practice and can help you work through the specific data protection risks associated with how you wish to implement generative AI for a specific use case.

Find out more about DPIAs in Part 2 of this paper.

Can a public sector customer comply with the GDPR when using a public cloud to use generative AI services?

Microsoft's public cloud services have been developed to ensure they can be used by public sector customers in compliance with the GDPR (and many public sector customers already make use of th
information set out in this paper
the Product Terms and Data Prote
can be used by you to undertake
risk-based assessment of any pro
Copilot for Microsoft 365 and Azu
so as to demonstrate compliance
requirements of the GDPR.

How can public sector
comply with their trans
obligations under the G
deploying AI technolog

Articles 12 to 14 of the GDPR req
organizations to provide data sub
key information about how their
used. This information is often pr
privacy notices. If you deploy a ne
as Copilot for Microsoft 365 or Az
and intend to use such technolog
reflected in your exiting privacy n
need to update their privacy notic
new processing activities.

The information set out in this pa
assist you to understand how Cop
and Azure OpenAI Service use da
what information needs to be cor
subjects.

Appendix 3:

Additional Resources

Microsoft is committed to providing our customers with clear information about how we use
choices they have in managing their data. This Appendix sets out additional resources which
supplement and expand on the information set out in this paper.

Responsible AI

- Empowering responsible AI practices
- Governing AI: A Blueprint for the Future
- Microsoft's principles and approach to Responsible AI
- Microsoft Responsible AI Standard

Microsoft's Customer Commitments

- AI Assurance Program and AI Customer Commitments
- Customer Copyright Commitment
- Protecting the data of our commercial and public sector customers in the AI era
- FAQ: Protecting the Data of our Commercial and Public Sector Customers in the AI Era

Understanding Generative AI

- The underlying LLMs that power Microsoft's generative AI solutions
- The art and science of prompting (the ingredients of a prompt)
- Prompting do's and don'ts

Data Protection Addendum and Product Terms

- Data Protection Addendum
- Microsoft Product Terms

Data Protection Impact Ass

- DPIAs and their contents
- Data Protection Impact A
  the GDPR

Copilot for Microsoft 365

- Copilot for Microsoft 365
- Copilot Lab
- Copilot for Microsoft 365
- Data, Privacy, and Securit
  Microsoft 365
- FAQs for Copilot data sec
- Microsoft 365 isolation c
- Encryption in the Microso

Azure OpenAI Service

- Azure OpenAI Service - D
  quickstarts and API refere
- Configure usage rights fo
  Information Protection
- Data, privacy and security
  OpenAI Service
- Prompt Engineering
- Azure OpenAI On Your D
- Azure OpenAI fine tuning
- Content filtering
- Abuse monitoring
- Enterprise security for Az
  Learning


Microsoft

Appendix 8 – Microsoft Online Services Subprocessors

[Captured 16/07/2024]

Microsoft

Microsoft Online Services Subprocesso

DATE OF ISSUE: July 2, 2024

When you use Microsoft Online Services, Microsoft subprocessors, as defined in the Products and Services Data Protec may process Customer Data and Personal Data (consisting of pseudonymized personal identifiers). In accordance with regulations, we disclose these subprocessors to you in advance of their first engagement with Microsoft and then on a permit these subprocessors to process your data only to perform the work Microsoft has retained them to perform, an from using your data for any other purpose.

Microsoft has designated three categories of subprocessors: (1) third-party subprocessors that power integrated cloud third-party subprocessors that provide ancillary services; and (3) third-party organizations that provide contract staff t Additionally, we are providing information about Microsoft datacenter entities that provide the infrastructure on which Services run.

Software as a service (SaaS) administrators (Microsoft 365, Dynamics 365) for tenants located in the European Econom United Kingdom will receive automatic notifications of updates to this list via the Service Message Center. Infrastructu and platform as a service (PaaS) customers (Azure) and any other users of SaaS services may sign up to receive notifica this disclosure via My Library on the Service Trust Portal.

Entity Name	Applicable Online Service or Product	Sub-processing Activity	Processing Location(s)	DnB Registered Address	Headquarters	DnB Registere Numbe
Accenture International Limited	SAP HANA on Azure (Large Instances)	Hardware and software installation and operations	In accordance with the customer-specified regionality of SAP HANA on Azure (Large Instances)	1 Grand Canal Square Dublin 2, Ireland	Ireland	9850153
Akamai Technologies, Inc.	Any Microsoft Online Service	Operating Content Delivery Network (CDN) infrastructure to efficiently deliver content	Worldwide	150 Broadway, Cambridge MA, 02142-1413 USA	United States	4777520
Databricks, Inc.	Azure Databricks	Deploying, operating, and troubleshooting Azure Databricks	Canada, France, Germany, Netherlands, United Kingdom, United States	160 Spear Street, FL 13, San Francisco, CA, 94105-1546 USA	United States	7935630
Edgio, Inc.	Any Microsoft Online Service	Operating Content Delivery Network (CDN) infrastructure to efficiently deliver content	Worldwide	11811 N. Tatum Blvd. Ste 3031 Phoenix, AZ 85028, USA	United States	1188905(

Entity Name	Applicable Online Service or Product	Sub-processing Activity	Processing Location(s)	DnB Registered Address	Headquarters	DnB Registere Numbe
NetApp, Inc.	Azure NetApp files	Deploying, operating, and troubleshooting Azure NetApp files	In accordance with the customer-specified regionality of Azure NetApp files	495 East Java Drive Sunnyvale, CA 94089-1125 USA	United States	8020547
Red Hat, Inc.	Azure Red Hat OpenShift	Deploying, operating, and troubleshooting Azure Red Hat OpenShift	Australia, Belgium, Brazil, Canada, China, Czech Republic, France, Germany, India, Ireland, Israel, Poland, Spain, United States	100 East Davie Street Raleigh, NC 27601-1806 USA	United States	136808
TomTom North America, Inc.	Azure Maps	Web services used by the Azure Maps APIs	United States, Germany, Ireland, Netherlands, Poland	11 Lafayette Street Lebanon, NH, 03766 USA	Netherlands	4137828

