**BUILD YOUR OWN DPIA**

**FOR**

**OFFICE 365**

**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 Office 365. 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 Office 365.

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 Office 365, 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 Office 365 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 [Product Terms](https://www.microsoft.com/licensing/terms/welcome/welcomepage) and [Data Protection Addendum](https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA) (“**DPA**”) and explains how Office 365 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 learn.microsoft.com for M365 which contains details about the product family in which Office 365 belongs, can be found in Annex 1.

**Contents**

[**Introduction** 1](#_Toc195550470)

[**Step 1: Identify the need for a DPIA** 3](#_Toc195550471)

[**Step 2: Describe the processing** 7](#_Toc195550472)

[**Step 3: Consultation process** 16](#_Toc195550473)

[**Step 4: Assess necessity and proportionality** 17](#_Toc195550474)

[4.1 Lawfulness, Fairness and Transparency 17](#_Toc195550475)

[4.2 Purpose Limitation 20](#_Toc195550476)

[4.3 Data Accuracy and Data Minimization 22](#_Toc195550477)

[4.4 The information that will be made available to individuals 22](#_Toc195550478)

[4.5 Data Subject Rights 23](#_Toc195550479)

[4.6 Processor Compliance 25](#_Toc195550480)

[4.7 International Transfers 25](#_Toc195550481)

[**Step 5: Identify and assess risksand Step 6: Identify measures to reduce risk** 28](#_Toc195550482)

[**Step 7: Sign off and record outcomes** 37](#_Toc195550483)

[**Annex****1** 39](#_Toc195550484)

# **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 procure Office 365 to improve internal communication, document management, and collaboration across departments and administrative functions. Office 365 would facilitate secure email communication, virtual meetings, and electronic record management. As part of Office 365, we may use Microsoft Teams and Outlook for communication between civil servants, while SharePoint and OneDrive will be used to store and manage records, files, and other documents. Microsoft Purview and Defender are to be employed to monitor user activity, file access, and system events to detect any potential breaches or misuse of personal data. |
| **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 Office 365 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 Office 365, potentially introducing new categories of data or processing purposes.*** * ***Situations where the customer’s intended specific use of an Office 365 application significantly diverges from the contents of the DPIA.*** * ***Expanding data processing to include new geographic regions.*** * ***Significant changes in the 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 software 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 Office 365, except for a limited number of optional connected experiences designed to enable our ability to create, communicate, and collaborate more effectively. Working with others on a document stored on OneDrive or translating the contents of a Word document into a different language are examples of connected experiences.  Optional connected experiences are available for use through Office 365 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. For further details on optional connected experiences in O365, 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)  This DPIA does not cover the optional connected experiences. |
| **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 Office 365. 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 or personal data in Office 365.  Since Office 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 Office 365. 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 Office 365 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 Office 365 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: Office 365 is a cloud-based productivity suite that enables the integration of various tools for communication, collaboration, and workflow management. Applications like Word, Excel, PowerPoint, and Outlook, along with cloud services such as OneDrive for file storage and SharePoint for document sharing allow users to manage data and collaborate in real-time. Additionally, Teams facilitates virtual meetings and group communication, while Exchange Online powers email services. Security features, such as data loss prevention and encryption, ensure that user data is protected during storage and transmission. It operates on a subscription model, accessible from various devices, ensuring seamless work across platforms. For further details on how Office 365 operates, see [here](https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-service-descriptions-technet-library).  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 Office 365, data processing refers to the collection, storage, sharing, and analysis of personal data as part of the suite’s core functionalities. For example, when using Teams for virtual meetings, personal data such as usernames, meeting participation data, and chat messages are processed. Similarly, when documents are created in Word or stored on OneDrive, the content, including potentially personal data (e.g. civil servant names, job titles, or customer details), is processed for purposes of editing, storage, and collaboration.  The key aspects of the data processing are the following:  Collection: personal data may be collected when civil servants interact with Office 365 tools, such as entering personal contact information in Outlook or creating shared documents in SharePoint.  Storage: Office 365 stores personal data across its cloud services, with security protocols in place.  Sharing: data may be shared among users within our organization, or with third parties (e.g. collaborators or external stakeholders) depending on the specific Office 365 service used. For example, SharePoint allows document sharing, while Teams facilitates collaboration on group chats or video calls.  Analysis: tools like Excel enable analysis of aggregated data, such as project performance.  The aim of using Office 365 is to enhance productivity, collaboration, and communication within our organization and for individuals. It provides tools for efficient communication, document creation, data analysis, and project management, while enabling teamwork through real-time collaboration and virtual interaction. Office 365 also ensures accessibility across devices and supports remote and hybrid work models. Ultimately, it helps streamline workflows and improve efficiency. |
| **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 Office 365. 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 Office 365 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 Office 365 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.   1. **Data that may be generated, derived or collected by Microsoft in connection with providing Office 365 include the following data that Microsoft comes into the possession of as Office 365 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 Office 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 Office 365. Certain diagnostic data is required, while some diagnostic data is optional. Required diagnostic data is the minimum data necessary to help keep Office 365 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. 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 article contains 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)  **Personal data in system-generated logs:** Office 365 creates 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 Office 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.   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 Office 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 Office 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 Office 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?**  Microsoft has outlined in Appendix B of the [DPA](https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA) a list to provide additional detail and transparency around the various categories of data that Microsoft may process in connection with Office 365. This list features personal data that is included in e-mail, documents and other data in an electronic form in the context of Office 365, 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 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 Office 365.  Depending on our use of Office 365 as a customer and a data controller, we may elect to include personal data from any of the following categories in the personal data:   * Civil servant and citizen correspondence: emails in Exchange Online containing inquiries, complaints, service requests or feedback from citizens. * Documents or files stored or shared in SharePoint Online or OneDrive for Business: budget planning, financial reports, case management files, project coordination materials, and official documents. * Meetings, conversations and chats: civil servant discussions and decision-making records captured in Teams. * Community and channel posts: comments and feedback from citizens posted in Teams community channels. * Chats. * Voicemails, recordings, transcriptions and call history of citizen interactions processed in Exchange Online and Teams.   **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). |
| **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 Office 365. 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 references.***  Illustrative example:  **Data subjects**:  The data subjects whose personal data may be processed in 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 Office 365 accounts): Office 365 is a productivity tool provided to civil servants for work-related communication and collaboration. Civil servants' data is processed to facilitate workflows, meetings, and document sharing.  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. |
| **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 Office 365.  Illustrative example:  Office 365 is a comprehensive cloud-based suite of applications and services designed to enhance productivity, communication, and collaboration. As part of its functionalities, Office 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, PowerPoint, Project, SharePoint, Stream, Sway, Teams, To Do, Visio, Viva Engage, Viva Insights, Whiteboard, and Word) in accordance with the applicable licensing arrangement.  Office 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 Office 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, Office 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 Office 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**: Office 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.   Office 365 is designed to support productivity, communication, and collaboration without inherently involving high-risk processing activities. While Office 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: Office 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. * Office 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 Office 365 applications, including editing, deleting, and restricting access to shared files. * Office 365 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** | 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:  The retention of data within Office 365 is customizable, ensuring that we have control over how long our Customer Data are stored. We can define our own retention policies based on our specific service, legal, and compliance requirements. 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 Office 365. |

