**BUILD YOUR OWN DPIA**

**FOR**

**MICROSOFT 365 COPILOT**

**PUBLIC SECTOR CUSTOMERS**



# **Introduction**

This Build Your Own Data Protection Impact Assessment (“**DPIA**”)is provided by Microsoft as a reference for existing and prospective public sector customers who may need or want to complete a DPIA when using Microsoft 365 Copilot. It is designed to help public sector organizations systematically identify, assess, and address potential data protection risks, making it easier to evaluate compliance with the General Data Protection Regulation (“**GDPR**”) in their use of Microsoft 365 Copilot.

The structured approach of this customizable template broadly follows the [Sample DPIA Template of the Data Protection Commission of Ireland](https://www.dataprotection.ie/sites/default/files/uploads/2024-11/Sample-DPIA-Template-EN.pdf), adapted in certain points to align with practical needs. It offers a clear and pragmatic framework for conducting a DPIA in line with regulatory expectations. This may differ from a customer’s own DPIA format and is meant as a general guide rather than a comprehensive solution.

**Please note that this document is for informational purposes only and does not constitute legal advice.** Customers remain responsible for meeting all legal requirements related to their DPIA and the use of Microsoft 365 Copilot, as outlined in their agreement with Microsoft and their role under data protection laws (e.g. as a “data controller” or “data processor”). This document provides baseline information from Microsoft; customers will need to adapt the content to reflect how they have configured and are using Microsoft 365 Copilot because a DPIA is an assessment of the customers’ specific use of the service Microsoft provides.

Throughout this document, Microsoft has included explanations in bold italic navy-blue font to help guide customers through the process. Some sections also include illustrative examples that customers can review and tailor to their specific needs and processing activities.

This customizable and illustrative template also includes references to the [Product Terms](https://www.microsoft.com/licensing/terms/welcome/welcomepage) and the [Data Protection Addendum](https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA) (“**DPA**”) and explains how Microsoft 365 Copilot operates. However, customers must add their own specific details, risk assessments, mitigation measures, and approvals based on their unique context. Any capitalized terms not defined here have the same meaning as in the DPA and Product Terms.

For more detailed resources on data protection, including audit controls, compliance guides, whitepapers, and ISO reports on how Microsoft cloud services safeguard data, customers can refer to the [Service Trust Portal](https://servicetrust.microsoft.com/ViewPage/TrustDocuments). Additional helpful links, including the <https://learn.microsoft.com/> for M365 which contains details about the product family in which Microsoft 365 Copilot belongs, can be found in Annex 1.

**Contents**

[**Introduction** 1](#_Toc198722647)

[**Step 1: Identify the need for a DPIA** 3](#_Toc198722648)

[**Step 2: Describe the processing** 8](#_Toc198722649)

[**Step 3: Consultation process** 21](#_Toc198722650)

[**Step 4: Assess necessity and proportionality** 22](#_Toc198722651)

[4.1 Lawfulness, Fairness and Transparency 22](#_Toc198722652)

[4.2 Purpose Limitation 25](#_Toc198722653)

[4.3 Data Accuracy and Data Minimization 27](#_Toc198722654)

[4.4 The information that will be made available to individuals 29](#_Toc198722655)

[4.5 Data Subject Rights 30](#_Toc198722656)

[4.6 Processor Compliance 33](#_Toc198722657)

[4.7 International Transfers 33](#_Toc198722658)

[**Step 5: Identify and assess risksand Step 6: Identify measures to reduce risk** 37](#_Toc198722659)

[**Step 6: Sign off and record outcomes** 48](#_Toc198722660)

[**Annex 1** 49](#_Toc198722661)

# **Step 1: Identify the need for a DPIA**

***A DPIA is a process used to identify, assess, and reduce data protection risks, especially in new projects. Under the GDPR, customers (data controllers) must conduct a DPIA if an activity is “likely to result in a high risk to the rights and freedoms of natural persons”. However, Microsoft recognizes that some customers prefer to take a cautious approach and complete DPIAs even when the legal requirement may not apply, as a good practice. If you are unsure whether a DPIA is needed, Microsoft recommends checking guidance from relevant data protection authorities. While data protection authorities across the EU and EEA have provided guidance and templates for DPIAs, the sample DPIA from the Irish Data Protection Commission, available at*** [***this link***](https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#sample-dpia-template), ***serves as the foundation for this customizable DPIA template, while incorporating certain adaptations for practical application. Consult the website of your national data protection authority for additional resources specific to your country. The European Data Protection Board also issued*** [***guidelines***](https://ec.europa.eu/newsroom/article29/items/611236) ***on DPIAs, and Microsoft’s additional*** [***recommendations on DPIAs***](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-data-protection-impact-assessments?view=o365-worldwide) ***can also serve as useful resources.This section provides introductory information about the DPIA being conducted, including high level descriptions of the processing activity, key dates, and stakeholders involved.*[[1]](#footnote-2)**

| **Title** | **Description** |
| --- | --- |
| **1.1 General overview of the project** | ***Explanation: Please give a broad explanation as to what the aims of the project are and the type of processing it involves. Additionally, providing reference or linkage to other documents could prove beneficial (e.g. project proposal).***  Illustrative example: We are a government organization that wants to purchase Microsoft 365 Copilot. Microsoft 365 Copilot would provide AI-powered productivity and chat capabilities by coordinating the following components: (i) large language models (LLMs); (ii) content in the Microsoft Graph (a hub for operational data, including calendar, emails, chats, documents and meetings that our users have permission to access); and (iii) the Microsoft 365 productivity apps that our users use every day such as Word, Excel and PowerPoint. Microsoft 365 Copilot would operate within our tenant and subject to our users’ (at least view) permissions. In practice, the underlying functionalities allow Microsoft 365 Copilot to analyze, summarize, or generate content tailored to user input. For example, it can generate PowerPoint slides, draft emails, or extract trends from Excel data. For further details on how Microsoft 365 Copilot operates, refer to this link: [What is Microsoft 365 Copilot? | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-overview)  Our aim of the use of Microsoft 365 Copilot is to provide our civil servant users with a digital assistant to increase efficiency across our organization. Microsoft 365 Copilot would effectively operate as an assistant sitting over the data to which any given user has access from the Microsoft 365 productivity apps (Word, Excel, Teams, PowerPoint, Outlook) and Microsoft Graph information (content and metadata) to respond to prompts.  We intend to use Microsoft 365 Copilot to identify trends and patterns in data related to resource allocation and operational timelines. By leveraging Microsoft 365 Copilot alongside data already collected and organized in tools such as Excel, we aim to gain insights that will enhance our ability to allocate resources effectively and improve service delivery. This approach is expected to provide valuable analytics, enabling us to optimize operations and better meet organizational objectives. |
| **1.2 Target implementation date** | ***Explanation: Indicate here the intended implementation date and, if appropriate, any key variables which may affect this and corresponding date ranges.*** |
| **1.3 DPIA prepared by and maintained by (specify if different individuals)** | ***Explanation: This could be a named individual or someone in a specific role within the organization. The responsibility for preparing, owning, and maintaining the DPIA depends on the organization’s structure. For example, it may be managed by the Privacy Program Owner or fall under the legal or compliance functions.*** |
| **1.4 Date of next review of the DPIA** | ***Explanation: Please include the dates of changes made to this DPIA and summary of key changes. Microsoft recommends keeping the DPIA up to date and conducting regular reviews to ensure it reflects the current processing activities and associated risks, in particular, if there is a substantial change in the nature, scope, context or purpose of processing contemplated under the DPIA by the customer.***  ***For example:***   * ***Adoption of new service offerings or features which have been made available in connection with Microsoft 365 Copilot that materially change the data collection, use, or processing, such as adding additional licenses across the customer’s organization, thereby increasing the number of data subjects whose data is processed. Customers can track important upcoming changes through the*** [***Microsoft 365 roadmap***](https://www.microsoft.com/en-us/microsoft-365/roadmap?msockid=24f275b6e9bf67382c73664de8876661) ***and in the announcements in the*** [***Message Center***](https://learn.microsoft.com/en-us/microsoft-365/admin/manage/message-center?view=o365-worldwide)***.*** * ***Implementing new integrations or tools that interact with Microsoft 365 Copilot, potentially introducing new categories of data or processing purposes.*** * ***Situations where the customer’s intended specific use of a Microsoft 365 application significantly diverges from the contents of the DPIA.*** * ***Expanding data processing to include new geographic regions.*** * ***Significant changes in customer’s policy requirements related to data retention, security measures, or access controls that could alter the overall risk profile of processing activities.*** * ***Introduction of new features or functions that may impact the risk profile of processing activities, such as automation features, or enhanced analytics capabilities, which could increase the volume or sensitivity of personal data processed.*** |
| **1.5 Data Controllership** | Explanation: ***Customers should conduct an independent assessment of data controllership based on the facts and circumstances of where they deploy Microsoft 365 Copilot and how it is used.***  Illustrative example:  Under the terms of the Product Terms and DPA, we are the controller of Personal Data and Microsoft is the processor of such data, except (a) when we act as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in the Product-specific terms or the DPA.  Notably, there are no product-specific exceptions to this arrangement within Microsoft 365 Copilot, except for a limited number of optional connected experiences designed to enable our ability to generate, communicate, and collaborate more effectively.  Optional connected experiences are available for use through Microsoft 365 Copilot application experiences. These optional cloud-backed services are not covered by our license with Microsoft and there are instances where Microsoft is a data controller of personal data. These experiences are licensed directly to the user and use of these services by our users can be disabled by our administrator.  Some privacy controls for connected experiences in Microsoft 365 Apps can affect the availability of Microsoft 365 Copilot features. This includes the privacy controls for connected experiences that analyze our content and the privacy control for optional connected experiences.  **Privacy control for connected experiences that analyze our content**  If we turn off connected experiences that analyze our content on devices in our organization, certain Microsoft 365 features will not be available to our users in the following apps: Excel, OneNote, Outlook, PowerPoint, Word. There is also a privacy control that turns off all connected experiences (except for Essential Services that are necessary for M365 application functions - see [Essential services for Office - Microsoft 365 Apps | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/essential-services)), including connected experiences that analyze our content. If we use that privacy control, Microsoft 365 Copilot features will not be available in the apps and on the devices described above.  **Privacy control for optional connected experiences**  If we turn off optional connected experiences in our organization, Microsoft 365 Copilot features that are optional connected experiences will not be available to our users. For example, turning off optional connected experiences could affect the availability of [web search](https://learn.microsoft.com/en-us/copilot/microsoft-365/manage-public-web-access#it-admin-control-for-both-microsoft-365-copilot-and-microsoft-365-copilot-chat).  For further details on connected experiences, see [Connected experiences in Office - Microsoft 365 Apps | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/connected-experiences) and [Overview of optional connected experiences in Office - Microsoft 365 Apps | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/optional-connected-experiences)  **Privacy control for web grounding in Microsoft 365 Copilot**  We can also manage whether Microsoft 365 Copilot sends web search queries to Bing to improve the quality of responses with the latest information from the web as part of optional connected experiences for Microsoft 365. This control can be set at the user/group/tenant level.  Microsoft explains controls for web search more in this documentation: [Data, privacy, and security for web search in Microsoft 365 Copilot and Microsoft 365 Copilot Chat | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/manage-public-web-access) |
| **1.6 Data Processors** | ***Explanation: Customers should include necessary information from their perspective if they have additional data processors responsible for processing personal data, such as a third-party connected app.*** The illustrative example in response to this question is based on the approach envisaged by Microsoft’s [***Product Terms***](https://www.microsoft.com/licensing/terms/welcome/welcomepage) ***and the*** [***DPA***](https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA)***.***  Illustrative example:  Microsoft Ireland Operations, Ltd. is Microsoft’s primary entity responsible for processing Personal Data as part of our use of Microsoft 365 Copilot. Microsoft may hire Subprocessors to provide certain limited or ancillary services on its behalf, in accordance with the terms of the DPA. The [Microsoft Online Services Subprocessor List](https://go.microsoft.com/fwlink/?linkid=2096306)identifies subprocessors authorized to subprocess Customer Data or Personal Data in Microsoft 365 Copilot.  Since Microsoft 365 is designed as an extensible platform, fostering a pro-competitive ecosystem that enables us to enhance functionality through third-party integrations, we may also choose to integrate any third-party applications that operate under their own independent terms and conditions for data processing. |
| **1.7 Decision whether to carry out a DPIA** | ***Explanation: Concisely detail why you believe there is a need or wish (as a good practice) to undertake a DPIA and emphasize if the DPIA is built on an existing DPIA / risk assessment, to the extent it is relevant. You may refer to Article 35 of the GDPR or the*** [***Guidelines of the European Data Protection Board on Data Protection Impact Assessment***](https://ec.europa.eu/newsroom/article29/items/611236)***, which outline the criteria for when a DPIA may be required. Please consider that the EDPB in its 2022 coordinated enforcement action on use of cloud-based services by the public sector assumed that a DPIA was likely needed if a public sector organization deploys cloud services. Also, data protection supervisory authorities establish guidance with illustrative examples of processing activities that require, or do not require, a DPIA.*** |