2) Third-party subprocessors that provide ancillary services

The following subprocessors provide ancillary services to help support, operate, and maintain the Microsoft Online Ser

Entity Name	Applicable Online Service or Product	Sub-processing Activity	Processing Location(s)	DnB Registered Address	Headquarters	Dr Regis Num
Amazon Web Services	Microsoft Purview	Acquisitions that run on AWS are eventually moved to be hosted on Microsoft Azure Multi-Cloud Scanning Connectors for Microsoft Purview	Microsoft Purview (processing location varies; will depend on location of customers' AWS storage account)	410 Terry Avenue Seattle, WA 98109-5210 USA	United States	88474
Arkose Labs, Inc.	Azure Active Directory, Azure Web Application Firewall	CAPTCHA based Fraud + Abuse Prevention activity	Australia, Ireland, Singapore, United States	250 Montgomery Street Floor 10 San Francisco, CA 94104-3431 USA	United States	8134
Intercom, R&D Unlimited Company *	Visual Studio App Center	Customer chat and support	United States	18-21 St Stephen's Green 2nd Floor Dublin, Ireland	Ireland	98558
Scuba Analytics, Inc. *	Teams, Stream, SharePoint Online, OneDrive for	Customer experience (CX) analytics	United States	800 West El Camino Real Suite 180 Mountain View, CA 94040-2586	United States	1837

3) Third-party organizations that provide contract staff

The following organizations provide contract staff who work in close coordination with Microsoft employees to operat the Microsoft Online Services. While doing so, the staff of these organizations may process Customer Data or Personal pseudonymized personal identifiers) on our behalf. In all such cases the data resides only on Microsoft systems and is policies and supervision. Organizations that only process pseudonymous personal data have been identified with an a below. Organizations that only process Dynamics 365 Customer Data and Personal Data have been identified with a ha below.

For more information regarding Microsoft's contract staff personnel locations, visit Locations of Microsoft Online Servi Remote Access to Data.

Staffing Provider	DnB Registered Address	Headquarters	DnB Registered Number	
Accenture International Limited	1 Grand Canal Square Dublin 2, Ireland	Ireland	985015354	A
Akvelon, Inc.	3120 139th Avenue SE Ste 100 Bellevue, WA 98005-4491 USA	United States	829720676	
Allegis Group Holdings, Inc.	7437 Race Road Hanover, MD 21076-1112 USA	United States	121768035	
	10210 NE Points Drive Kirkland WA			

Staffing Provider	DnB Registered Address	Headquarters	DnB Registered Number	
Aptly Technology Corporation	12951 Bel-Red Road Ste 160 Bellevue, WA 98005	United States	086158760	
Atos It Solutions and Services, Inc.	4851 Regent Blvd Irving, TX 75063-0214 USA	United States	101188514	
Beyondsoft Consulting, Inc *	3025 112th Avenue NE, Suite 200, Bellevue, WA 98004-8002 USA	United States	32506448	E
Blueprint Technologies	505 106th Avenue NE 3rd Floor Bellevue WA 98004-9600 USA	United States	70678945	E
Concentrix Corporation #	44111 Nobel Drive Fremont, CA 94538 USA	United States	07-930-9922	(
Csi Interfusion, Inc.	11808 Northup Way Bellevue WA 98005-1944 USA	United States	2587864	(
Dxc Technology Services LLC *	20408 Bashan Drive Suite 231 Ashburn, VA 20147-5551 USA	United States	80521853	D:

Staffing Provider	DnB Registered Address	Headquarters	DnB Registered Number	
Aptly Technology Corporation	12951 Bel-Red Road Ste 160 Bellevue, WA 98005	United States	086158760	
Atos It Solutions and Services, Inc.	4851 Regent Blvd Irving, TX 75063-0214 USA	United States	101188514	
Beyondsoft Consulting, Inc *	3025 112th Avenue NE, Suite 200, Bellevue, WA 98004-8002 USA	United States	32506448	E
Blueprint Technologies	505 106th Avenue NE 3rd Floor Bellevue WA 98004-9600 USA	United States	70678945	E
Concentrix Corporation #	44111 Nobel Drive Fremont, CA 94538 USA	United States	07-930-9922	(
Csi Interfusion, Inc.	11808 Northup Way Bellevue WA 98005-1944 USA	United States	2587864	(
Dxc Technology Services LLC *	20408 Bashan Drive Suite 231 Ashburn, VA 20147-5551 USA	United States	80521853	D:

Staffing Provider	DnB Registered Address	Headquarters	DnB Registered Number	
E-Search	Bulevar Mihaila Pupina 10Z/IV Beograd, Serbia 11070	Serbia	600793038	
Experis	29973 Network Place Chicago, IL 60673-1299 USA	United States	19639852	
Harman Connected Services, Inc.	636 Ellis Street Mountain View, CA 94043-0650 USA	United States	47653555	
Hcl America, Inc.	330 Potrero Avenue Sunnyvale, CA 94085-4113 USA	United States	197298524	H
Hi-Tech Talents LLC *	1530 140th Avenue NE Bellevue WA 98005-4574 USA	United States	67938874	
Infosys Limited	5010 148th Ave NE Ste 100 Redmond, WA, 98052-5127 USA	United States	109508454	

