Customizable DPIA document

for

Microsoft

Online ServicES

# Introduction

**This customizable Data Protection Impact Assessment (DPIA) document is provided by Microsoft for reference by our customers in the event that they need or want to complete a DPIA for their organization’s use while using a Microsoft Online Service.**

**This document does not constitute legal advice on behalf of Microsoft or any of its affiliates and should only be construed as a helpful and illustrative customizable template. All obligations under any applicable law in relation to the DPIA or the relevant Microsoft software or service continues to vest with the relevant parties as set forth in the agreement governing Online Services.**

**A note on special formatting and text: Throughout this document, Notes will be identified as such and will be formatted in bold italic navy-blue font such as seen directly below.**

***Note:***

***A Data Protection Impact Assessment (“DPIA***”) is a process for assessing ***and demonstrating data protection compliance as mandated by the General Data Protection Regulation (“GDPR”) under Article 35. Organizations who need to understand when to perform a DPIA can refer to the applicable regulator’s guidance for you to make a determination on the matter. Here are a few sample resources that might help in reaching a conclusion:*** [***Irish Data Protection Commission***](https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments)***,*** [***United Kingdom Information Commissioner’s Office***](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)***, and an additional*** [***Microsoft article on the topic***](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-data-protection-impact-assessments?view=o365-worldwide)***.***

***This document is provided by Microsoft for existing and prospective enterprise customers conducting DPIAs in relation to a Microsoft Online Service. It sets out an illustrative, non-exhaustive model in this regard. In order to provide customers easy access to relevant information in relation to their use of Microsoft services we suggest referencing the - DPIA Service Elements Matrix*** [***here***](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-office365?view=o365-worldwide)***. Also, customers will want to reference the*** [***Online Service Terms***](https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46) ***and the*** [***Data Protection Addendum***](https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67) ***for completion of their DPIA and an understanding of how Microsoft operates the service(s).***

***Customer-specific information and contextual assessments of data protection risks, mitigations and approvals are to be added by individual customers on a case-by-case basis whilst completing their DPIAs. Notes have been added throughout the form to assist outlining what this process might look like. The format used in this template may differ from a customer’s own DPIA format and is illustrative only.***

***Access to detailed and contextual data protection resources including audited controls, compliance guides, white papers and ISO reports about how Microsoft cloud services protect data, and how an organization can manage cloud data security and compliance for your organization, are set out in the Service Trust Portal, accessible*** [***here***](https://servicetrust.microsoft.com/ViewPage/TrustDocuments)***.***

***Additional information on DPIAs for Data Controllers Using Microsoft services including but not limited to Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams is provided*** [***her******e***](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-office365)***.***

***It’s 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, service configurations, and privacy controls 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.***

[Microsoft volume licensing Online Services Terms](https://aka.ms/onlineservicesterms)

[Microsoft volume licensing Online Services Data Protection Addendum](https://aka.ms/DPA)

[Microsoft Enterprise documentation and resources](https://docs.microsoft.com/en-gb/microsoft-365/enterprise/index)

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

[Microsoft Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Office 365](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-office365)

[Microsoft privacy statement](https://privacy.microsoft.com/en-gb/privacystatement)

[Accountability Readiness Checklist for Microsoft Office 365](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365)

[Data Subject Requests for the GDPR and CCPA](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365)

[Information Protection for GDPR](https://docs.microsoft.com/en-gb/microsoft-365/compliance/office-365-information-protection-for-gdpr)

[DPIA Service Elements Matrix](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-office365?view=o365-worldwide)

Contents

[Introduction 1](#_Toc46385879)

[1. DPIA setup and changelog 4](#_Toc46385880)

[2. About the processing activity in scope 7](#_Toc46385881)

[3. Data necessity, proportionality and transparency 11](#_Toc46385882)

[3.1 Lawfulness, Fairness and Transparency 11](#_Toc46385883)

[3.2 Purpose Limitation 12](#_Toc46385884)

[3.3 Data Accuracy and Data Minimization 13](#_Toc46385885)

[3.4 Accountability 13](#_Toc46385886)

[3.5 Data Subject Rights 15](#_Toc46385887)