# **Step 2: Describe the processing**

This section describes and analyses the processing activity under review in the DPIA in more detail. It includes questions relating to the rationale behind carrying out this processing, objectives sought to be achieved, the personal data likely to be processed, and the individuals whose personal data will be processed. This section can provide customers’ detailed information about the envisaged processing.

| **Title** | **Description** |
| --- | --- |
| **2.1 Please outline the type of processing involved: what methods will be used for the collection, usage, storage and deletion of the data? How is the data being sourced? Is the data to be shared with anyone? A flow diagram or some other way of describing data flows may prove useful. Are any of the types of processing identified as high risk?**  **(Articles 13 and 14 of the GDPR)** | Explanation: This section provides a high-level description of the operation of Microsoft 365 Copilot. However, customers should check that this reflects factually the activities that they are undertaking, and any additional customer-specific information that is relevant should be added on a case-by-case basis. This should include the primary purposes for which the data are collected and used, and a brief description of the use of Microsoft 365 Copilot to facilitate such purposes. ***Microsoft has included an illustrative example as well.*** The description should help the customer / a regulator understand the specific context in which the customer’s specific use of Microsoft 365 Copilot may pose high risks from a data protection perspective. T***his evaluation should be carried out only if the customer considers the processing to be high risk, as DPIAs are primarily required to assess potentially high-risk processing activities.***  Illustrative example:  Microsoft 365 Copilot 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. Microsoft 365 Copilot provides real-time, intelligent assistance which enables our civil servant users to enhance their creativity, productivity, and skills. Microsoft 365 Copilot is built on top of the same cloud infrastructure as its Microsoft 365 applications, and adheres to all existing privacy, security, and compliance commitments that apply to Microsoft 365. Microsoft 365 Copilot uses the organizational content in our Microsoft 365 tenant.  What this means in practice is that Microsoft 365 Copilot accesses content and context through Microsoft Graph (which includes data processed in our organization, such as user documents, emails, calendar, chats, meetings, and contacts and more only in accordance with existing access permissions). Microsoft 365 Copilot then combines this content with the working context of our relevant civil servant user, such as the meeting our civil servant user is in now, the email exchanges the user had on a topic, or the chat conversations the user had last week, subject to our data retention practices and settings. Microsoft 365 Copilot uses this combination of content and context to help provide relevant and contextual responses. Microsoft 365 Copilot only surfaces organizational data to which individual users have at least view permissions.  Copilot responds to prompts from our users. A “prompt” is the term used to describe how our user asks Microsoft 365 Copilot to do something for us - such as creating, summarizing, editing, or transforming. When Microsoft 365 Copilot uses content from our Microsoft 365 tenant to augment the user’s prompt and enrich the response, as described above, this is called “grounding”. Grounding is different to training.  When our civil servant user interacts with Microsoft 365 Copilot (using apps such as Word, PowerPoint, Excel, OneNote, Loop, or Whiteboard), Microsoft stores data about these interactions. The stored data includes the user's prompt and Microsoft 365 Copilot's response, including citations to any information used to ground Microsoft 365 Copilot's response. The record of those interactions is the user’s Microsoft 365 Copilot activity history. This data is processed and stored in alignment with the DPA terms that already apply to our other content in Microsoft 365. The data is encrypted while it is stored and is not used to train generative foundation AI models, including those used by Microsoft 365 Copilot, unless instructed by us.  Under the GDPR, “data processing” means “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”. In the context of using Microsoft 365 Copilot, data processing refers to the collection, access, analysis and generation of outputs based on personal data (such as emails, documents, chats, calendar entries, and other content stored within Microsoft 365) in order to provide intelligent assistance, suggestions, summaries, and content creation.  Potential use cases within our organization:   * **Microsoft Teams**: it can provide real-time discussion summaries, take meeting minutes, identify action items, compile next steps and assign tasks to team members. In this case, for example, meeting transcripts and recordings (if enabled), chat content, participant names and roles, calendar invites and scheduling data, action items, tasks, and follow-ups, shared files or links can be processed. * **Microsoft Word**: it can assist in generating draft documents from instructions or bullet points, and also enhancing text, grammar, and style while adapting tone to the target audience. It can also summarize lengthy documents and reports. In this case, for example, text and content within Word documents, user inputs (instructions, bullet points), document data (author, version history), target audience references (for tone adaptation) can be processed. * **Microsoft Excel**: it can analyze data sets to identify trends and patterns, and simplify complex layouts. It can also generate advanced formulas using natural language inputs, and recommend charts and graphs for effective data visualization. In this case, for example, spreadsheet data (tables, numbers, text), column and row labels, user queries in natural language, data structure, and summaries can be processed. * **Microsoft Outlook**: it can summarize long e-mail chains and generate suggested responses based on context, tone, and prior communication. It can also identify and suggest calendar appointments or tasks derived from email content to draft initial replies to e-mails. In this case, for example, email subject lines and content, email data (sender/receiver), threaded email chains, tone and context from prior communications, calendar entries linked to emails, and tasks suggested from email content are processed. * **PowerPoint**: it can generate full presentations from documents or ideas, including suggestions for text, images, and design. It can also offer layout, color, and graphic recommendations, and transform reports into presentations by highlighting key points. In this case, input text, summaries, previously generated decks, author, images and graphics embedded or recommended, and design preferences are processed. * **SharePoint**: it can assist with content creation and editing, including text suggestions and structuring. It can also enable semantic searches to locate relevant content based on meaning rather than keywords, and analyze site content to identify knowledge gaps or overlapping information. In this case, for example, text and documents stored in SharePoint, site structure and usage data, content relationships (e.g. tags, topics, owners), user activity data (e.g. edits, views), search queries are processed.   The key aspects of the data processing are the following:  **Collection**: personal data may be collected when civil servants interact with Microsoft 365 Copilot, such as entering content in their user inputs (e.g. typed text, commands, uploaded documents).  **Access**: Microsoft 365 Copilot accesses content within Microsoft 365 apps (Word, Excel, Outlook, Teams, SharePoint, etc.), it may pull data from across different Microsoft 365 services to respond to a civil servant user’s query, and it may access previously generated or shared content relevant to the prompt.  **Analysis**: it may include language processing and semantic understanding of user input, contextual analysis of communications and documents (e.g. tone, purpose), pattern recognition in data sets (e.g. trends in Excel) and the extraction of tasks, decisions, or action items from communications.  **Generation of outputs**: it may include drafted emails, documents, or presentations, summarized content (e.g. meeting notes, email threads, reports), visuals and formulas (e.g. Excel charts, PowerPoint slides), suggestions for tasks, responses, or follow-up actions.  Microsoft 365 Copilot respects user specific permissions to any content or Microsoft Graph information it retrieves and only generates responses based on information that the user explicitly has permission to access.  For further details about Microsoft 365 Copilot, refer to these links:   * [Microsoft 365 Copilot – Microsoft Adoption](https://adoption.microsoft.com/en-us/copilot/) * [Microsoft 365 Copilot documentation | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/?ocid=CopilotLab_SMC_Resources_Admin) * [GDPR and Generative AI: A Guide for Public Sector Organizations](https://wwps.microsoft.com/blog/gdpr-genai) |
| **2.2 Please describe the scope of the processing: what type of data is involved, and does any of it fall under special category data? How much data will you be collecting and using? How often?**  **(Articles 5, 9, 13 and 14 of the GDPR)** | Explanation: This section can be used to set out the types of personal data expected to be processed in the context of the use of Microsoft 365 Copilot. Please update if there are specific categories of personal data that are processed and should be emphasized for the purposes of the data processing. It may be helpful for customers to leverage data classification systems and standards such as ISO 19944. Appendix B of the DPA (Data Subjects and Categories of Personal Data) contains a list of the ***types of Personal Data that customers may elect to include in Customer Data.***  Illustrative example:  **Scope of the Processing**  **What type of Personal Data is involved?**  In the context of our contract with Microsoft, we have considered that the DPA defines Personal Data in accordance with the GDPR, ensuring consistency with its legal framework as follows:  **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.  Pseudonymized identifiers may be included in data processed by Microsoft as a data processor in connection with Microsoft 365 Copilot 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.  We have also considered the types of data involved in the processing in the context of our contract with Microsoft.  According to the DPA, the types of Personal Data processed by Microsoft when providing the Microsoft 365 Copilot include: (i) Personal Data that we - as customer and data controller - elect 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 as data processor, including data sent to Microsoft as a result of our use of service-based capabilities or obtained by Microsoft from locally installed software. In the following part, we will provide examples of the types of Personal Data, accompanied by a more detailed textual description, including data sent to Microsoft as a result of our use of service-based capabilities or obtained by Microsoft from locally installed software.   1. **Customer Data** means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft as data processor by, or on behalf of, us - as customer and data controller - through use of the Online Service.   Microsoft treats all Customer Data as Personal Data, simply because only we - as customer and data controller - control whether the data we provide contains Personal Data. Microsoft treats all Customer Data as Personal Data because we, as the customer and data controller, determine what data is provided and processed to achieve our desired functional outcomes. In other words, we decide whether it contains Personal Data and, if so, what categories of Personal Data we have provided.  Prompts and responses are Customer Data, which does not change where these are retained so they can be accessed through Purview Content Search and/or E-Discovery.  For data subject request documentation in general and for Microsoft 365 Copilot specifically, refer to: [Office 365 Data Subject Requests Under the GDPR and CCPA - Microsoft GDPR | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365?view=o365-worldwide#microsoft-copilot-for-microsoft-365-and-personal-data)   1. **Data that may be generated, derived or collected by Microsoft in connection with providing Microsoft 365 Copilot include the following data that Microsoft comes into the possession of as Microsoft 365 Copilot is used:**   **Diagnostic data** are collected or obtained by Microsoft from software that is locally installed by us - as customer and data controller - in connection with the Online Service. Microsoft uses diagnostic data to keep Microsoft 365 secure and up to date, detect, diagnose and fix problems, and also for product improvements. This data does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Microsoft 365 Copilot. Certain diagnostic data is required, while some diagnostic data is optional. Required diagnostic data is the minimum data necessary to help keep Microsoft 365 Copilot secure, up-to-date, and performing as expected on the device it is installed on. The categories of required diagnostic data include software setup and inventory, product and service usage, product and service performance and device connectivity and configuration. Optional diagnostic data is additional data that helps Microsoft make product improvements and provides enhanced information to help detect, diagnose, and fix issues. This data may also be used in aggregate to train and improve experiences powered by machine learning, such as recommended actions, text predictions, and contextual help. Microsoft gives us the ability to choose whether to send Microsoft required or optional diagnostic data through the use of privacy controls, such as policy settings. We can see the diagnostic data being sent to Microsoft by using the “Diagnostic Data Viewer”. Examples of optional diagnostic data include data Microsoft collects about the shapes users insert into Word documents so Microsoft can provide better options, and data Microsoft collects about the time it takes for a PowerPoint slide to appear on the screen so Microsoft can improve the experience if it is slow.  The following articles contain further examples of diagnostic data:  [Required diagnostic data for Office - Microsoft 365 Apps | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/required-diagnostic-data)  [Optional diagnostic data for Office – Microsoft 365 Apps | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/optional-diagnostic-data)  Audit log schema (API), which includes Service Generated Data, is documented here: [Office 365 Management Activity API schema | Microsoft Learn](https://learn.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema)  **Personal data in system-generated logs:** Microsoft 365 generates system-generated logs as part of the regular operation of the services. These logs continuously record system activity over time to allow Microsoft to monitor whether systems are operating as expected. “Logging” (the storage and processing of logs) is essential to identify, detect, respond to, and prevent operational problems, policy violations, and fraudulent activity; optimize system, network, and application performance; assist in security investigations and resilience activities; and to comply with laws and regulations. While the focus of these logs is on how systems are operating and not on individual users, when events in Microsoft 365 are initiated by user interaction with a cloud service, some logs directly reflecting these events will – and must in order to fulfill their purposes – contain fields that either identify or can identify specific persons. These logs contain personal data. Examples of system-generated logs that may contain personal data include: (i) product and service usage data such as user activity logs; and (ii) data specifically generated by the interaction of users with other systems.  **Feedback data**: user-initiated feedback about Microsoft 365 Copilot is collected through Copilot experiences - for example, when our civil servant user selects the thumbs-up or thumbs-down icon on a Microsoft 365 Copilot response. After our user makes a selection, a feedback pane appears, prompting them to provide more details: what they liked (if thumbs-up) or what went wrong (if thumbs-down). This feedback mechanism helps to (i) improve the product quality of Microsoft 365 Copilot, including resolving issues more quickly with specific information about what we experienced; and (ii) prioritize feature requests that will enhance the Microsoft 365 Copilot experience. Feedback data may include prompts, generated responses, relevant content samples and/or additional log files. Microsoft does not use this feedback to train the generative AI foundation models that power Microsoft 365 Copilot. Our IT administrator has the ability to disable and manage feedback or prevent access to the community feedback portal.  Microsoft also provides additional details about how feedback data is collected in Microsoft 365 Copilot (for example, fields that are specific to the Copilot feedback experience) and what feedback data is collected with Copilot, as detailed in this article: [Providing feedback about Microsoft Copilot with Microsoft 365 apps - Microsoft Support](https://support.microsoft.com/en-us/topic/providing-feedback-about-microsoft-copilot-with-microsoft-365-apps-c481c26a-e01a-4be3-bdd0-aee0b0b2a423).  In addition to the above, the following articles contain general information about Microsoft 365 feedback:  [Manage Microsoft feedback for your organization - Microsoft 365 admin | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-feedback-ms-org?view=o365-worldwide)  [Learn about Microsoft feedback for your organization - Microsoft 365 admin | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/admin/misc/feedback-user-control?view=o365-worldwide)   1. **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 us (or that we authorize Microsoft to obtain from Microsoft 365) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services. Professional Services Data is not included in Customer Data.   