Staffing Provider	DnB Registered Address	Headquarters	DnB Registered Number	
Latentview Analytics Corporation *	2540 North First Street Suite 108 San Jose, CA 95131-1016 USA	United States	964739804	
Launch Consulting	275 118th Avenue SE Bellevue WA 98005-3538 USA	United States	17980124	
Maq LLC *	2027 152nd Avenue NE Redmond WA 98052-5501 USA	United States	6650365	
Matchpoint It Ltd.	6 Hahoshlim St., P.O.B. 12195 Herzliya Pituach, Israel 46733	Israel	533527867	
LTIMindtree Limited (Formerly known as Mindtree Limited)	Global Village, RVCE Post, Mysore Road Bangalore, KA 560059 IN	India	650046436	
Mu Sigma Business Solutions, LLC *	3400 Dundee Road Suite 160 Northbrook, IL 60062-3400 USA	United States	796812233	
Centific Technologies, Inc.	14980 NE 31ST Way Ste 120 Redmond, WA, 98052-5349 USA	United States	84526354	Pa

Staffing Provider	DnB Registered Address	Headquarters	DnB Registered Number	
Shanghai Wicresoft Co, Ltd.	No.1000, Zixing Road, Wujing Town, Minhang District Shanghai, Shanghai, 200241 China	China	544851165	
Sonata Software Limited	1/4, APS Trust Building, Bull Temple Bangalore, India 56004	India	808157663	S
Tata Consultancy Services Ltd.	14335 NE 24th Street, Bellevue WA 98007-3737 USA	United States	54328054	Ta
Tek Experts #	2nd Floor Nicosia City Center 64 Kallipoleos Nicosia 1071 Cyprus	Cyprus	565541241	
Teleion Consulting, LLC *	1000 Dexter Avenue N. Suite 520 Seattle WA 98109-3581 USA	United States	19550357	
Telus International Ai, Inc.	2251 S. Decatur Boulevard, Las Vegas NV 89102 USA	United States	824891477	L

Staffing Provider	DnB Registered Address	Headquarters	DnB Registered Number	
Wipro Limited	Sy. No. 76P-80P Bengaluru, KA 560035 India	India	650174378	
Zen3 Infosolutions America, Inc.	2035 158th Court NE Bellevue, WA 98008-2128 USA	United States	79528045	

Microsoft datacenter infrastructure entities

The following Microsoft entities provide the datacenter infrastructure on which the Microsoft Online Services run. The datacenters is encrypted, and no personnel within the datacenters are permitted to access it. This is a list of all Microso infrastructure entities; those relevant to your scenario may vary depending on the regions in which you deploy or use (when regional selection is available).

For more information on Microsoft datacenters, please see the Azure global infrastructure site: Global Infrastructure | M

For more information regarding Microsoft's personnel locations, visit Locations of Microsoft Online Services Personnel Data.

Microsoft datacenter infrastructure entity	Country
Microsoft Datacenter (Australia) Pty Limited	Australia

Microsoft datacenter infrastructure entity	Country
Microsoft 3465 Finland Oy	Finland
Microsoft 1985 France S.à r.l.	France
Microsoft Deutschland MCIO GmbH	Germany
Microsoft Datacenter Holdings (HK) Limited	Hong Kong
Microsoft Corporation (India) Private Limited	India
Microsoft Ireland Operations Limited	Ireland
Microsoft 4772 Israel Ltd.	Israel
Microsoft 4825 Italy S.R.L.	Italy
Microsoft Japan Co., Ltd.	Japan
Microsoft 5673 Korea Yuhan Chaegim Hoesa	Korea, Republic of
Microsoft Payments (Malaysia) Sdn. Bhd.	Malaysia
Microsoft 6394 Mexico S. de R.L. de C.V.	Mexico
Microsoft Datacenter Netherlands B.V.	Netherlands
Microsoft 6399 New Zealand Limited	New Zealand
Microsoft Datacenter Norway AS	Norway
Microsoft Poland Operations Sp.z o.o.	Poland
Microsoft 7282 Qatar QFZ LLC	Qatar
Microsoft Operations Pte Ltd	Singapore
Microsoft 1968 South Africa (Pty.) Ltd.	South Africa
Microsoft 7724 Spain, S.L.	Spain
Microsoft Sweden 1172 AB	Sweden
Microsoft MCIO Schweiz GmbH	Switzerland
Microsoft Operations Taiwan Limited	Taiwan
Microsoft Operations 38224 FZE	United Arab Emirates
Microsoft Corporation - Abu Dhabi	
MSFT MCIO Limited	United Kingdom

Summary of changes since the last disclosure

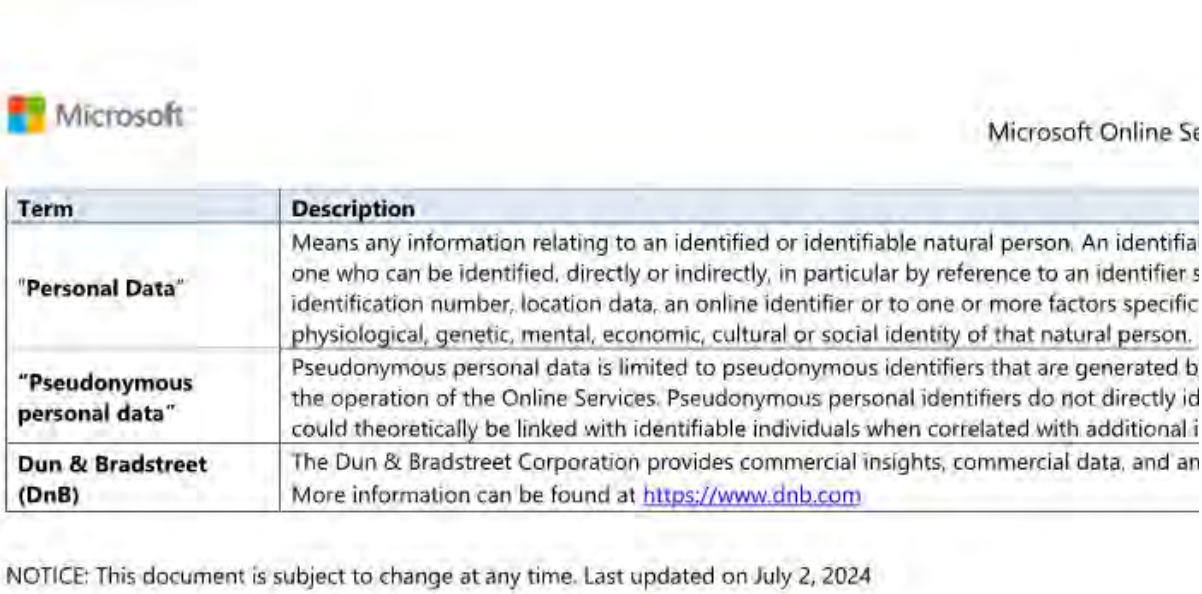
This is a list of substantive changes since our last disclosure.