[4. Data Security 16](#_Toc46385888)

[5. Data Processors and International Transfers 19](#_Toc46385889)

[6. Stakeholder engagement 22](#_Toc46385890)

[7. Diagram of Personal Data Flows 24](#_Toc46385891)

[8. Data Protection Risk Identification, Assessment and Mitigation 25](#_Toc46385892)

# DPIA setup and changelog

***This section provides introductory information about the DPIA being conducted, including high level descriptions of the processing activity, key dates, and stakeholders involved.***

|  |  |
| --- | --- |
| **Title** | **Description** |
| 1.1 Project Title |  |
| 1.2 Target implementation date |  |
| 1.3 DPIA prepared by and person responsible for upkeep of this DPIA (indicate if they are separate) | ***.*** |
| 1.4 Date of next review of this DPIA | ***Note: Any updates to an online service that materially changes the data collection, use or processing could prompt a DPIA review. In addition, you (the customer, and note that “you” and your” throughout this document refer to the customer) may choose to require DPIAs be reviewed on a given set schedule.*** |
| 1.5 DPIA change log (dates of changes made to this DPIA and summary of key changes) | Note: Include necessary information from your perspective in your DPIA as required. This may include the date and summary of key changes made (if applicable). Consider things like, is this a ‘brand-new processing activity’, or is there a ‘change to an existing personal data processing activity? |
| 1.6 Data Controllership:   * Customer is Controller * Customer is a joint controller * Customer is Processor * Not yet known | ***Note: You may conduct an independent assessment of data controllership based on the facts and circumstances of where you deploy software and how it is used. Under the terms of the Online Services Terms (OST) and Data Protection Addendum (DPA), a customer is the controller of personal data and Microsoft is the processor of such data, except:***   * ***When you act as a processor of personal data, in which case Microsoft is a subprocessor; or*** * ***As stated otherwise in the OST or the DPA.***   ***To the extent Microsoft uses or otherwise processes personal data subject to the GDPR or other data protection requirements in connection with Microsoft’s legitimate business operations, Microsoft will be an independent data controller for such use and will be responsible for complying with all applicable laws and controller obligations.*** |
| 1.7 Third parties responsible for processing personal data | ***Note: Include necessary information from your perspective if you have additional third parties responsible for processing personal data such as a third party connected app.***  Example:  Microsoft Corporation  Microsoft Sub processors (as applicable) |
| 1.8 Is this a ‘Mandatory’ or ‘Good Practice’ DPIA | Note: As set out in the introduction, the DPIA may be needed under the GDPR, or it may be a good practice DPIA undertaken without being strictly necessary and it can be helpful to signify what is prompting the DPIA. |
| 1.9 Product or Service version(s) (if applicable) | Note: ***Information on which version(s) are be used or are deployed. It is understandable that for large organizations there may be more than one version currently deployed across your (the customers) environment. If there are more than one version deployed it may be good to note if there are any privacy impacting setting or control differences between the versions.***  Example Microsoft Teams: Information on which version of Microsoft Teams you may be using can be found [***here***](https://support.office.com/en-gb/article/find-the-version-of-teams-you-re-using-e6d3421f-b4f2-4fc6-a69e-ebc528fb1216)***.*** Unlike traditional software, Microsoft Online Services are visionless. There are applications and software to be considerate of, but Microsoft Online Services are not versioned. |
| 1.10 External reference materials relied upon (version or publication date if applicable) | ***Note: Listed and hyperlinked in the introduction of this document are some Microsoft references and documents that might typically be relevant for the purposes of completing a DPIA. The links and the information contained in them are subject to change as are other reference materials that you (a customer) might rely on such as regulatory guidance. As such ensure that the correct version/information is used/referred to when completing the initial DPIA and for each subsequent review or update of a DPIA it may be good practice to validating if any privacy impacting changes within relevant referenced materials has occurred. One initial step might be to document the version or publication data of a document you rely upon for the creation of the DPIA.***  ***Please also note that you (the customers) may wish to refer to other external reference materials (such as regulatory guidance) and again noting the point in time of the referenced guidance might be helpful.***  Example: Microsoft Online Service Terms (August 2020 version). |