In the context of Microsoft 365, Professional Services Data is relevant only to the extent that (i) we engage Microsoft for technical support related to problems or issues associated with the function of the services and applications, and (ii) we do not do so under the auspices of a separately negotiated contract for Unified Support or consulting services. We understand that it is solely under our control what data is provided to Microsoft, if any, for a technical support engagement. Accordingly, the only data that is treated as Professional Services Data by Microsoft for Microsoft 365 is the data we provide to Microsoft to obtain technical support. Professional Services Data is used by Microsoft solely for delivering the technical support services we request, including troubleshooting, addressing security issues, and improving the delivery of the services and products(s) for which we raise an issue, as described and limited in the DPA. We have determined which civil servants in our organization are permitted to initiate support engagements with Microsoft, and have instructed them appropriately to ensure they provide to Microsoft only that data minimally necessary to obtain necessary technical support, including but not limited to ensuring we do not provide to Microsoft for technical support any sensitive data that may be included within our Customer Data.  **What categories of personal data are involved, how much personal data will be collected and used, and how often?**  Appendix B of our DPA with Microsoft provides additional detail and transparency around the various categories of data that may be processed in connection with Microsoft 365 Copilot. The list in Appendix B features personal data that is included in e-mail, documents and other data in an electronic form in the context of Microsoft 365 Copilot , and any other data we – as customer and data controller - may elect to include in Customer Data and Professional Services Data, as identified in records maintained by us acting as data controller pursuant to Article 30 of the GDPR, as well as data that may be generated, derived or collected by Microsoft in connection with providing Microsoft 365 Copilot.  Depending on our use of Microsoft 365 Copilot as a customer and a data controller, we may elect to include personal data from any of the following categories in the personal data:   * **Organizational data**: Microsoft 365 Copilot will process the same data as the Microsoft 365 platform, subject to the applicable data classifications. This is “Customer Data” as defined in the [Product Terms](https://www.microsoft.com/licensing/terms/welcome/welcomepage) and the [Data Protection Addendum](https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA). Microsoft 365 Copilot can generate responses from our organizational data, such as our user documents, emails, calendar, chats, meetings, and contacts. The data subjects are our employees and all stakeholders involved in our operations.   Personal data is collected in different ways:   * data provided directly by our civil servant user (for example, in emails or documents); * data provided by others about our civil servant user (for example, creating documents with others' information); and * recording of meetings in Teams and transcription of completed meetings (this can also include physical meetings in rooms where Teams listens in). * **User Interactions with Microsoft 365 Copilot**: Our civil servant users enter prompts into Microsoft 365 Copilot and data is stored about these interactions. This includes the information contained within prompts, the data they retrieve, and the generated responses. Use of Microsoft 365 Copilot can lead to the collection of personal data, as a user can enter personal data in the prompt and ask Microsoft 365 Copilot to retrieve personal data in the response. Personal data can then be generated in Microsoft 365 Copilot's response. The record of interactions is the user’s Copilot interaction history, which is protected as Customer Data. * **Usage Data**: This could include specific actions the user takes within the application, such as the time they log in, the feature/Microsoft 365 product they used, and how often they use the application. The following article provides an overview of audit logs generated for user interactions and admin activities related to Microsoft 365 Copilot and AI applications: [Audit logs for Copilot and AI activities | Microsoft Learn](https://learn.microsoft.com/en-us/purview/audit-copilot)   It is worth noting that Microsoft 365 Copilot can also process data from the web, and commands issued to the web via Microsoft 365 Copilot may contain personal data.  **Does any of the Personal Data fall under special category data?**  Customer Data and Professional Services Data may contain special categories of personal data (e.g. benefits applications) and/or personal data relating to criminal convictions and offences (e.g. law enforcement case files).  Details on the processing of data are extensively documented here, including technical details of the supporting infrastructure:  [Data, Privacy, and Security for Microsoft 365 Copilot | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy)  [Transparency Note for Microsoft 365 Copilot | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-transparency-note)  [Data, privacy, and security for web search in Microsoft 365 Copilot and Microsoft 365 Copilot Chat | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/manage-public-web-access) |
| **2.3 Please describe the context of the processing: describe your relationship with the data subjects. How many individuals are you collecting data from? What is the area covered? What level of control will individuals have? Are they aware that their data will be used this way? Are children or other vulnerable groups included in the processing? Are there pre-existing security concerns? Is it unique in any way? What is the status of technology within the area? Should you consider any prevailing public concerns? Are you a part of any approved code of conduct or certification schemes?**  **(Articles 13 and 14 of the GDPR)** | Explanation: ***This section can be used to outline the types of data subjects whose personal data is expected to be processed in the context of using Microsoft 365 Copilot. It is the customer's responsibility to determine the relevant data subjects based on their specific use case. Please update this section if certain types of data subjects should be specifically emphasized for the purposes of data processing. Appendix B of the DPA (Data Subjects and Categories of Personal Data) provides a list of potential data subject categories for reference.***  Illustrative example:  **Data subjects**:  The data subjects whose personal data may be processed is the data that we – as customer and data controller - provide to Microsoft are civil servants and all stakeholders involved in our operations (such as contractors, suppliers, or individuals interacting with us via email, meetings, or shared documents).  Nature of relationship with the data subjects:  Internal users (civil servants with Microsoft 365): Microsoft 365 Copilot is a productivity-enhancing tool provided to civil servants for supporting their daily administrative, communication, and documentation tasks. Civil servants' data is processed to generate content, summarize information, suggest actions, and improve workflow efficiency based on their existing Microsoft 365 data.  External stakeholders: personal data of external contacts may be processed when they communicate with us via Teams, Outlook, or shared documents.  Estimated number of data subjects: the estimated number of data subjects whose personal data will be processed depends on our organizational structure and external interactions. The actual number may vary based on usage patterns, service adoption, and service needs.  The level of control of data subjects:  Based on our review of the product design and functionality of Microsoft 365 Copilot, we are confident that Microsoft continues to provide additional customer managed data compliance options, to control the use and access of Customer Data through Microsoft 365’s compliance tools.   * Data labelling allows to visually and technically protect the sensitivity labels of the information in the object (such as a document). This can be a file/email/prompt etc. The visual representation is being extended with dynamic watermarking and allows admins to prevent information protected by sensitivity labels attribution leakage by rendering a watermark dynamically on Word, Excel and PowerPoint documents when they are opened. * The new capability of extended protection for SharePoint files streamlines the labelling process by extending sensitivity labels to all documents at rest in a SharePoint library based on the sensitivity label of the library itself. This ensures that the documents in the library inherit the parent site label and are protected when downloaded or referenced by Microsoft 365 Copilot. * The extension of Data Loss Prevention policies to Microsoft 365 Copilot prevents Microsoft 365 Copilot to process files based on the sensitivity labels. This allows admins to configure Data Loss Prevention policies to exclude content to be processed from Microsoft 365 Copilot. Information with the sensitivity label connected to this Data Loss Prevention policy cannot be shown or processed by Microsoft 365 Copilot, helping to address oversharing concerns. |
| **2.4 Please describe the purposes of the processing: what do you want to achieve? What effect do you envisage this to have on individuals? What benefits will arise from the processing, both for you and on a wider scale?**  **(Articles 13 and 14 of the GDPR)** | Explanation: The response needs to contain sufficient detail to understand what and how the personal data will be processed and by whom. The narrative should help the customer / a regulator understand how personal data is processed and how the data flows using Microsoft 365 Copilot.  Illustrative example:  Microsoft 365 is a comprehensive cloud-based suite of applications and services designed to enhance productivity, communication, and collaboration. As part of its functionalities, Microsoft 365 involves the processing of personal data across its various applications, such as Word, Excel, PowerPoint, Outlook, and Teams, as well as cloud services like Exchange Online, Teams, OneDrive and SharePoint. We can specify the relevant suite of applications (e.g. Bookings, Calendar, Excel, Forms, Lists, OneDrive, OneNote, Outlook, Planner, Power Apps, Power Automate, Power BI, PowerPoint, Project, SharePoint, Stream, Sway, Teams, To Do, Visio, Viva Engage, Viva Insights, Whiteboard, and Word) in accordance with the applicable licensing arrangement.  Microsoft 365 processes a range of personal data depending on the services used, including user identification details (e.g. name, email), content created by our users and provided to the services (e.g. documents, emails, messages), and usage data (e.g. login times, interactions with apps) generated in delivering the service. This data is necessary for ensuring proper functioning of the service.  The primary purpose of using Microsoft 365 is to enhance productivity and collaboration by providing a suite of applications and services that enable users to create, edit, share, and manage documents, while facilitating seamless communication and teamwork across different platforms. This functionality is achieved through various applications, each serving a specific role in the ecosystem:   1. **Document creation and editing**: applications like Word, Excel, and PowerPoint allow users to create, edit, and collaborate on documents in real time. For example, Word enables users to draft text-based content, Excel allows for data analysis and spreadsheet management, and PowerPoint is used for creating presentations. These documents can be shared with colleagues for simultaneous editing, improving collaboration and reducing time spent on revisions. 2. **Document sharing and management**: through tools like SharePoint and OneDrive, Microsoft 365 facilitates secure document storage and sharing. Files can be easily uploaded to the cloud, organized in shared folders, and accessed by authorized users from different devices. OneDrive allows individuals to store personal files, while SharePoint is designed for team collaboration and document management across departments, ensuring that everyone has access to the most current version of a document. 3. **Team collaboration**: Teams serves as the central hub for team collaboration. Teams can chat in real time, share documents, and hold discussions, all within a unified platform. Users can create dedicated channels for specific topics, projects, or departments, allowing for focused conversations and easy access to relevant resources. Teams also works together with other Microsoft 365 tools, providing a cohesive environment where users can collaborate on documents, schedule meetings, and track tasks. 4. **Communication**: email and messaging functionalities are provided by Exchange Online and Teams. Outlook together with Exchange Online is used for managing email, scheduling meetings, and maintaining contacts, while Teams offers a platform for instant messaging and voice or video calls. Both tools enable smooth communication between colleagues, whether they are working in the same office or remotely. Outlook also integrates with calendars, helping users stay on top of appointments, meetings, and deadlines. 5. **Virtual meetings and scheduling**: Microsoft 365 includes scheduling and meeting tools. Teams enables users to schedule, host, and participate in virtual meetings with video, audio, and screen-sharing capabilities. These meetings can be recorded for future reference, and participants can collaborate on shared documents during the session. The integration with Outlook's calendar helps schedule meetings by finding available times and sending invitations, while Teams provides seamless communication for remote or hybrid teams.   Microsoft 365 is designed to support productivity, communication, and collaboration without inherently involving high-risk processing activities. While Microsoft 365 processes personal data - including user identification details (e.g. name, email) and content generated (e.g. documents, emails, messages) - these processing activities align with standard service operations and do not typically involve high-risk elements.  Several factors support this approach:   * Purpose and context of data processing: Microsoft 365 is primarily used for office productivity, document management, and communication. * The processing of personal data is incidental to these activities rather than the core purpose of the service. * The majority of data processed consists of standard service information, such as work emails, calendar entries, and shared documents. * Microsoft 365 provides granular access controls, privacy settings, and data governance tools, allowing organizations to manage permissions, restrict access, and implement data minimization practices. Users can actively provide, manage, and control their data within Microsoft 365 applications, including editing, deleting, and restricting access to shared files. * Microsoft 365 Copilot incorporates strong security measures defined in the “Data Security” section and in the table entitled “Security Measures” in Appendix A of the DPA. |
| **2.5 Describe how your data will be retained.**  **(Article 5(1)(e) of the GDPR)** | Explanation: The data retention is controlled by the customers. Customers have full authority to set, manage, and modify their retention policies to align with their specific service, legal, and compliance needs.  Illustrative example:  We have implemented retention policies and retention labels that are essential for managing the data lifecycle in Microsoft 365, allowing for the retention or deletion of content as needed. These retention settings can be applied to various Microsoft 365 services, including Exchange, SharePoint, OneDrive, Teams, and Viva Engage. Microsoft 365 Copilot can only access data that is still available and has not been permanently deleted according to the retention policy of a specific app. For example, if a retention policy is set to delete Teams chats after a certain period, Microsoft 365 Copilot will not be able to access those chats once deleted. Retention policies can be adaptive or static, and they can be applied at both the container level (e.g. SharePoint sites, Exchange mailboxes) and the item level (e.g., individual files or emails).  For further details, refer to [Learn about retention for Copilot and AI apps | Microsoft Learn](https://learn.microsoft.com/en-us/purview/retention-policies-copilot).  All user prompts to Microsoft 365 Copilot and responses from Microsoft 365 Copilot are stored as a record of those interactions in the user's Microsoft 365 Copilot interaction history and individual conversations or the entire history can be deleted by the user or administrators. Microsoft 365 Copilot can retain and delete messages for compliance reasons, including user prompts and Microsoft 365 Copilot responses.  It is possible to retrieve prompts in case of a data breach, investigation, or safeguarding concern (including Prevent), and administrators can use Microsoft Purview for investigations. Further details are available in this article: [Search for and delete Copilot data | Microsoft Learn](https://learn.microsoft.com/en-us/purview/ediscovery-search-and-delete-copilot-data).  We have also considered the data retention requirement in the context of our contract with Microsoft and are confident that the terms and conditions of the DPA enable us to meet our obligations under the GDPR. According to the provisions of the “*Data Retention and Deletion*” section of the DPA, at all times during the term of our subscription or the applicable Professional Services engagement, we will have the ability to access, extract and delete Customer Data stored in each Online Service and Professional Services Data. Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of our subscription so that we may extract the data. After the 90-day retention period ends, Microsoft will disable our account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless authorized under the DPA to retain such data. The following articles contain further information on data retention policies, retention labels, data deletion, and data destruction: [Data retention, deletion, and destruction in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview) and [Learn about retention policies & labels to retain or delete | Microsoft Learn](https://learn.microsoft.com/en-us/purview/retention?tabs=table-overriden). |