Entity name	Change Description
Edgio, Inc.	Edgio, Inc. acquired Edgecast which previously provided CDN service
Amazon Web Services	Removed Visual Studio App Center Test from scope
Arkose Labs, Inc.	Expanded scope to include Azure Web Application Firewall
Intercom, Inc.	Updated entity name to Intercom R&D Unlimited Company
Launch Consulting	Updated Parent Company to The Planet Group
Microsoft 6399 New Zealand Limited	Added to list of Datacenters
Microsoft Operations Puerto Rico, LLC	Removed from list of Datacenters

Helpful Definitions and Related Information

For the most up-to-date definitions, refer to the Microsoft Products and Services Data Protection Addendum (DPA) located on the

Term	Description
"**Subprocessor**"	Means other processors used by Microsoft to process Customer Data, Professional Service Data, as described in Article 28 of the GDPR.
"**Customer Data**"	Means all data, including all text, sound, video, or image files, and software, that are provi or on behalf of, Customer through use of the Online Service. Customer Data does not incl Services Data.
	Means all data, including all text, sound, video, image files or software, that are provided t behalf of a Customer (or that Customer authorizes Microsoft to obtain from a Product) or



Microsoft

Microsoft Online Se

Term	Description
"Personal Data"	Means any information relating to an identified or identifiable natural person. An identifia one who can be identified, directly or indirectly, in particular by reference to an identifier s identification number, location data, an online identifier or to one or more factors specific physiological, genetic, mental, economic, cultural or social identity of that natural person.
"Pseudonymous personal data"	Pseudonymous personal data is limited to pseudonymous identifiers that are generated b the operation of the Online Services. Pseudonymous personal identifiers do not directly id could theoretically be linked with identifiable individuals when correlated with additional i
Dun & Bradstreet (DnB)	The Dun & Bradstreet Corporation provides commercial insights, commercial data, and an More information can be found at https://www.dnb.com

NOTICE: This document is subject to change at any time. Last updated on July 2, 2024

Appendix 9 – Search for and delete Microsoft CoPilot for Microsoft 365 Data

Search for and delete Microsoft Copilot for Microsoft 365 data | Microsoft Learn

[Captured 26/7/2024]

Search for and delete Microsoft Copilot for Microsoft 365 data

- Article
- 04/01/2024
- 2 contributors

Feedback

In this article

Show 4 more

You can use eDiscovery (Premium) and the Microsoft Graph Explorer to search for and delete user prompts and Microsoft Copilot for Microsoft 365 responses in supported applications and services. This feature can help you find and remove sensitive information or inappropriate content included in Copilot activities. This search and deletion workflow can also help you respond to a data spillage incident, when content containing confidential or malicious information is released through Copilot-related activity.

Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview compliance portal trials hub. Learn details about signing up and trial terms.

Before you search and delete Copilot data

- To create an eDiscovery (Premium) case and use collections to search for Copilot activity data, you have to be a member of the *eDiscovery Manager* role group in the Microsoft Purview compliance portal. To delete Copilot data, you have to be assigned the *Search And Purge* role. This role is assigned to the *Data Investigator* and *Organization Management* role groups by default. For more information, see Assign eDiscovery permissions.
- A maximum of 10 items per mailbox can be removed at one time. Because the capability to search for and remove Copilot data is intended to be an incident-response tool, this limit helps ensure that this data is quickly removed.

Step 1: Create a case in eDiscovery (Premium)

The first step is to create a case in eDiscovery (Premium) to manage the search and deletion process. For information about creating a case, see Use the new case format.

Step 2: Create a collection estimate

After you create a case, the next step is to create a collection estimate to search for the Copilot data that you want to delete. The deletion process you perform is Step 5 deletes all Copilot-related items that are found in the collection estimate (within the 10 item per location limit).

In eDiscovery (Premium), a *collection* is an eDiscovery search of the content locations that contain Copilot data that you want to delete. Create the collection estimate in the case that you created in the previous step. For more information, see Create a collection estimate.

Data sources for Copilot data

The following table lists the applications and services that are sources for Copilot data. All user prompts to Copilot and responses from Copilot are stored in a user's mailbox.

Expand table

For this type of Microsoft Copilot data...	Search this item class...
Excel	IPM.SkypeTeams.Message.Copilot.Excel
Loop	IPM.SkypeTeams.Message.Copilot.Loop
Microsoft 365 App	IPM.SkypeTeams.Message.Copilot.M365App
Microsoft Copilot for Bing (Bizchat)	IPM.SkypeTeams.Message.Copilot.BizChat
Microsoft Forms	IPM.SkypeTeams.Message.Copilot.Forms
OneNote	IPM.SkypeTeams.Message.Copilot.OneNote
Outlook	IPM.SkypeTeams.Message.Copilot.Outlook
PowerPoint	IPM.SkypeTeams.Message.Copilot.Powerpoint
Teams Channel	IPM.SkypeTeams.Message.Copilot.Teams
Teams Chat	IPM.SkypeTeams.Message.Copilot.Teams
Teams Copilot Chat (Bizchat)	IPM.SkypeTeams.Message.Copilot.BizChat
Teams Meeting	IPM.SkypeTeams.Message.Copilot.Teams
Teams Microsoft 365 Chat (BF)	IPM.SkypeTeams.Message
Whiteboard	IPM.SkypeTeams.Message.Copilot.Whiteboard
Word	IPM.SkypeTeams.Message.Copilot.Word

Note

In Step 4, you also have to identify and remove any holds and retention policies assigned to the mailbox that contains the type of Copilot data that you want to delete.