# About the processing activity in scope

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 readers detailed information about the envisaged processing.

|  |  |
| --- | --- |
| **Title** | **Description** |
| 2.1 Provide a brief description of what the data processing is intended to accomplish (i.e., the primary purposes for which the data are collected and used). Generally, this can be a high-level description of the services. This can **briefly** describe the service, the data subjects whose personal data is processed as well as the purpose/value derived from the processing system. Put simply, why does this exist? | Note: This section can describe the service and processing activity (e.g. deploying a specific Microsoft Online Service) at a high level and may include information contained in Microsoft documentation in addition to your own context.  Example Exchange Online***:*** Exchange Online provides email related services. It is a hosted messaging, calendaring, and note-taking service that requires processing of large amounts of data to deliver the capabilities of Microsoft Exchange Server as a cloud-based service. It gives users access to email, calendar, contacts, and tasks from PCs, the web, and mobile devices.  In addition to these core services, Exchange Online provides an extensibility platform that allows first party and third-party applications to connect to the service and provide additional features or services, such as notetaking and bill paying services.  Exchange Online integrates with Microsoft Azure Active Directory, enabling administrators to use group policies, as well as other administration tools, to manage Exchange Online features across their environment. |
| 2.1 Is there a joint controllership? If so, explain how responsibilities are sought to be captured and divided. | Note: Refer to section 1.6 for understanding the relationship between Microsoft and you (the customer). A joint-controllership scenario is not contemplated under the terms of the OST and DPA. However, you should consider if there is joint controllership in other relationships you may establish in connection with data processing. This could be the case if you work with an independent third-party partner and jointly determine the purpose and means for processing. |
| 2.2 Explain and provide a narrative overview of the personal data processing in detail and highlight any steps that are high risk.   * sourced * processed * stored * shared * deleted   This needs to contain sufficient detail to understand what and how the personal data will be processed and by whom. The narrative should allow a reader, such as a regulator, to understand how the data flows. | Note: This section can detail the processing activity in a manner that helps understand how personal data is processed using a Microsoft online service and specific context in which this may pose high risks from a data protection perspective.  Include necessary information from your perspective, in relation to collection specifics and the deployment context of your environment. How and how often will the personal data be collected and used? Will personal data typically be collected in an electronic form, as users create documents, uploads, shares and/or use the service? Consider the terms of the Microsoft OST/DPA in this section and how personal data is sourced.  Personal data processed through online services will typically be stored in the cloud or computer-based file systems, databases, and folders, depending on the deployment method used and individual customer and user (e.g. employees) choices. Depending on the mode of deployment, this may be on-prem, hybrid or cloud-based storage. Describe in detail your processing activities and consider including the nature and processing as related to Microsoft, per the terms of the Microsoft OST/DPA and how core features in a service may be relevant for this purpose.  ***Give details of external processors/companies who will have access to the personal data and explain why and how it will be shared/transferred e.g. third-party suppliers (including on site contractor’s utilities, government departments, councils or any other commercial entity as part of a project).*** Information in relation to Microsoft’s use of third party subprocessors may be found here in this [***guidan******ce***](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-office365)and the OST/DPA. Subprocessors are engaged by Microsoft in order to support ancillary services and functions such as customer technical support and service maintenance.  ***Include necessary information about the storage and retention of personal data. In connection with Online Services, it is expected that most personal data will be included within data you or your uses choose to process and store (“Customer Data” in the OST), and customer solely determines the retention period for such data. It might be helpful to reference retention policies that exist, it’s also may be important to consider what external/third party policies are in this regard. Information relating to data retention by Microsoft is based on the Microsoft DPA and*** [***Microsoft guidance***](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-office365) ***might be helpful for your understanding.*** Microsoft services such as[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)can also support the management of removable media. Additional guidance in this regard is also included in the[***FedRAMP Moderate FedRAMP System Security Plan***](https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=053666de-e359-43ef-a7bb-3cf379208ed8&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_FedRAMP_Reports)(Media protection section).  It can be important ***to understand requirements around the retention of personal data past its use for the identified purposes, consider this topic in your creation of this section. For example, how does your organization check temporary file deletion and validate this against policy.***  Articulate disposal policies, in addition, information relating to Microsoft and data disposal may be located in the DPA and additional sources such [***Microsoft 365 guidance on Data Subject Requests***](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365#deleting-personal-data) ***deleting personal data.*** |