# **Step 3: Consultation process**

This section of the DPIA helps take a holistic view of the various multidisciplinary stakeholders involved in the DPIA process and account for their views and recommendations. These may be within the organization or external stakeholders.

|  |  |
| --- | --- |
| **Title** | **Description** |
| **3.1 Consider how to consult with relevant stakeholders: detail how and when you will seek the views of individuals or explain why it may not be correct to do so. Who within your organization needs to be involved? Do you need to seek the assistance of your processor? Do you plan to consult with information security experts or any other technical experts?**  **(Article 35.9 of the GDPR)** | ***Explanation: Please include all key stakeholders involved in completing this DPIA, e.g. the Data Protection Officer (DPO), Information Security Officer, or Privacy Program Owner. This is an indicative list of stakeholders who may be involved in the DPIA process. However, note that this list is likely to vary on a customer-by-customer basis. While Microsoft provides the information in this DPIA as guidance, it is the customer’s responsibility to apply it within their own context. Please include the necessary information from the customer's perspective, for example, how the customer will seek the views of those whose personal data will be processed as a result of this activity or justify why it may not be appropriate to do so. Additionally, if residual high risks are identified as part of this DPIA, the customer may need to formally consult the data protection supervisory authority regarding the envisaged processing activity on specific open questions they have regarding the deployment of a service. It is suggested that before proceeding with a consultation with the regulator, customers should contact their Microsoft contact person, such as their CSAM, for additional information.***  Illustrative example:  As part of the stakeholder engagement process, we reviewed the information provided by Microsoft, in particular, in the [Trust Center](https://www.microsoft.com/en-us/trust-center/) and the DPA, and conducted a full risk assessment in the context of our use of the service before the deployment of Microsoft 365 Copilot. |

# **Step 4: Assess necessity and proportionality**

***This section sets out accompanying rights that can be considered and complied with in relation to the processing activity, documentation can be drafted so the reader understands the basis and necessity of the activity, together with the compliance and proportionality measures.***

## 4.1 Lawfulness, Fairness and Transparency

| **Title** | **Description** |
| --- | --- |
| **4.1.1 Is there a lawful basis for the processing? Does the processing actually achieve your purpose?**  **(Articles 5 and 6 of the GDPR)** | Explanation: Under Article 6 of the GDPR, any processing of personal data must be justified by a legal basis. Without a valid legal basis, data processing would be unlawful, and customers would be in breach of their obligations as a data controller. For public sector organizations, defining the appropriate legal basis is crucial to ensure that the use of Microsoft 365 Copilot aligns with their statutory functions while respecting the rights and freedoms of data subjects. Establishing a legal basis ensures transparency, accountability, and compliance with data protection principles, particularly lawfulness, fairness, and transparency. Therefore, please include necessary information, based on the assessment of lawful basis under Article 6 of the GDPR. The first step is to map and describe the processing that occurs when Microsoft 365 Copilot is used for a specific purpose. Often, Microsoft 365 Copilot will be integrated with existing processing operations. By mapping the changes introduced by its use, customers can compare the "existing" and "new" processing operations and identify any additional or modified processing activities ("series of operations") that may arise. As regards the application of Article 6(1)(e) of the GDPR, there are two alternatives under this provision: (i) the performance of a task carried out in the public interest, and (ii) the exercise of official authority. The relevant alternative must be identified with a view to the particular operations of the public sector organization.  Illustrative example:  Microsoft 365 Copilot is a core service technology at our organization essential for delivering our statutory functions. It integrates with a suite of familiar Microsoft 365 applications (e.g. Word, Excel, Teams, Outlook, PowerPoint) to enhance productivity, streamline routine tasks, and support data-driven decision-making.  For example:  **Communications**: summarizing Teams meetings and suggesting action items.  **Document management**: drafting and refining documents in Word based on prompts.  **Task management**: extracting tasks from emails or meeting notes in Outlook or Teams.  **Data analysis**: generating insights and visualizations from Excel datasets using natural language queries.  In other words, Microsoft 365 Copilot can be used as a means to perform many different processing operations for different purposes, each with its own legal basis. The pre-defined purpose and the necessity to achieve that purpose determine the limits on what personal data can be processed and how.  We have considered this requirement in the context of our contract with Microsoft and are confident that the terms and conditions of the DPA enable us to meet this obligation under the GDPR. According to the provisions of the “*Nature of Data Processing; Ownership*” section of the DPA, Microsoft will process Customer Data and Personal Data only as described and subject to the limitations provided in the DPA: (a) to provide us with Microsoft 365 Copilot in accordance with our documented instructions and (b) for business operations incident to providing Microsoft 365 Copilot to us. Providing Microsoft 365 Copilot requires the service provider to process and store data to enable its functionalities, ensure the tool remains secure, up to date, and delivers the expected performance and productivity benefits. These are all “processing” of the data regardless of the technical activity being performed.  The DPA, defines “business operations” as the processing operations authorized by us in the “Processing for Business Operations Incident to Providing the Products and Services to Customer” section of the DPA. More specifically, in the DPA, we have authorized 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 Microsoft 365 Copilot to us.  Those purposes are: (i) billing and account management; (ii) compensation such as calculating employee commissions and partner incentives; (iii) internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and (iv) financial reporting.  When used for the specific business operation, the data is limited to aggregated or statistical data and not data that can identify or single out an individual.  Considering the above, our data processing is justified because, under Article 6(1)(e) of the GDPR, it is *necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us as data controller*”  This legal basis applies to public sector organizations like ours, as our operations involve delivering public services or exercising official authority. Processing personal data through Microsoft 365 Copilot supports these functions by enhancing productivity, streamlining administrative tasks, and facilitating communication and decision-making, all of which are essential for fulfilling our statutory obligations, aligned with our official duties and improving public service delivery.  For civil servants, the data processing is based on their contractual relationship with us. We provide Microsoft 365 Copilot as a necessary tool for fulfilling job responsibilities (Article 6(1)(b) of the GDPR). Thus, while both legal bases permit data processing within Microsoft 365 Copilot, the distinction reflects the different relationships and obligations we have toward stakeholders and civil servants.  **Additional preconditions of processing of special categories of personal data and/or personal data relating to criminal convictions and offences:**  Explanation: Processing of special categories of personal data and personal data relating to criminal convictions and offences requires compliance with additional preconditions under the GDPR; customers are advised to carefully assess and identify the specific legal basis and applicable conditions that justify such processing. |
| **4.1.2 Is there another way to achieve the same outcome?**  **(Article 5 of the GDPR)** | Explanation: ***Please update the illustrative example response with specific customer information, including why the customer chose Microsoft 365 Copilot as the best tool to achieve the intended purpose. How does it improve the effectiveness of achieving that purpose? Are there alternative methods that could meet the specific needs just as effectively, e.g. other less intrusive means (involving less processing of personal data)? Microsoft has included an illustrative example to assist with this process.***  Illustrative example:  The processing of Customer Data within Microsoft 365 Copilot is ongoing, making anonymization of Personal Data (following which information cannot be used to identify individuals) or pseudonymization of Customer Data (following which information cannot be used to identify individuals without access to additional information held separately) unworkable in these contexts. For instance, while the logs are pseudonymized, the Customer Data, including content of files is not. It is encrypted in storage but is unencrypted and is not modified to pseudonymize or anonymize our content when processed.  It is also worth noting that Microsoft 365 Copilot is tightly integrated into Microsoft 365 applications and adapted to the interface and work tasks within each tool. This integration allows users to receive assistance directly within the application, eliminating the need to move information between different applications or interfaces. This is highly beneficial as it streamlines workflows, enhances productivity, and reduces the risk of errors or data loss during transitions between systems.  However, there are no other less intrusive means to achieve the same outcomes as Microsoft 365 Copilot, considering the following factors:   * **Integration with existing Microsoft ecosystem**: Microsoft 365 Copilot is natively integrated with Microsoft 365 tools (e.g. Word, Outlook, Teams), which are already in widespread use across our organization, avoiding the need for additional third-party tools or data transfers. * **Data security controls**: Microsoft 365 Copilot benefits from the enterprise-grade security, compliance features, and data residency options of Microsoft 365, reducing the need for additional processing environments that could pose higher risks. * **Minimal duplication of data**: Microsoft 365 Copilot works on top of data already stored in Microsoft 365, ensuring no additional or parallel data storage is necessary. * **Efficiency and contextual relevance**: Microsoft 365 Copilot leverages user context (e.g. recent emails, calendar invites, documents) to provide precise and task-relevant assistance, which would otherwise require more manual processing or less efficient tools. * **Administrative and audit controls**: we can manage Microsoft 365 Copilot via the Microsoft 365 admin center, allowing detailed control over access and activity logging, unlike external tools which may not offer the same level of oversight. |