Tips for searching for Copilot data

To help ensure the most comprehensive collection of Copilot data, use the Type condition and select the Copilot activity option when you build the search query for the collection estimate. We also recommend including a date range or several keywords to narrow the scope of the collection to items relevant to your search and delete investigation.

For more information, see Build search queries for collections.

Step 3: Review and verify Copilot data to delete

The deletion process in Step 5 will delete the items returned by the collection. It's important that you review the collection estimate results to ensure that the collection only returns the items that you want to delete. To review a sample of items in a collection estimate, see the Next steps after a collection estimate is complete section in Create a collection estimate.

Additionally, you can use the collection statistics (specifically the *Top Locations* statistics) to generate a list of the data sources that contain items returned by the collection. Use this list in the next step to remove hold and retention policies from the user mailboxes that contain search results. For more information, see Collection statistics and reports.

Step 4: Remove holds and retention policies from data sources

Before you can delete Copilot data from a mailbox, you have to remove any hold or retention policy that is assigned to a target mailbox. If not, then the data you're trying to delete is retained.

Use the list of mailboxes that contain the Copilot data that you want to delete and determine if there's a hold or retention policy assigned to those mailboxes, and then remove the hold or retention policy. Be sure to identify the hold or retention policy that you remove so that you can reassign to the mailboxes in Step 7.

For instructions about how to identify and remove holds and retention policies, see Step 3: Remove all holds from the mailbox in Delete items in the Recoverable Items folder of cloud-based mailboxes on hold.

Step 5: Delete Copilot data

Note

Because Microsoft Graph Explorer is not available in some US Government clouds (GCC High and DOD), you must use PowerShell to accomplish these tasks. See the Delete Copilot data with PowerShell for details.

Now you're ready to delete Copilot data from user mailboexes. Use the Microsoft Graph Explorer to perform the following three tasks:

1. Get the ID of the eDiscovery (Premium) case that you created in Step 1. This is the case that contains the collection created in Step 2.
2. Get the ID of the collection that you created in Step 2 and verified the search results in Step 3. The search query in this collection returns the Copilot data to be deleted.
3. Delete the Copilot data returned by the collection.

For information about using Graph Explorer, see Use Graph Explorer to try Microsoft Graph APIs.

Important

To perform these three tasks in Graph Explorer, you may have to consent to the eDiscovery.Read.All and eDiscovery.ReadWrite.All permissions. For more information, see the "Consent to permissions" section in Working with Graph Explorer.

Get the case ID

1. Go to https://developer.microsoft.com/graph/graph-explorer and sign in to the Graph Explorer with an account that's assigned the *Search And Purge* role in the Microsoft Purview compliance portal.
2. Run the following GET request to retrieve the ID for the eDiscovery (Premium) case. Use the value https://graph.microsoft.com/v1.0/security/cases/ediscoveryCases in the address bar of the request query. Be sure to select v1.0 in the API version dropdown list.

This request returns information about all cases in your organization on the Response preview tab.

3. Scroll through the response to locate the eDiscovery (Premium) case. Use the displayName property to identify the case.
4. Copy the corresponding ID (or copy and paste it to a text file). You'll use this ID in the next task to get the collection ID.

Tip

Instead of using the previous procedure to obtain the case Id, you can open the case in the Microsoft Purview compliance portal and copy the case Id from the URL.

Get the eDiscoverySearch ID

1. In Graph Explorer, run the following GET request to retrieve the ID for the collection that you created in Step 2, and contains the items you want to delete. Use the value https://graph.microsoft.com/v1.0/security/cases/ediscoveryCases/{ediscoveryCaseI

D}/searches in the address bar of the request query, where *{ediscoveryCaseID}* is the CaseID that you obtained in the previous procedure.

2. Scroll through the response to locate the collection that contains the items that you want to delete. Use the *displayName* property to identify the collection that you created in Step 3.

In the response, the search query from the collection is displayed in the *contentQuery* property. Items returned by this query are deleted in the next task.

3. Copy the corresponding ID (or copy and paste it to a text file). You'll use this ID in the next task to delete Copilot data.

Tip

Instead of using the previous procedure to obtain the search Id, you can open the case in the Microsoft Purview compliance portal. Open the case and navigate to the Jobs tab. Select the relevant collection and under Support information, find the job ID (the job ID displayed here is the same as the collection ID).

Delete Copilot data

1. In Graph Explorer, run the following POST request to delete the items returned by the collection that you created in Step 2. Use the value https://graph.microsoft.com/v1.0/security/cases/ediscoveryCases/{ediscoveryCaseID}/searches/{ediscoverySearchID}/purgeData in the address bar of the request query, where *{ediscoveryCaseID}* and *{ediscoverySearchID}* are the IDs that you obtained in the previous procedures.

If the POST request is successful, an HTTP response code is displayed in a green banner stating that the request was accepted.

For more information on purgeData, see sourceCollection: purgeData.

Delete Copilot data with PowerShell

Note

Because Microsoft Graph Explorer is not available in the US Government cloud (GCC, GCC High, and DOD), you must use PowerShell to accomplish these tasks.

You can also delete Copilot data using PowerShell. For example, to delete Copilot data in the US Government cloud you could use a command similar to:

```
Connect-MgGraph -Scopes "ediscovery.ReadWrite.All" -Environment USGov
```

Invoke-MgGraphRequest -Method POST -Uri '/v1.0/security/cases/ediscoveryCases/<ediscoverySearchID>/searches/<search ID>/purgeData'

For more information on using PowerShell to delete Copilot data, see ediscoverySearch: purgeData.

Step 6: Verify Copilot data is deleted

After you run the POST request to delete Copilot data, this data is removed from the user's mailbox. There isn't any visible notification or confirmation for the user that the data has been deleted.