# **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 Office 365 aligns with their statutory functions while respecting the rights and freedoms of data subjects. Establishing a legal basis ensures 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 Office 365 is used for a specific purpose. Often, Office 365 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:  Office 365 is a core service technology at our organization essential for delivering our statutory functions, consisting of a suite of software applications and services (e.g. Word, Excel, Teams, SharePoint) used to facilitate various tasks including communication, collaboration, and document management.  For example:  **Communications**: using Teams for messaging and video calls.  **Document management**: storing and sharing files in OneDrive or SharePoint.  **Task management**: using Planner or To Do to organize work tasks.  **Analytics**: if analytics tools (like Viva Insights) are used to track civil servant productivity.  In other words, Office 365 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 Office 365 in accordance with our documented instructions and (b) for business operations incident to providing Office 365 to us. Providing a cloud service requires the cloud service provider to compute, transmit and store data to provide the service, keep the product secure, up to date and performing as expected. 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 Office 365 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 Office 365 supports these functions by enabling communication, collaboration, and secure information management. Whether facilitating engagement with citizens, coordinating inter-agency collaboration, or ensuring efficient service delivery, our use of Office 365 is aligned with our official duties.  For civil servants, the data processing is based on their contractual relationship with us. We provide Office 365 as a necessary tool for fulfilling job responsibilities (Article 6(1)(b) of the GDPR). Thus, while both legal bases permit data processing within Office 365, 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 Office 365 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 Office 365 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 content of Word files may be pseudonymized, the Customer Data- such as the properties of a document, e.g. identification of the document's owner, labels etc. - remains linked to the user and therefore constitutes directly identifiable personal data.  However, there are no other less intrusive means to achieve the same outcomes as Office 365, considering the following factors:   * Office 365 provides a unified suite of tools, such as Word, Excel, PowerPoint, Outlook, Teams, OneDrive and SharePoint, designed to work seamlessly together. This integration allows for efficient document creation, real-time collaboration, communication, and data storage. Achieving the same level of functionality with separate, non-integrated tools would likely require multiple platforms, each processing data independently, leading to more fragmented systems that may ultimately process more personal data across different services. * Features like real-time document editing and collaboration in Teams, along with file sharing through OneDrive and SharePoint, rely on cloud-based infrastructure and data exchange between users. Achieving the same level of real-time collaboration without processing personal data would require either highly restrictive data policies or the use of more limited, less efficient alternatives that do not support the same workflows. * Office 365’s cloud infrastructure enables high levels of data security, redundancy, and scalability, which are difficult to replicate with alternative, on-premises solutions. The security features in Office 365, such as encryption, data loss prevention, and compliance certifications, minimize risks associated with personal data processing and ensure data protection standards are met. Using alternative, less intrusive tools would likely involve additional manual processes to ensure security and compliance, potentially increasing the overall risk and burden. * Office 365 provides organizations with extensive control over personal data processing, allowing them to configure settings, disable non-essential features, and manage data retention policies. While less intrusive alternatives might reduce the amount of personal data processed, they would likely lack the same flexibility, requiring significant manual interventions to control and protect data in ways that Office 365 automates and optimizes. |