## 4.2 Purpose Limitation

| **Title** | **Description** |
| --- | --- |
| **4.2.1 Can function creep be prevented? In other words, what controls are in place to prevent personal data being used for another purpose incompatible with the primary purpose of collection or those falling under the lawful basis for collection and processing?**  **(Articles 5 and 6 of the GDPR)** | Explanation: Purpose limitation is a principle under Article 5 of the GDPR that personal data should only be collected for specified, legitimate purposes and not further processed in a way that is incompatible with those purposes. ***Please include the necessary information as required, based on controls established in relation to compliance with the GDPR’s purpose limitation principle. For example, if Microsoft 365 Copilot is used for a few selected roles that perform a limited amount of processing, this should be clearly outlined.***  Illustrative example:  The purpose limitation principle asserts that personal data must be collected for specified, explicit, and legitimate purposes, and cannot be further processed in ways that are incompatible with those purposes. When evaluating the purposes of processing, it is crucial to recognize that Microsoft 365 Copilot serves as a tool or function - essentially a means to achieve the intended processing purpose. Therefore, the use of Microsoft 365 Copilot itself is not a purpose but rather a method employed to fulfill the specified objectives of the data processing.  We meet the purpose limitation principle through ensuring that the purpose of data processing is clearly defined to align with the expectations of the data subjects. We ensure transparency by providing comprehensive privacy notices that offer civil servants and stakeholders clear insights into the data processing activities, detailing the specific ways in which their data is being used. This approach ensures that the use of Microsoft 365 Copilot is consistent with the data subjects' reasonable expectations and complies with privacy regulations.  We will also define the purpose of processing and the permitted use of Microsoft 365 Copilot for each individual user, ensuring they adhere to it with every instruction. To achieve this, we will establish a clear framework for civil servants, including guidelines, routines, and training, to ensure they use Microsoft 365 Copilot in compliance with the purpose limitation principle, aligned with each user's role in the organization and their respective access rights. This framework will mandate that personal data cannot be processed outside its intended context or for a different purpose. For instance, we ensure that civil servants have a clear understanding of expected usage, prohibited activities, and the appropriate channels for raising queries when considering new or innovative uses of a particular application. We will also train civil servants to limit the scope of their searches by providing clear and effective instructions. We have considered that Microsoft is providing us with certain information and controls we need to make choices when we are using Microsoft 365 Copilot. Further information on those controls is available at [Overview of privacy controls for Microsoft 365 Apps for enterprise - Microsoft 365 Apps | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/overview-privacy-controls)  We have also considered this requirement in the context of our contract with Microsoft and are confident that the terms and conditions of the DPA enable us to meet this obligation under the GDPR. In the “Nature of Data Processing; Ownership” section of the DPA, Microsoft undertakes that it will use and otherwise process Customer Data, Professional Services Data, and Personal Data only as described and subject to the limitations provided in the DPA. According to the provisions of the “Data Access” subsection of the “Data Security” section of the DPA, Microsoft employs least privilege access mechanisms to control access to Customer Data (including any Personal Data therein). Role-based access controls are employed to ensure that access to Customer Data required for service operations is for an appropriate purpose and approved with management oversight. For Core Online 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.  Further details on the data security for Microsoft 365 Copilot are available in this documentation: [Data, Privacy, and Security for Microsoft 365 Copilot | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy) |

## 4.3 Data Accuracy and Data Minimization

| **Title** | **Description** |
| --- | --- |
| **4.3.1 How will data quality and data minimization be assured?**  **(Article 5 of the GDPR)** | Explanation: Data accuracy refers to the principle under Article 5 of the GDPR that personal data must be accurate, complete, and kept up to date. Customers must take reasonable steps to ensure that any inaccurate data is corrected or erased without delay. Data minimization means that personal data collected should be limited to what is necessary for the purposes for which it is processed. Customers may want to amend the list below to align with specific controls used  Illustrative example:  Under the principle of accuracy, there is a legal obligation to ensure personal data is accurate, and reasonable steps must be taken to rectify or erase any inaccurate data in relation to the purposes for which it is processed. We understand and recognize the importance of such principle and that we are responsible for the content produced by our users when using Microsoft 365 Copilot, a tool designed to help them be more productive by providing ideas, suggestions, proposals for their consideration. We also recognize the risks of over-reliance on AI generated content and factor that into our use of Microsoft 365 Copilot.  To reduce the risk of incorrect personal data being generated, we implement several measures. These measures include establishing rules, guidelines, and providing training and upskilling for users, with a focus on effective instruction design and clear rules regarding the appropriate use of Microsoft 365 Copilot. Users are encouraged to engage in responsible prompting and use of available tools and configuration to ensure that the prompts they input into Microsoft 365 Copilot are clear, specific, and designed to minimize the likelihood of generating outputs that are unnecessary, irrelevant, or do not meet accuracy and fairness standards. Users can influence or guide how Microsoft 365 Copilot responds through their prompting. For example, if a user prompts Microsoft 365 Copilot with “Summarize this email in a friendly tone," it will respond more casually, whereas a prompt like "Draft a formal response to a customer complaint" will result in a more formal reply. We also implement post-processing controls to review generated content and procedures for promptly correcting or deleting inaccurate data. To prevent the use of incorrect personal data potentially generated by Microsoft 365 Copilot, users must always verify whether the response contains errors and assess whether such errors could pose a risk to the rights of the data subject. In other words, it is crucial that the user critically evaluates the outputs of Microsoft 365 Copilot and has the time and expertise to detect and correct any inaccurate personal data that may arise. Human oversight should be integrated into decision-making processes where the outputs of Microsoft 365 Copilot could lead to legal or significant consequences for individuals. This includes ensuring that automated decisions are subject to review by qualified personnel who can assess the fairness, accuracy, and relevance of the outputs.  Based on our review of the product design and functionality of Microsoft 365 Copilot (with notice about capabilities and limitations of generative AI) and the product naming and positioning as an assistant, we are confident that it helps set appropriate expectations about using this type of technology and supports the measures mentioned above as follows:   * Microsoft explicitly named the product “**Co**pilot” to reflect that it is intended to “assist” humans and not replace human judgment, autonomy or responsibility. * Microsoft 365 Copilot goes beyond verbatim data and aggregates/summarizes underlying documents and sources to generate results, and it points to the sources used in providing generated output suggestions for the user to review and easily revise. For further details, please refer to the following article: [Traditional Search vs. Copilot | Microsoft Copilot](https://www.microsoft.com/en-us/bing/do-more-with-ai/traditional-search-vs-bing-chat-ai-search?msockid=02ed0781eebd625030dc1397ef2c63a4&form=MA13KP) * Microsoft provides in-product notice to the user that generated output content may not be accurate and should be reviewed and revised. * Microsoft 365 Copilot leverages search technology intended to only process data in the Microsoft Graph that is relevant to a user’s prompt; therefore, with focused prompting we can minimize what data is processed in order to generate a response. * Microsoft provides reasonable notice and information to us and our users to support their ability to review and control the accuracy of their final content when aided by use of Microsoft 365 Copilot. * Microsoft includes information about the technical limitations of generative AI in their public documentation: [Data, Privacy, and Security for Microsoft 365 Copilot | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy#about-the-content-that-microsoft-365-copilot-create) * We may also evaluate the use of agents for specific, more sensitive scenarios, as they offer greater control over the data used in generating responses and allow the use of predefined instructions (similar to metaprompts) to guide Microsoft 365 Copilot’s behaviour.   Feedback data collected by Microsoft and the underlying feedback mechanism also contribute to improved data accuracy. For example, when our user flags a response as incorrect (e.g. thumbs-down), Microsoft receives a direct signal that the output may be inaccurate. This allows them to investigate and improve how Microsoft 365 Copilot handles similar prompts in the future. In addition, because our users can provide additional comments, Microsoft can understand why a response was potentially inaccurate (e.g. outdated information, misinterpretation of context), and improve future responses. In addition, if there are concerns about specific personal data appearing in a response, we can submit a support request to Microsoft for further investigation. |

## 4.4 The information that will be made available to individuals

| **Title** | Description |
| --- | --- |
| **4.4.1 What information will be made available to individuals?**  **(Articles 13 and 14 of the GDPR)** | Explanation: Under Article 13 and Article 14 of the GDPR, organizations must provide individuals - in the form of a data protection notice (also known as a privacy notice) - with clear and concise information about the collection and processing of their personal data. Microsoft has provided an illustrative example response that customers may wish to update by including references to relevant external and internal privacy notices that may be shared with data subjects. It is strongly recommended to use the functionality provided in Microsoft 365 to ensure the customer’s privacy policy appears to users within the service experience. This article explains how an administrator can add privacy-related info to an organization's directory, through the Microsoft Entra admin center: [Add your organization's privacy information - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/entra/fundamentals/properties-area)  Illustrative example:  We have reviewed our privacy notices and confirmed that they are comprehensive enough to cover the processing activities associated with the use of Microsoft 365 Copilot. This includes, if necessary, detailing specific use cases, and the operations that stem from the implementation of Microsoft 365 Copilot. To ensure clarity, we will present this information in the most understandable way possible. Wherever possible, we will directly communicate with data subjects to inform them about the processing activities carried out and how it affects them individually. If direct communication is not feasible, we will ensure that the relevant information is accessible through our contact points, such as on our website or intranet. This information will be regularly reviewed and, if necessary, updated to reflect any changes in our use case.  Our administrators have added our global privacy contact and our privacy statement here: […].  Based on our review of the product design and functionality of Microsoft 365 Copilot, we are also confident that Microsoft has demonstrated its commitment to transparency as a core principle of its Responsible AI program. For more details on the Responsible AI principles of Microsoft, refer to: [Microsoft Responsible AI Transparency Report | Microsoft CSR](https://www.microsoft.com/en-us/corporate-responsibility/responsible-ai-transparency-report?msockid=088cf58b8cb2676b179de1368d0166b1)  Microsoft also provided transparency in its new Microsoft 365 Copilot transparency note (see: [Transparency Note for Microsoft 365 Copilot | Microsoft Learn)](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-transparency-note), which provides more detailed insights into Microsoft’s Responsible AI protections. For example, Microsoft 365 Copilot uses AI-based classifiers and content filters. Content filters are models, and their training data was developed using data that has been labelled, reviewed, and iteratively refined by human experts, ensuring an additional layer of oversight and a comprehensive contextual understanding, in alignment with the Responsible AI standards of Microsoft.  Microsoft 365 Copilot has been certified for compliance with ISO 42001 (AI Management System). |

## 4.5 Data Subject Rights

| **Title** | **Description** |
| --- | --- |
| **4.5.1 How will you safeguard the rights of individuals?**  **(Chapter III of the GDPR)** | Explanation: Under Chapter III of the GDPR, data subjects have the right to access, rectify, and erase their personal data. They can also restrict processing, object to its use, and request data portability. Additionally, individuals have rights related to automated decisions, including profiling, and can withdraw consent at any time. Please include necessary information based on external and internal procedures for supporting data subject rights. Illustrative and Microsoft supportive information in this regard is set out below. Where the customer uses a third-party system, they can determine which (if any) parts of the system provide tools related to enabling individuals to exercise their rights (e.g. using the [***DSR Case Tool***](https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool)in the Office 365 Security & Compliance Center to manage data subject requests).  Illustrative example:  We will update our internal data subject rights management processes to include procedures reflecting the use of Microsoft 365 Copilot to acknowledge the following:   * According to the transparency documentation by Microsoft and providers of its LLMs, the large language models used in Microsoft 365 Copilot have been trained with privacy by design. This includes measures such as avoiding the active collection of personal data, filtering training data to exclude personal data where possible, and ensuring that personal data when incidentally present in training data is used only to help the model understand language patterns, such as how publicly available names or addresses appear in context. Output generated by Microsoft 365 Copilot may contain personal data. If this occurs, we may be subject to the right of access from the data subject, who may have the right to receive a copy of their personal data. We will always consider whether an access request can be fully answered, ensuring that we can identify all places where personal data is processed in Microsoft 365 Copilot. * Additionally, Microsoft 365 Copilot can generate new personal data based on user prompts and inputs. In the event of an access request, we will strive to disclose the source of any personal data that Microsoft 365 Copilot has generated based on user prompts. * We intend to tag content generated using Microsoft 365 Copilot. The storage location of generated content will depend on the specific use case, but it should align with the storage location of other documents for the task or use case prior to using Microsoft 365 Copilot. * One notable aspect of using Microsoft 365 Copilot is the storage of interaction records. Interaction records will be stored in accordance with our current retention policy and searchable by administrators. However, the data subject will only have the right to access their own personal data that may be stored in the interaction records. The right of access shall not adversely affect the rights and freedoms of others. * Personal data could potentially be stored with all users in the organization, for example, in a document that is only stored with one person. In these cases, we will do our best efforts to facilitate the enforcement of the data subjects' rights, and to have an overview of where the relevant personal data is stored. Data subjects can also correct and delete personal data they have access to, for example, when interacting with others in Teams channels. * Microsoft 365 Copilot may generate personal data about data subjects that is incorrect. This will be personal data associated with a person, which may be perceived as incorrect by the data subject but not necessarily by others who process the personal data. To manage this, we will establish clear guidelines for users on how to interact with Microsoft 365 Copilot, emphasizing principles for user prompting that minimize processing of personal data and the importance of verifying the accuracy of the data generated. Regular training will help users better understand how to assess the content produced by Microsoft 365 Copilot. We will also implement processes for users to review and validate personal data generated by Microsoft 365 Copilot. This will help ensure that any inaccuracies are promptly identified and corrected. Finally, we will set up a system for users to flag potentially incorrect or inaccurate information generated by Microsoft 365 Copilot. This system will alert data owners or relevant personnel to investigate and make necessary corrections. We have an internal policy prohibiting our users from using Microsoft 365 Copilot to make automated decisions without appropriate human oversight when such decisions may have a consequential impact on an individual’s legal or financial position, life or employment opportunities, human rights, or may result in physical or psychological harm, consistent with Microsoft’s Enterprise AI Services Code of Conduct. * All user prompts to Microsoft 365 Copilot and responses from Microsoft 365 Copilot are stored by default as a record of those interactions in the user's Microsoft 365 Copilot interaction history and individual conversations or the entire history can be deleted by the user or administrators.   We have considered the requirement of ensuring that data subjects are able to exercise their data protection rights in the context of our contract with Microsoft and are confident that the terms and conditions of the DPA enable us to meet this obligation under the GDPR. As a data processor, Microsoft provides assistance in supporting us to fulfil data subject requests. This is made clear in the “Data Subject Rights; Assistance with Requests” section of the DPA. Microsoft will make available to us, in a manner consistent with the functionality of Microsoft 365 Copilot 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 our 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 us. We will be responsible for responding to any such request including, where necessary, by using the functionality of Microsoft 365. Microsoft shall comply with reasonable requests to assist us with our response to such a data subject request. In Attachment 1 of the DPA (*European Union General Data Protection Regulation Terms*), Microsoft also confirms that taking into account the nature of the processing, it shall assist us by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the our obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR. The following article contains further information on addressing a data subject request for Copilot-related personal data: [Office 365 Data Subject Requests Under the GDPR and CCPA - Microsoft GDPR | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365) |