Deleted Copilot data is moved to the *SubstrateHolds* folder, which is a hidden mailbox folder. Deleted Copilot data is stored there for at least 1 day and then are permanently deleted the next time the timer job runs (typically between 1-7 days).

Step 7: Reapply holds and retention policies to user mailboxes

After you verify that the Copilot data is deleted, you can reapply the holds and retention policies to user mailboxes that you removed in Step 4.

Appendix 10 – Data Residency for Microsoft Copilot for M365

Data Residency for Microsoft Copilot for Microsoft 365 - Microsoft 365 Enterprise | Microsoft Learn

[Captured 26/07/2024]

Data Residency for Microsoft Copilot for Microsoft 365

- Article
- 03/01/2024
- 3 contributors

Feedback

In this article

1. Overview
2. Data Residency Commitments Available for Microsoft Copilot for Microsoft 365

Overview

Service documentation: Microsoft Copilot for Microsoft 365 overview and Data, Privacy, and Security for Microsoft Copilot for Microsoft 365

Capability Summary: Microsoft Copilot for Microsoft 365 is an AI-powered productivity tool that coordinates large language models (LLMs), content in Microsoft Graph, and the Microsoft 365 apps that you use every day, such as Word, Excel, PowerPoint, Outlook, and Teams. This integration provides real-time intelligent assistance, enabling users to enhance their creativity, productivity, and skills. The following applications provide the ability to interact with Microsoft Copilot for Microsoft 365: Microsoft Word, Excel, PowerPoint, Loop, Outlook, Teams (Chat, Meetings, Calls, Whiteboard), and OneNote.

The content of interactions and the related semantic index with Microsoft Copilot for Microsoft 365 are stored at rest in the relevant *Local Region Geography*.

Data Residency Commitments Available for Microsoft Copilot for Microsoft 365

Product Terms

Required Conditions:

1. *Tenant* has a sign-up country/region included in Australia, Brazil, Canada, the European Union, France, Germany, India, Japan, Norway, Qatar, South Africa, South Korea, Sweden, Switzerland, the United Kingdom, the United Arab Emirates, or the United States.

Commitment:

For current language, refer to the Privacy and Security Product Terms and view the section titled "Location of Customer Data at Rest for Core Online Services."

Advanced Data Residency (ADR) add-on

Required Conditions:

1. *Tenant* has a sign-up country/region included in *Local Region Geography*.
2. *Tenant* has a valid Advanced Data Residency subscription for all users in the *Tenant*
3. For existing *Tenant* that has data stored in a *Macro Region Geography*, the *Tenant* Global Admin must opt in to move the *Tenant* data into the *Local Region Geography*.
4. The Microsoft Copilot for Microsoft 365 subscription customer data is provisioned in *Local Region Geography*.

Commitment:

Refer to the ADR Commitment page to understand the specific data at rest commitments for Microsoft Copilot for Microsoft 365. Examples of the committed data include:

- "Content of Interactions" such as the user's prompt and Microsoft Copilot's response, including citations to any information used to ground Microsoft Copilot's response.

Multi-Geo add-on

Required Conditions:

1. *Tenants* have a valid Multi-Geo subscription that covers all users assigned to a *Satellite Geography*
2. Customer must have an active Enterprise or CSP Partner Agreement.
3. Total purchased Multi-Geo units must be greater than 5% of the total eligible licenses in the *Tenant*.

Commitment: Multi-Geo capabilities in Microsoft Copilot for Microsoft 365 enable content of interactions with Microsoft Copilot for Microsoft 365 to be stored at rest in a specified *Macro Region Geography* or *Local Region Geography* location. Microsoft Copilot for Microsoft 365 uses the Preferred Data Location (PDL) for users and groups to determine where to store data. If the PDL isn't set or is invalid, data is stored in the *Tenant's Primary Provisioned Geography* location. The *Geography* where the content of interactions with Microsoft Copilot for Microsoft 365 are stored is determined by the PDL of the user interacting with Microsoft Copilot for Microsoft 365. This means that the storage of content of interactions for users in different regions will be based on their respective PDL configurations.

To find the current location of a user's content of interactions with Microsoft Copilot for Microsoft 365 by referencing the PDL configuration for that user. Refer to Multi-Geo Testing

Illustrative examples

Collaboration Experience Two people are working together on a Microsoft Word document. User A authored the document and stored it in the OneDrive for Business personal storage site, which is located in France. User B is in Canada and asks Microsoft Copilot for Microsoft 365 to rewrite a paragraph in the document. The paragraph User B submitted as the prompt, as well as the rewrite options Microsoft Copilot for Microsoft 365 provides (the "content of interactions" in this case) are stored in Canada; the original document remains in France, as does any rewrite the user accepts into that document.

Teams Meeting Experience Microsoft Teams meeting recording video location is determined by the user PDL that starts the recording, or when meetings have an automatic recording policy, the location is determined from the first person joining the meeting. When users in other regions interact with Microsoft Copilot for Microsoft 365 in Teams, those user prompts and corresponding responses are stored in the location of the user that asks the Microsoft Copilot for Microsoft 365 questions.

Migration

Microsoft Copilot for Microsoft 365 is part of the Microsoft 365 Advanced Data Residency migration. You can learn more at ADR Migration

How can I determine customer data location?

You can find the actual data location in Microsoft 365 admin center. In the coming months, you will be able to find the actual data location for committed data, by navigating to Settings > Org settings > Organization profile > Data location.

Appendix 11 – Learn about retention for Copilot for Microsoft 365

Learn about retention for Microsoft Copilot for Microsoft 365 | Microsoft Learn

[Captured 26/07/2024]

Learn about retention for Copilot for Microsoft 365

- Article
- 05/06/2024
- 2 contributors

Feedback

In this article

1. What's included for retention and deletion
2. How retention works with Microsoft Copilot for Microsoft 365
3. When a user leaves the organization
4. Configuration guidance

Microsoft 365 licensing guidance for security & compliance.