## 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 Office 365 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 Office 365 serves as a tool or function - essentially a means to achieve the intended processing purpose. Therefore, the use of Office 365 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 Office 365 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 Office 365 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 Office 365 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 have considered that Microsoft is providing us with certain information and controls we need to make choices when we are using Office 365. 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. |

## 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. Customer Data within Office 365 applications, such as Word, Forms, and Excel, can be updated by civil servants to correct eventual inaccuracies. In relation to Customer Data, Microsoft ensures all data is available to us, with features (e.g. version control) and tools (e.g. search), supporting us in managing data quality and data minimization. However, all data generated by Microsoft (logs) or collected by Microsoft (diagnostic data from client apps) serve as factual records of activities and, therefore, are inherently accurate.  We adhere to the principle of data minimization by processing only what is adequate, relevant, and necessary for the task at hand. For instance, Office 365 does not process personal data that is not relevant to its functioning, such as physical location, unless it is required for a specific feature. We assess data minimization with a thorough review and follow-up, based on the specific purpose of the processing to determine what personal data is needed to achieve that purpose. In other words, each processing activity is tied to a clearly defined purpose. We mitigate excessive sharing of personal data with Microsoft through the implementation of robust policies that provide clear guidance and control measures. We address the specific risk of civil servants oversharing personal data on open forums such as Teams and SharePoint through targeted measures, including training of civil servants, the implementation of usage policies, and the development of detailed “How-to” and etiquette guides to reinforce appropriate practices. |

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

|  |  |
| --- | --- |
| **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 Office 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 Office 365. This includes, if necessary, detailing specific use cases, and the operations that stem from the implementation of Office 365. 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: […]. |

## 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 confirm that our internal data subject rights management processes already encompass the processing activities contemplated by Office 365, ensuring compliance with GDPR requirements regardless of the specific services used. Most importantly, 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.  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 Office 365 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 Office 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 Office 365 data subject requests: [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 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 at https://aka.ms/subprocessor) 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 Office 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.  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 GDPR and, if applicable, 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 the 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 Office 365 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 might leak 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 Office 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, Office 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**  **Source of risk:** phishing, brute-force attacks, or password reuse. Additionally, privileged access misuse, weak identity federation, excessive admin privileges, improper SSO configurations, and delayed deactivation of former civil servants. For example, a 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:** unauthorized exposure of public sector data, identity fraud, financial loss, legal consequences, and a loss of public trust in digital services. For instance, if a compromised civil servant account is used to alter citizen records, individuals may face incorrect liabilities, or unauthorized access to citizen databases could result in fraudulent claims filed in a citizen’s name.  **Associated compliance and public sector risks:** 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 non-compliance with 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 Office 365 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 for 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.***  **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 Office 365 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 Office 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 Office 365 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 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 Office 365 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 7: 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/)

[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)

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

**SPECIFIC RESOURCES**

| **GDPR** | **Subject** | **MSFT 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/) |
| 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) |
| Art 28.3(a) | Documented instructions | Customer agreement (incl. DPA), product documentation and customer’s use and configuration |
| 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[:](:%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) |
| Art 35 | Data Protection Impact Assessments (DPIA) | 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 | 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)