## 4.6 Processor Compliance

| **Title** | **Description** |
| --- | --- |
| **4.6.1 How do you arrange for processor compliance?**  **(Article 28 of the GDPR)** | Explanation: Please include necessary information from the perspective of the customer as required.  Illustrative example:  We have considered the need to monitor the data processor’s compliance with the data protection requirements in the context of our contract with Microsoft and are confident that the terms and conditions of the DPA allow us to do so.  In the “Auditing Compliance” subsection of the “Data Security” section of the DPA, Microsoft commits to conduct regular audits of its security measures related to Customer Data, Professional Service Data, and Personal Data, in line with applicable standards or frameworks. Audits are performed annually by independent, third-party auditors at Microsoft’s expense, with the results shared via the Microsoft Audit Report. If needed, Microsoft will support additional audits requested by us, agreeing on scope, timing, and fees. On the [Service Trust Portal](https://servicetrust.microsoft.com/), among the Audit Reports, we can review the available independent audit reports for Microsoft's cloud services, which provide information about compliance with data protection standards and regulatory requirements, such as International Organization for Standardization (ISO), Service Organization Controls (SOC), National Institute of Standards and Technology (NIST), Federal Risk and Authorization Management Program (FedRAMP), and the GDPR. |

## 4.7 International Transfers

This section covers the use and sharing of data as part of the envisaged processing activity outside the customer’s organization. The customer and Microsoft may use external/third party sub-processors, share data for a variety of purposes, and transfer data internationally. These factors have important implications for GDPR compliance and are additionally considered here.

| **Title** | **Description** |
| --- | --- |
| **4.7.1 How will you protect any international transfers?**  **(Chapter V of the GDPR)** | Explanation: Please include necessary information from the perspective of the customer depending on the specific geographical location and mode of deployment that is applicable. Microsoft has included information regarding international transfers and location including details on the EU Data Boundary. Configuration instructions for this are set out in the Product Terms under the “Privacy & Security Terms” section.  ***With the development of its EU Data Boundary, Microsoft has significantly reduced transfers outside of the EU and the EFTA. The remaining data transfers are needed to successfully and efficiently provide Microsoft’s products and services globally to Microsoft’s customers and manage the processing and security of Personal Data. Customer and its users may also move, copy, or access their data from any location globally.***  ***As stated in the*** [***DPA***](https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA)***,* for *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 detailed in the section “Location of Customer Data for EU Data Boundary Services” of the Product Terms. For certain services and scenarios, some limited transfers of data outside of the EU Data Boundary have continued. These services and scenarios are further explained here:*** [***What is the EU Data Boundary? - Microsoft Privacy | Microsoft Learn***](https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn)  ***The Microsoft Online Services Subprocessors List (available on the*** [***Service Trust Portal***](https://servicetrust.microsoft.com/DocumentPage/f2cc90fe-471f-4f07-a9ae-af71ebce8486)***) identifies subprocessors authorized to process Customer Data or Personal Data. It represents the locations of personnel across the globe who could potentially access Customer Data and Personal Data.***  ***As stated in the DPA, all transfers of Customer 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. 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.***  Illustrative example:  Based on our review of the Microsoft contract stack and the various commitments within, we are confident that we meet the GDPR requirements as they relate to the transfer of data.  We configured our Microsoft 365 subscription with a sign-up country within the EU/EFTA, so we benefit from Microsoft's EU Data Boundary. The EU Data Boundary is a geographically defined boundary within which Microsoft has committed to store and process Customer Data and Personal Data for Microsoft enterprise online services and to store Professional Services Data for those services. The EU Data Boundary uses or may use Microsoft datacenters announced or currently operating in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Netherlands, Norway, Poland, Spain, Sweden, and Switzerland. There are limited, documented exceptions to the EU Data Boundary that may result in Microsoft processing Customer Data (including Personal Data) and Personal Data outside of Customer Data outside of the EU Data Boundary. Where this is the case, Microsoft relies on compliant data transfer mechanisms as set out in the GDPR. In addition, Microsoft discloses the location of processing personal Data in the Microsoft Online Services Subprocessor List available to customers on the [Service Trust Portal](https://servicetrust.microsoft.com/DocumentPage/f2cc90fe-471f-4f07-a9ae-af71ebce8486) and links to additional information on personnel locations from that list. The contractual, technical and organizational safeguards that Microsoft has implemented and that supplement the Standard Contractual Clauses are explained in the following whitepaper: [Compliance with EU transfer requirements for personal data in the Microsoft Cloud](https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Compliance-with-EU-White-Paper-Final.pdf?culture=en-us&country=us).  As detailed there and in the DPA, and regardless of the location of data, Microsoft makes commitments to restrict any disclosures, including that it will only disclose or provide access to Customer Data, Personal Data, Professional Services Data and customers’ confidential 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. It further commits to 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. And it commits to indemnify our data subjects for any damage to them 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.  The information contained within prompts to Microsoft 365 Copilot and the data they retrieve along with the generated responses remain within our existing Microsoft 365 service boundary. As such use of Microsoft 365 Copilot should not see any data shared with any parties outside of our organization, other than Microsoft and its Subprocessors as per the existing Product Terms and the DPA. Microsoft 365 Copilot uses the Preferred Data Location (PDL) for users and groups to determine where to store data. If the PDL is not set or is invalid, data is stored in the Tenant’s Primary Provisioned Geography location.  For further details on the data residency for Microsoft 365 Copilot, refer to this link: [Data Residency for Microsoft 365 Copilot - Microsoft 365 Enterprise | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/enterprise/m365-dr-workload-copilot?view=o365-worldwide)  For further details on the EU Data Boundary, refer to this link: [What is the EU Data Boundary? - Microsoft Privacy | Microsoft Learn](https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn)  For further details on the current data residency and data residency commitments of Microsoft, refer to this link: [Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide) |

# Step 5: Identify and **assess** risks and **Step 6: Identify measures to reduce risk**

***Explanation:***

***Risk identification, assessment and mitigation are important aspects to the work being done in a DPIA. The assessment must be conducted by the customer and there are many different industry standards that might be helpful to use in implementing this step of a DPIA. Some data protection authorities have released materials and tools to assist organizations in conducting this assessment, which you may find useful in determining the approach to take for assessing the risks involved in your project. The table in the illustrative example below is based on the*** [***Sample DPIA Template of the Data Protection Commission of Ireland***](https://www.dataprotection.ie/sites/default/files/uploads/2024-11/Sample-DPIA-Template-EN.pdf)***, adapted in certain points to align with practical needs. It highlights risk areas and mitigation suggestions, providing a selection of options to consider.***

The information provided here will depend on the specific risks identified. For example, if there is a concern that users may have access to data which they should not access, the mitigation should be ensuring correct permission restrictions. The likelihood and severity of harm will depend on the specific context and is to be assessed on a case-by-case basis.

When considering the risks, you should evaluate the following topics:

* ***The specifics and the deployment context in their environment.***
* ***External processors/companies who will have access to personal data and explain why and how it will be shared/transferred e.g. third-party suppliers (including onsite contractor’s utilities, government departments, councils or any other commercial entity as part of the use of Office 365). Information in relation to Microsoft’s use of third party Subprocessors may be found here in this*** [***Guidance***](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365)and the Product Terms / DPA.
* ***Information about the storage and retention of personal data.***
* Articulate any internal policies with respect to the use of Office 365 in the customer’s organization.

***According to the methodology of such Sample DPIA, please assess and insert into the relevant columns the likelihood of harm ("remote", "possible" or "probable"), the severity of harm ("minimal", "significant" or "severe"), the overall risk ("low", "medium" or "high") and the residual risk ("low", "medium" or "high"). Following the illustrative mitigation area, please insert the effect of the proposed measures on the risk ("eliminated", "reduced" or "accepted"), and whether the measure is approved from your side ("yes" or "no"). You should consider the mitigation steps only if you assess the risk as medium or high.***

Illustrative example:

We understand that security and compliance in the cloud is a [shared responsibility](https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide) and the division of those responsibilities between us as customer and data controller and Microsoft as the cloud service provider and data processor. We evaluated the shared responsibility model, including which security tasks Microsoft, as a cloud service provider and data processor, handles and which tasks we handle. Generally, Microsoft is responsible for managing security and compliance of the cloud as the provider. We remain responsible for managing and configuring security and compliance in the cloud in accordance with our needs and risk tolerance. For further details on the shared responsibility model, refer to this link: [Compliance for Microsoft 365 - Microsoft 365 Enterprise | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/enterprise/essentials-compliance?view=o365-worldwide#shared-responsibility-model).

Microsoft, as a cloud service provider and data processor, provides information, assurance and contractual commitments for controls and measures it operates to manage risks, including:

1. **Contracting** (e.g., Product Terms, the DPA, the SLA)
2. **Assurance Reports**

We have considered this requirement in the context of our contract with Microsoft and are confident that the terms and conditions of the DPA on “Security Practices and Policies” enable us to meet this obligation under the GDPR as follows:

* 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 us, along with other information reasonably requested by us 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. For further details on ISO/IEC 27701, please refer to [ISO/IEC 27701:2019 Privacy Information Management - Microsoft Compliance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-27701)
* A description of the security controls for these requirements is available to us. For further details on the Microsoft managed controls, refer to this overview: [Risk Assessment Guide for Microsoft Cloud - Microsoft Service Assurance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide)
* Each Core Online Service also complies with the control standards and frameworks shown in the table in the Product Terms.

1. **Descriptive Information (e.g. whitepapers, learning resources)** – we referred to the relevant information reviewed throughout the DPIA and its Annex.
2. **Interactive Information (e.g. audit logs, graphs, messages)** – we referred to the relevant information reviewed throughout the DPIA.

As a cloud service customer and data controller, we are responsible for:

1. **Compliance Requirements**, such as internal policies, adherence to applicable laws (primarily the GDPR and, if applicable, the UK GDPR), and security standards we apply (e.g. ISO 27002).
2. **Risk Assessments,** including conducting this DPIA, security risk assessments, and **compliance**/legal assessments.
3. Implementation of **additional technical and organizational measures** managed by us. This may include: (i) using security defaults (i.e. pre-configured security settings that provide a right level of protection for users and accounts, such as multi-factor authentication, also known as two-step verification); (ii) setting up and protecting our administrator accounts; (iii) using preset security policies to protect email and collaboration content; (iv) protecting the devices civil servants use to access our data; (v) training everyone on email best practices (i.e. protecting ourselves against phishing and other attacks, spam or junk mail, spoofing, and malware); (vi) providing a secure environment for files and folders in the context of collaboration and sharing; and (vii) implementing data governance policies and procedures. For further suggestions, refer to this link: [Accountability readiness checklist for the GDPR - Microsoft GDPR | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-arc-office365)
4. **Ongoing verification** of the above responsibilities.

The requirements applicable to Microsoft as a data processor and to us as a data controller form part of our shared responsibility and are subject to continuous evaluation.