Note

Microsoft Copilot for Microsoft 365 messages are automatically included in the retention policy location named Teams chats and Copilot interactions because they are retained and deleted by using the same mechanisms. Users don't have to be using Teams for the retention policy to apply to Copilot for Microsoft 365.

The information in this article supplements Learn about retention because it has information that's specific to Microsoft Teams messages and interactions with Microsoft Copilot for Microsoft 365.

For other workloads, see:

- Learn about retention for SharePoint and OneDrive

- Learn about retention for Viva Engage
- Learn about retention for Exchange
- Learn about retention for Teams

For more information about Microsoft Purview integration with Copilot, see Microsoft Purview data security and compliance protections for generative AI apps.

Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview compliance portal trials hub. Learn details about signing up and trial terms.

What's included for retention and deletion

Retention policies for the location Teams chats and Copilot interactions include user prompts to Microsoft Copilot for Microsoft 365, and the Copilot responses to users. These messages can be retained and deleted for compliance reasons.

User prompts include text that users type, and selecting Microsoft Copilot for Microsoft 365 prompts that are captured as a prepopulated message. Copilot responses include text, links, and references. Because messages to indicate that a response is in progress don't have business value, these messages aren't captured.

How retention works with Microsoft Copilot for Microsoft 365

Use this section to understand how your compliance requirements are met by backend storage and processes, and should be verified by eDiscovery tools rather than by messages that are currently visible in Copilot.

You can use a retention policy to retain data from messages in Microsoft Copilot for Microsoft 365, and delete those messages. Behind the scenes, Exchange mailboxes are used to store data copied from these messages. Data from Copilot messages is stored in a hidden folder in the mailbox of the user who runs Copilot. This hidden folder isn't designed to be directly accessible to users or administrators, but instead, store data that compliance administrators can search with eDiscovery tools.

The Exchange mailbox for retaining Microsoft Copilot for Microsoft 365 messages has the RecipientTypeDetails attribute of UserMailbox, which also stores message data for Teams private channels and cloud-based Teams users.

After a retention policy is configured for Microsoft Copilot for Microsoft 365 interactions, a timer job from the Exchange service periodically evaluates items in the hidden mailbox folder where these messages are stored. The timer job typically takes 1-7 days to run. When these items

have expired their retention period, they're moved to the SubstrateHolds folder—another hidden folder that's in every user mailbox to store "soft-deleted" items before they're permanently deleted.

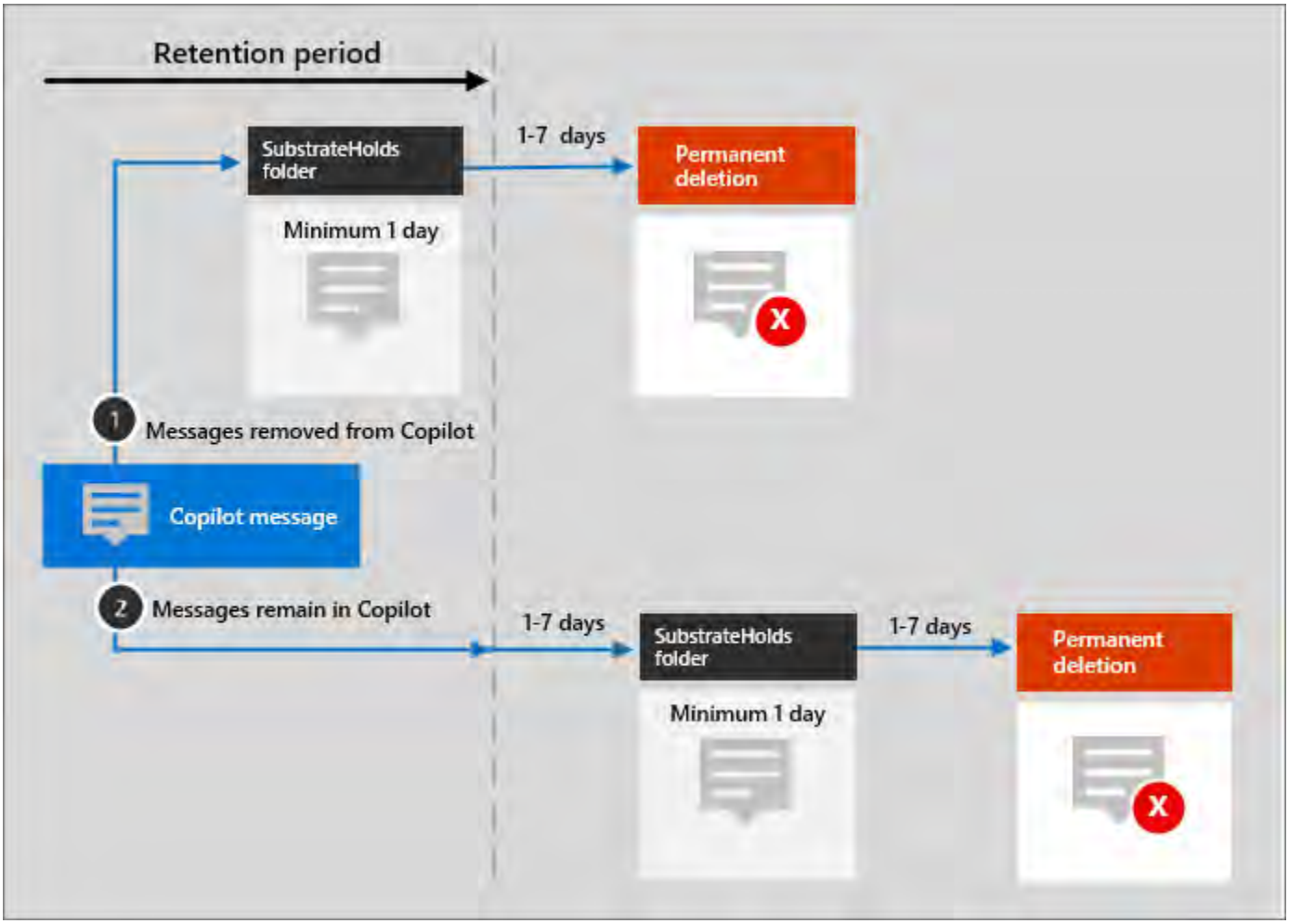
Messages remain in the SubstrateHolds folder for at least 1 day, and then if they're eligible for deletion, the timer job permanently deletes them the next time it runs.

Important

Because of the first principle of retention and since Copilot messages are stored in Exchange Online mailboxes, permanent deletion from the SubstrateHolds folder is always suspended if the mailbox is affected by another Copilot or Teams retention policy for the same location, Litigation Hold, delay hold, or if an eDiscovery hold is applied to the mailbox for legal or investigative reasons.

After a retention policy is configured for Microsoft Copilot for Microsoft 365, the paths the content takes depend on whether the retention policy is to retain and then delete, to retain only, or delete only.

When the retention policy is to retain and then delete:



In most scenarios, Copilot messages aren't removed. For example, they remain but are hidden when users close a chat window or close the app. However, Copilot messages are removed in the following scenarios:

- Users delete (when this option is available) the associated chat in Microsoft Copilot Graph-grounded chat.
- A request is submitted to delete a user's history of all interactions with Microsoft Copilot for Microsoft 365.

For the two paths in the diagram:

1. If messages are removed from Copilot, the message is moved to the SubstrateHolds folder where it remains for at least 1 day. When the retention period expires, the message is permanently deleted the next time the timer job runs (typically between 1-7 days).
2. If messages remain in Copilot after the retention period expires, the message is copied to the SubstrateHolds folder. This action typically takes between 1-7 days from the expiry date. When the message is in the SubstrateHolds folder, it's stored there for at least 1

day, and then the message is permanently deleted the next time the timer job runs (typically between 1-7 days).

Note

Messages stored in mailboxes, including the hidden folders, are searchable by eDiscovery tools. Until messages are permanently deleted from the SubstrateHolds folder, they remain searchable by eDiscovery tools.

When the retention period expires and copies a message to the SubstrateHolds folder, a delete operation is communicated to the backend service for Copilot, that then relays the same operation to the user app with Copilot. Delays in this communication or caching can explain why, for a short period of time, users continue to see these messages in Copilot.

Important

Messages visible in Copilot are not an accurate reflection of whether they are retained or permanently deleted for compliance requirements.

When the retention policy is retain-only, or delete-only, the content's paths are variations of retain and delete.

Content paths for retain-only retention policy

1. If messages are removed from Copilot the message is moved to the SubstrateHolds folder after the retention period expires. This action typically takes between 1-7 days from the expiry date. If the retention policy is configured to retain forever, the item remains there. If the retention policy has an end date for the retention period and it expires, the message is permanently deleted the next time the timer job runs (typically between 1-7 days).

2. If messages remain in Copilot after the retention period expires, nothing happens before and after the retention period; the message remains in its original location.

Content paths for delete-only retention policy

1. If messages are removed from Copilot during the retention period, the message is moved to the SubstrateHolds folder. The message is stored in the SubstrateHolds folder for at least 1 day and permanently deleted the next time the timer job runs (typically between 1-7 days).

2. If messages remain in Copilot after the retention period expires, the message is copied to the SubstrateHolds folder. This action typically takes between 1-7 days from the expiry date. The message is retained there for at least 1 day and then permanently deleted the next time the timer job runs (typically between 1-7 days).

Example flows and timings for retention policies

Use the following examples to see how the processes and timings explained in the previous sections apply to retention policies that have the following configurations:

- Example 1: Retain for 30 days and then delete
- Example 2: Delete-only after 1 day

For all examples that refer to permanent deletion, because of the principles of retention, this action is suspended if the message is subject to another retention policy to retain the item or it's subject to an eDiscovery hold.

Example 1: Retain for 30 days and then delete

On day 1, a user sends a prompt to Microsoft Copilot for Microsoft 365 and the prompt is removed after 10 days.

Retention outcome:

- After day 10, the message is moved to the SubstrateHolds folder, where it can still be searched with eDiscovery tools.
- At the end of the retention period (30 days from day 1), the message is permanently deleted typically within 1-7 days after the minimum of 1 day, and then won't be returned with eDiscovery searches.

Example 2: Delete-only after 1 day

Note

Because of the short one-day duration of this configuration and retention processes that operate within a time period of 1-7 days, this section shows example timings that are within the typical time ranges.

On day 1, a user sends a prompt to Microsoft Copilot for Microsoft 365 and this prompt isn't removed from Copilot.

Example retention outcome if the user's prompt isn't removed:

- Day 5 (typically 1-7 days after the start of the retention period on day 2):
    - The message is copied to the SubstrateHolds folder and remains there for at least 1 day.
- Day 9 (typically 1-7 days after a minimum of 1 day in the SubstrateHolds folder):
    - The message is permanently deleted and then won't be returned with eDiscovery searches.

As this example shows, although you can configure a retention policy to delete messages after just one day, the service undergoes multiple processes to ensure a compliant deletion. As a result, a delete action after 1 day could take 16 days before the message is permanently deleted so that it's no longer returned in eDiscovery searches.

When a user leaves the organization

If a user leaves your organization and their Microsoft 365 account is deleted, their Copilot messages that are subject to retention are stored in an inactive mailbox. The Copilot messages remain subject to any retention policy that was placed on the user before their mailbox was made inactive, and the contents are available to an eDiscovery search. For more information, see Learn about inactive mailboxes.

Configuration guidance

If you're new to configuring retention in Microsoft 365, see Get started with data lifecycle management.

If you're ready to configure a retention policy for Microsoft Copilot for Microsoft 365 interactions, see Create and configure retention policies.