Considering the above, the data protection risks associated with using Microsoft 365 Copilot and the related mitigation measures, based on the described use case, include the following:

| **Describe the source of risk and nature of potential impact on individuals: where appropriate, include associated compliance and public sector risks.** | **Likelihood of harm** | **Severity of harm** | **Risk** |
| --- | --- | --- | --- |
| **Risk area for consideration:**  ***Explanation: The examples below highlight risk areas for consideration.***  **Data breach notification**  **Source of risk:** data breaches and insider threats arise from unauthorized access due to security vulnerabilities, misconfigurations, malicious attacks, or misuse of access rights by civil servants or contractors. For example, an unauthorized access incident, or a misconfigured database could expose citizens' records.  **Nature of potential impact on individuals:** data protection violations leading to identity theft or fraud, financial loss from compromised details, reputational damage to public sector services due to loss of trust, and emotional distress caused by uncertainty over data misuse. For instance, a breach involving citizen records’ details could lead to identity fraud and might undermine public confidence.  **Associated compliance and public sector risks:** non-compliance with GDPR can result in regulatory penalties of up to 4% of annual turnover, litigation risks from data subject claims, and operational disruptions due to resource-intensive incident response and remediation efforts. For example, failure to notify affected individuals of a breach could trigger damage to public trust.  **Mitigation area for consideration:**  ***Explanation: Consider the mitigation steps only if the risk is assessed as medium or high.***  We have considered the above and are confident that Microsoft 365 will ensure that we are able to meet the data breach notification requirements as data controllers. In particular, Microsoft is providing us with an ability to specify a dedicated privacy contact who will be notified in the event of a breach. We can specify this contact using the Privacy reader role settings for Message Center. In addition, Microsoft will notify us of a personal data breach within 72 hours of a breach being declared. Notifications will be published to the Message Center. Secondarily, email notifications are sent to specified contacts indicating a new Message Center post has been published. In addition, Microsoft 365 enforces a zero-standing access policy, granting engineers temporary, least-privilege access only when necessary, with strict role separation to minimize unauthorized data access. Security monitoring systems detect and respond to illicit access attempts, maintain detailed records of elevation requests, and conduct red-team penetration tests to enhance defenses. Additionally, civil servants and processes ensure security awareness, incident response readiness, and compliance through a Standard Operating Procedure (SOP), ongoing training, and centralized breach management protocols. The following link contains further information on the mitigation measures: [Office 365 Breach Notification Under the GDPR - Microsoft GDPR | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365) |  |  |  |
| **Risk area for consideration:**  ***Explanation: The examples below highlight risk areas for consideration.***  **Access control (external threats)**  **Source of risk:** external actors may exploit vulnerabilities, such as phishing, brute-force attacks, or password reuse. Threats may also arise from misconfigured identity federation, improper single sign-on (SSO) settings, or excessive administrative privileges that are accessible through external compromise. For example, a successful phishing attack targeting a public sector portal could allow attackers to manipulate contract awards, or delayed deactivation of a former civil servant’s credentials could lead to unauthorized access to citizen records.  **Nature of potential impact on individuals:** external compromise of public sector systems - such as through phishing or credential theft - could lead to the unauthorized exposure of public sector data, identity fraud, financial loss, legal consequences, and a loss of public trust in digital services. For instance, if an attacker gains control of a civil servant’s compromised account and alters citizen records, the affected individuals may face incorrect liabilities, or become victims of fraudulent claims filed in their name.  **Associated compliance and public sector risks:** external compromise - such as through unauthorized access by attackers - may lead to regulatory penalties, operational disruptions, and contractual risks, potentially affecting compliance, service continuity, and public sector procurement eligibility. For example, a failure to secure privileged access in a citizen data registry could lead to GDPR fines, while an external breach exploiting weak access control measures might result in the loss of security clearance.  **Mitigation area for consideration:**  ***Explanation: Consider the mitigation steps only if the risk is assessed as medium or high.***  We have considered the above in the context of our use of Microsoft 365 Copilot and are confident that Microsoft provides for identity and access management (IAM) strategies to mitigate the above security risks. For example, Microsoft Entra ID provides a full suite of identity management and security capabilities against identity-based attacks. Multifactor authentication (MFA) requires our users to provide two forms of verification, such as a user password plus a notification from the Microsoft Authenticator app or a phone call. Microsoft Entra ID evaluates the conditions of the user sign-in and uses Conditional Access policies to determine the allowed access. Conditional Access policies, device management with Intune, and even permissions to files and sites in our organization rely on the assignment to user accounts or Microsoft Entra groups. Microsoft Entra ID Protection enables us to detect potential vulnerabilities affecting our organization's identities and configure automated remediation policy. Self-service password reset (SSPR) allows our users to reset their passwords securely and without help-desk intervention, by providing verification of multiple authentication methods that the administrator can control. Microsoft Entra password protection detects and blocks known weak passwords and their variants and additional weak terms that are specific to our organization. Additional access controls cover the following categories: guest access, user management, information classification, user segmentation, and data residency. The following links contain further information on the mitigation measures: [Deploy your identity infrastructure for Microsoft 365 - Microsoft 365 Enterprise | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/enterprise/deploy-identity-solution-overview?view=o365-worldwide) and [Governing access in Microsoft 365 groups, Teams, and SharePoint | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/solutions/groups-teams-access-governance?view=o365-worldwide)  In addition to the above, we also considered that Microsoft Purview Customer Lockbox ensures that Microsoft cannot access our content in Exchange Online, SharePoint, OneDrive, and Teams to do service operations without our explicit approval. Global administrators and anyone assigned the Customer Lockbox access approver admin role are notified when there is a request to access our content. These are also the same users who can approve Customer Lockbox requests. Global administrators and anyone assigned the Customer Lockbox access approver admin role can approve Customer Lockbox requests. We control these role assignments in our organization. The following article contains further information on the Microsoft Purview Customer Lockbox: [Customer Lockbox requests | Microsoft Learn](https://learn.microsoft.com/en-us/purview/customer-lockbox-requests) |  |  |  |
| **Risk area for consideration:**  ***Explanation: The examples below highlight risk areas for consideration.***  **Access control (unintended internal access)**  **Source of risk:** insufficiently configured access controls may lead to users unintentionally accessing information beyond their authorization. This can occur due to system misconfigurations, overly broad permissions, or unanticipated outputs generated by Microsoft 365 Copilot, which may surface personal data outside of intended access boundaries.  **Nature of potential impact on individuals:** improper internal access control may result in the unintended disclosure of personal data to unauthorized personnel. This can lead to personal data breaches, reputational harm, emotional distress, or misuse of personal data - particularly if the information is used in decision-making without proper context.  **Associated compliance and public sector risks:** failures in internal access control can result in non-compliance with the GDPR, potentially leading to regulatory investigations, fines, and enforcement actions. In the public sector, these risks may also disrupt service delivery, damage institutional credibility and reduce public confidence in digital services.  **Mitigation area for consideration:**  ***Explanation: Consider the mitigation steps only if the risk is assessed as medium or high.***  We will ensure that appropriate access controls are in place and maintained throughout the use of Microsoft 365 Copilot. This includes enforcing role-based access, applying the principle of least privilege, and conducting regular access reviews. Technical safeguards - such as audit logging and privileged access monitoring - should be complemented by organizational measures like user training on the responsible use of Microsoft 365 Copilot. We will also establish controls to validate the outputs generated by Microsoft 365 Copilot and prevent unintended exposure of personal data. Based on our assessment, we also confirm that Microsoft 365 Copilot attained the ISO/IEC 42001:2023 certification. ISO/IEC 42001 is an internationally recognized Artificial Intelligence Management System (AIMS) standard that provides a framework for organizations to develop, deploy, and use AI systems responsibly. For more information, refer to this announcement: [Microsoft 365 Copilot Achieves ISO/IEC 42001:2023 Certification | Microsoft Community Hub](https://techcommunity.microsoft.com/blog/microsoft365copilotblog/microsoft-365-copilot-achieves-isoiec-420012023-certification/4397144) |  |  |  |
| **Risk area for consideration:**  ***Explanation: The examples below highlight risk areas for consideration.***  **Business continuity**  **Source of risk:** service continuity failures, operational vulnerabilities and communication failures can disrupt services, hinder data recovery, expose critical functions to errors, and cause confusion or reputational damage due to inadequate planning, untested recovery protocols, or poor crisis communication. For example, an untested disaster recovery plan could delay access to citizen records during an IT outage, or a misconfigured backup system could lead to the loss of critical citizen data needed for audits.  **Nature of potential impact on individuals:** disrupted access to public services, data loss, persistent service disruptions, and unclear communication during crises can lead to inconvenience, erode trust in the public sector, and cause emotional distress among affected individuals. For instance, if a personal data breach on our side is improperly communicated, affected individuals may struggle to mitigate identity theft risks.  **Associated compliance and public sector risks:** regulatory non-compliance, fines, operational downtime, financial loss, and reputational damage. For example, a prolonged IT failure in our system could disrupt our official proceedings, leading to legal challenges and public scrutiny.  **Mitigation area for consideration:**  ***Explanation: Consider the mitigation steps only if the risk is assessed as medium or high.***  First, we complete a Business Impact Assessment (BIA), where each function in our organization and the services and processes that support them is ranked according to how critical it is, and we identify the processes and services that each one depends on. Next, we look across processes to see where any cascading dependency relationships exist. Based on our Dependency Analysis (DA), we prioritize and form resiliency strategies, and standard operating procedures supporting our strategies. We have considered the above in the context of our use of Microsoft 365 Copilot and we can use [Microsoft Service Map](https://learn.microsoft.com/en-us/azure/azure-monitor/insights/service-map) to help us in with this mapping. Once we have reviewed our service processes and mapped out relationships to other processes and technologies, we build validation scenarios for all the processes. During a service incident, normal communications channels may be impacted or degraded, so we prearrange alternatives to help our organization stay connected during an incident. We also considered external communications in the same way as internal communications. The following article provides guidance on developing a business continuity plan, including a Sample Business Impact Assessment (BIA), a sample Dependency Analysis (DA), and methods for analyzing our functions and identifying the ones that depend on Microsoft 365: [Considerations for your Enterprise Business Continuity Management Plan - Microsoft Service Assurance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/assurance/assurance-developing-your-ebcm-plan?view=o365-worldwide)  We have also considered the above in the context of our contract with Microsoft and are confident that the terms and conditions of Appendix A – Security Measures of the DPA on “Business Continuity Management” provide for adequate risk mitigation. Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data or Professional Services Data are located. In addition, 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. |  |  |  |
| **Risk area for consideration:**  ***Explanation: The examples below highlight risk areas for consideration.***  **Prepare for audit and monitoring**  **Source of risk:** limited audit logging and real-time monitoring can prevent timely detection of security incidents, making it difficult to trace unauthorized access or insider threats. In addition, inadequate audit controls and gaps in forensic records may delay response efforts, increasing the risk of data breaches and compliance violations. For example, if we lack sufficient logging, fraudulent access to citizens' records may go undetected.  **Nature of potential impact on individuals:** insufficient audit logging can lead to undetected data breaches, exposing personal data to unauthorized access and increasing the risk of financial fraud or identity theft. Repeated security failures and lack of accountability may erode public trust and result in legal or administrative consequences. For instance, if our system is breached without proper audit trails, citizens may not be able to identify fraud without clear evidence of the breach.  **Associated compliance and public sector risks:** incomplete or missing audit logs can result in regulatory violations, financial penalties, and legal disputes, particularly under GDPR and other data protection laws. Additionally, inadequate audit controls can delay incident response, harm an organization's reputation, and lead to operational inefficiencies. For example, without proper audit trails, our systems could be vulnerable, leading to regulatory investigations and loss of public trust.  **Mitigation area for consideration:**  ***Explanation: Consider the mitigation steps only if the risk is assessed as medium or high.***  We considered that Microsoft service records include data such as user activities, exceptions, faults, and information security events, with guidance on accessing these logs for record-keeping purposes. Relevant documentation includes instructions on searching the audit log in the Office 365 Security and Compliance Center. Search in Microsoft Purview Audit (Standard) and Audit (Premium) give(s) our organization access to critical audit log event data to gain insight and further investigate user activities. The following article contains further information on “Search the audit log in Office 365 Security and Compliance Center“: [Search the audit log | Microsoft Learn](https://learn.microsoft.com/en-us/purview/audit-search?tabs=microsoft-purview-portal). We can also use the Office 365 Management Activity API to retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra activity logs: [Office 365 Management Activity API reference | Microsoft Learn](https://learn.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-reference). Microsoft Purview eDiscovery can be used to identify, review, and manage content in Office 365 to support our investigations, as described in more detail at the following link: [Learn about eDiscovery solutions | Microsoft Learn](https://learn.microsoft.com/en-us/purview/edisc). The following links contain further information on auditing solutions: [Get started with auditing solutions | Microsoft Learn](https://learn.microsoft.com/en-us/purview/audit-get-started) |  |  |  |
| **Risk area for consideration:**  ***Explanation: The examples below highlight risk areas for consideration.***  **Cloud policy enforcement**  **Source of risk:** inconsistent cloud policies, lack of granular access controls, and inadequate monitoring can lead to unauthorized data access, accidental sharing, or delayed breach detection, increasing the risk of compromised data integrity and security. For example, if we fail to restrict document sharing, confidential policy drafts or citizen data may be exposed.  **Nature of potential impact on individuals:** unauthorized access or exposure of personal data due to misconfigured cloud policies can lead to privacy violations, financial loss, emotional distress, and legal consequences for individuals affected. For instance, if a misconfigured cloud storage policy may result in unauthorized access to citizens' records, and individuals may face identity theft or fraudulent claims using stolen personal details.  **Associated compliance and public sector risks:** non-compliance with data protection regulations, reputational damage, operational disruptions, and contractual or legal liabilities can result from improperly configured cloud policies, potentially leading to fines and security incidents. For example, storing citizen records in a non-compliant cloud service or using improperly secured cloud-based collaboration tools may result in GDPR fines.  **Mitigation area for consideration:**  ***Explanation: Consider the mitigation steps only if the risk is assessed as medium or high.***  We have considered the above in the context of our use of Microsoft 365 Copilot and are confident that Microsoft provides for a Cloud Policy to mitigate the above security risks. The following article provides guidance on the steps for creating a policy configuration, managing policy configurations, and how the policy configuration is applied: [Overview of Cloud Policy service for Microsoft 365 - Microsoft 365 Apps | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365-apps/admin-center/overview-cloud-policy) |  |  |  |
| **Risk area for consideration:**  ***Explanation: The examples below highlight risk areas for consideration.***  **Data governance**  **Source of risk:** system failures, disasters, unauthorized data sharing, user error, and a lack of real-time monitoring, along with improperly configured Data Loss Prevention (DLP) policies, can lead to inadvertent data leaks, data loss or destruction, delayed detection, and escalating security incidents. For example, a misconfigured DLP policy could allow unauthorized sharing of citizen records or a system failure in our database could result in lost citizen records.  **Nature of potential impact on individuals:** if data is lost or destroyed without proper recovery, individuals may face risks related to the unavailability of their personal or professional data, affecting privacy, access to services, or continuity of operations. For instance, if our database suffers a failure and loses citizen records, affected individuals may be unable to prove eligibility for certain benefits.  **Associated compliance and public sector risks:** non-compliance with data protection regulations, reputational harm from repeated breaches, operational disruptions, and legal or contractual risks can result in significant fines, loss of trust, and potential legal actions. For example, failing to prevent data loss in our system due to weak DLP controls may result in regulatory penalties under the GDPR for not ensuring data availability, and undermine public confidence in the judicial process.  **Mitigation area for consideration:**  ***Explanation: Consider the mitigation steps only if the risk is assessed as medium or high.***  We have considered the above in the context of our use of Microsoft 365 Copilot and are confident that DLP measures protect personal data from unauthorized access, sharing, and accidental exposure. In Microsoft Purview, we can implement data loss prevention by defining and applying DLP policies. With a DLP policy, we can identify, monitor, and automatically protect sensitive items across Office applications such as Word, Excel, and PowerPoint. The following article contains further information on the use of DLP: [Learn about data loss prevention | Microsoft Learn](https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp) |  |  |  |

# Step 6: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| Item | Name/date | Notes |
| Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion. |
| Residual risks approved by: |  | If accepting any residual high risk, consult the competent data protection supervisory authority before going ahead. |
| DPO advice provided: |  | DPO should advise on compliance and whether processing can proceed. |
| Summary of DPO advice: | | |
| DPO advice accepted by or overruled by: |  | If overruled, you must explain your reasons. |
| Comments | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals' views, you must explain your reasons. |
| Comments: | | |
| This DPIA will be kept under review by: |  | The DPO should also review ongoing compliance with DPIA. |

# Annex 1

**Helpful Microsoft Links**

***Explanation: It is important to note when a customer renews or purchases a new subscription to an Online Service, the then-current underlying documentation and information for that service will apply, and it is the customer’s sole responsibility to ensure that the most up to date documentation and information is relied on in the creation of a DPIA. If a customer uses the same DPIA template year over year, it can be important that supporting documentation is also validated and critical privacy impacting documentation, as well as the customer’s service configurations, use of privacy controls and use of the service in general are reviewed for impact.***

***Listed and hyperlinked below are Microsoft documents and resources that would typically be relevant for the purposes of completing a DPIA. These links and the information contained in them are subject to change.***

**GENERAL RESOURCES**

[Microsoft Product Terms](https://www.microsoft.com/licensing/terms/welcome/welcomepage)

[Microsoft Products and Services Data Protection Addendum (DPA)](https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA)

[Cloud Data Integrity and Compliance | Microsoft Trust Center](https://www.microsoft.com/en-us/trust-center/)

[Service Trust Portal](https://servicetrust.microsoft.com/)

[Microsoft 365 Roadmap | Microsoft 365](https://www.microsoft.com/en-us/microsoft-365/roadmap?msockid=24f275b6e9bf67382c73664de8876661)

[General Data Protection Regulation - Microsoft GDPR](https://learn.microsoft.com/en-gb/compliance/regulatory/gdpr)

[Guidance for Data Controllers using Office 365 - Microsoft GDPR](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365)

[Office 365 Data Subject Requests Under the GDPR and CCPA - Microsoft GDPR](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365)

[Overview of privacy controls for Microsoft 365 Apps for enterprise - Microsoft 365 Apps | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/overview-privacy-controls)

[Compliance for Microsoft 365 - Microsoft 365 Enterprise | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/enterprise/essentials-compliance?view=o365-worldwide)

[GDPR and Generative AI: A Guide for Public Sector Organizations](https://wwps.microsoft.com/blog/gdpr-genai)

[What is Microsoft 365 Copilot? | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-overview)

[Microsoft 365 Copilot – Microsoft Adoption](https://adoption.microsoft.com/en-us/copilot/)

[Microsoft 365 Copilot documentation | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/?ocid=CopilotLab_SMC_Resources_Admin)

[Microsoft Responsible AI Transparency Report | Microsoft CSR](https://www.microsoft.com/en-us/corporate-responsibility/responsible-ai-transparency-report?msockid=088cf58b8cb2676b179de1368d0166b1)

**SPECIFIC RESOURCES**

| **GDPR** | **Subject** | **Microsoft response/resource** |
| --- | --- | --- |
| Art 5.2 | Accountability | DPA (appendices!) | Accountability Readiness Checklists: [Accountability readiness checklists for the GDPR - Microsoft GDPR | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-arc)  Additional assurance: ISO 27701 - [ISO/IEC 27701:2019 Privacy Information Management - Microsoft Compliance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-27701)  Additional assurance: EU Cloud CoC - [EU Cloud Code of Conduct - Azure Compliance | Microsoft Learn](https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-eu-cloud-coc)  Learning: [Understand Microsoft 365 privacy - Training | Microsoft Learn](https://learn.microsoft.com/en-us/training/modules/audit-privacy/)  Data, Privacy, and Security for Microsoft 365 Copilot - [Data, privacy, and security for web search in Microsoft 365 Copilot and Microsoft 365 Copilot Chat | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/manage-public-web-access) and [Data, Privacy, and Security for Microsoft 365 Copilot | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy?source=recommendations)  Transparency: [Transparency Note for Microsoft 365 Copilot | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-transparency-note) |
| Art 32 | Security, appropriate measures | DPA – Appendix A, SOC2 Reports, ISO certifications: [Service Trust Portal Home Page](https://servicetrust.microsoft.com/)  Customer Lockbox – customer control over Microsoft’s access to Customer Data contents (where the customer's most sensitive data is stored) in M365 primary storage repositories: [Customer Lockbox requests | Microsoft Learn](https://learn.microsoft.com/en-us/purview/customer-lockbox-requests)  Purview Data Security Solutions – [Microsoft Purview data security solutions | Microsoft Learn](https://learn.microsoft.com/en-us/purview/purview-security)  Audit Logging – enables customers to monitor activities within their tenant: [Audit log activities | Microsoft Learn](https://learn.microsoft.com/en-us/purview/audit-log-activities) Through audit logs, the customer can determine whether Microsoft accessed customer-owned storage repositories (e.g. OneDrive) ex post, even if the customer does not choose to purchase and configure Customer Lockbox to control access ex ante. The customer can then reach out for more information about an access event if necessary.  Management Activity API: [Office 365 Management Activity API schema | Microsoft Learn](https://learn.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema)  Security, Oversharing Controls, and Data Storage in Microsoft 365 Copilot: [Microsoft 365 Copilot data protection architecture | Microsoft Learn](https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data-protection-auditing) |
| Art 28.3(a) | Documented instructions | Customer agreement (incl. DPA), product documentation and customer’s use and configuration  [Audit logs for Copilot and AI activities | Microsoft Learn](https://learn.microsoft.com/en-us/purview/audit-copilot) |
| Art 28.3(a) | Data residency | DPA + Product Privacy & Security Terms: [Microsoft Product Terms](https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all)  EU DB documentation: [Microsoft EU Data Boundary Overview | Microsoft Trust Center](https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb)  M365 Data Residency documentation: [Overview and Definitions - Microsoft 365 Enterprise | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/enterprise/m365-dr-overview?view=o365-worldwide) |
| Art 28.3(e) | Data Subject Rights (DSR) | DPA + DSR tooling: [Data Subject Requests for the GDPR and CCPA - Microsoft GDPR | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-data-subject-requests)  Data Retention[:](file://C:\Users\towyrwic\AppData\Local\Microsoft\Olk\Attachments\ooa-51aabde9-6773-456e-873b-dbbf1b430b31\8d18880eb94aceab69dcbb43d87912f512542728ec1d55faebae817dd21879f9\%20https\learn.microsoft.com\en-us\compliance\assurance\assurance-data-retention-deletion-and-destruction-overview) [Data retention, deletion, and destruction in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview) and [Learn about retention policies & labels to retain or delete | Microsoft Learn](https://learn.microsoft.com/en-us/purview/retention?tabs=table-overriden).  Overview of Microsoft Teams Export APIs, including Microsoft 365 Copilot activities (Preview): [Export content with the Microsoft Teams Export APIs - Microsoft Teams | Microsoft Learn](https://learn.microsoft.com/en-us/microsoftteams/export-teams-content)  Managing and Deleting Microsoft 365 Copilot Activity History: [Delete your Microsoft 365 Copilot activity history - Microsoft Support](https://support.microsoft.com/en-us/office/delete-your-microsoft-365-copilot-activity-history-76de8afa-5eaf-43b0-bda8-0076d6e0390f)  Retention for Copilot & AI apps: [Learn about retention for Copilot and AI apps | Microsoft Learn](https://learn.microsoft.com/en-us/purview/retention-policies-copilot#how-retention-works-with-ai-apps)  Feedback:  [Providing feedback about Microsoft Copilot with Microsoft 365 apps - Microsoft Support](https://support.microsoft.com/en-us/topic/providing-feedback-about-microsoft-copilot-with-microsoft-365-apps-c481c26a-e01a-4be3-bdd0-aee0b0b2a423)  [Manage Microsoft feedback for your organization - Microsoft 365 admin | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-feedback-ms-org?view=o365-worldwide)  [Learn about Microsoft feedback for your organization - Microsoft 365 admin | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/admin/misc/feedback-user-control?view=o365-worldwide)  Deletion: [Search for and delete Copilot data | Microsoft Learn](https://learn.microsoft.com/en-us/purview/ediscovery-search-and-delete-copilot-data). |
| Art 35 | Data Protection Impact Assessments (DPIA) | Risk assessment guide: [Risk Assessment Guide for Microsoft Cloud - Microsoft Service Assurance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide)  DPIA documentation and templates: [Data protection impact assessments - Microsoft GDPR | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-data-protection-impact-assessments) |
| Art 33 | Personal data breach notification | DPA + documentation here: [Breach Notification - Microsoft GDPR | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification)  Message Center Privacy Reader Role – ensures that privacy-related incident notifications are routed to the appropriate person(s) in the customer's organization: [Message center in the Microsoft 365 admin center - Microsoft 365 admin | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/admin/manage/message-center?view=o365-worldwide) |
| Art 28.4 | Subprocessing | Supplier & subprocessor management: [Supplier management overview - Microsoft Service Assurance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/assurance/assurance-supplier-management)  SSPA: [Supplier Security and Privacy Assurance Program - Microsoft Service Assurance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/assurance/assurance-supplier-security-and-privacy-assurance-program)  Subprocessor list: [Service Trust Portal](https://servicetrust.microsoft.com/DocumentPage/f2cc90fe-471f-4f07-a9ae-af71ebce8486) |
| Art 44 (Chapter V) | Data transfers | Microsoft 365 Data Locations: [Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide)  Data Residency: [Data Residency for Microsoft 365 Copilot - Microsoft 365 Enterprise | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/enterprise/m365-dr-workload-copilot?view=o365-worldwide)  EU Data Boundary: [What is the EU Data Boundary? - Microsoft Privacy | Microsoft Learn](https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn)  Data Transfer Whitepaper: [Compliance with EU transfer requirements for personal data in the Microsoft Cloud](https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Compliance-with-EU-White-Paper-Final.pdf?culture=en-us&country=us)  Standard Contractual Clauses: [Service Trust Portal](https://servicetrust.microsoft.com/DocumentPage/d4e2c91a-1c8f-40f6-a1ae-432f5dc2d6f5) |

1. The illustrative examples and explanations in this DPIA are written in the first-person plural (“you”). The potential examples should be customized and specified by the customer based on their specific use case. [↑](#footnote-ref-2)