| 2.3 List personal data being processed. | Note: ***This section can be used to set out the types of personal data expected to be processed. For example, this could include employee/client names, addresses and other contact information, employee records, customer IDs, etc. It may be helpful for organizations to leverage data classification systems and standards such as ISO 19944.*** The types of personal data that you elect to include in Customer Data may include any categories of personal data identified in records maintained by you acting as a controller pursuant to Article 30 of the GDPR; including but not limited to, the categories of personal data set forth in the Standard Contractual Clauses (Processors) of the DPA.  ***Search and discovery tools in Microsoft Online Services can help to find data that may be personal data or the subject of a data subject request. More information in this regard is provided*** [***here***](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365?view=o365-worldwide#using-the-content-search-ediscovery-tool-to-respond-to-dsrs) ***and it could be possible to leverage the audit log function in the*** [***Security and Compliance Center***](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide) ***to help maintain records for accountability under the GDPR.*** |
| 2.4 Privacy screening criteria met | Note: This section can describe the DPIA risk factors (if any) under a privacy risk assessment undertaken by you (the customer), or in relation to deploying an online service. For example, the risk factor may be processing data from many individuals and/or processing special categories of data. Such factors will differ by organization. |
| 2.5 Approximate number of individual data subjects whose personal data is envisaged to be processed | Note: Include necessary information from your perspective in your DPIA as required. |
| 2.6 What categories of data subjects are impacted and exist by the data processing/whose personal data is being processed, what is the nature of your relationship with the individuals?  Examples: employee; contractor; supplier; member of employee’s household; member of public; children or other vulnerable groups | Note: The information provided here will depend on the specific deployment scenario. For example, the personal data of employees, customers or patients may be processed through the use of the online service in the ordinary course of business.  These categories may also include any other categories of data subjects as identified in records maintained by you as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in The Standard Contractual Clauses (Processors) of the Data Protection Addendum, under which you may elect to include personal data from any of the following types for illustrative purposes of data subjects in the Customer Data:   * Employees, contractors, and temporary workers (current, former, prospective) of data exporter; * Dependents of the above; * Data exporter's collaborators/contact persons (natural persons) or employees, contractors, or temporary workers of legal entity collaborators/contact persons (current, prospective, former); * Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services; * Partners, stakeholders, or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter; * Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter); * Minors; or * Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).   Finally, are their special categories of data that might need extra considerations as you draft this DPIA for example; racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person’s sex life or sexual orientation, or data relating to criminal convictions or offences that might warrant special thought and consideration.  It is likely of note that under the terms of the Microsoft Data Protection Addendum categories of data subjects are specifically contemplated and it’s suggested that you review this as part of your creation process for a DPIA and understanding the role of the online service. |

# Data necessity, proportionality and transparency

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

## Lawfulness, Fairness and Transparency

|  |  |
| --- | --- |
| **Title** | **Description** |
| 3.1.1 What is the lawful basis for this processing? | Note: Include necessary information from your perspective in your DPIA as required, based on your assessment of lawful basis under Article 6 of the GDPR, under which processing may be based on consent, contract, legal obligation, vital interests, public task or legitimate interests. It may be desired to consider any requirements related to the lawful basis of processing, such as whether consent must first be given.  From Microsoft’s perspective, please note that under the OST customers are the controllers of personal data and Microsoft is the processor of such data, except (a) when customers act as a processor of personal data, in which case Microsoft is a subprocessor. To the extent Microsoft uses or otherwise processes personal data subject to the GDPR or other Data Protection Requirements in connection with Microsoft’s legitimate business operations, Microsoft will be an independent data controller for such use. |
| 3.1.2 Are there other less privacy impacting ways to achieve the same outcome? |  |
| 3.1.3 What information or privacy impacting notices are provided to data subjects in relation to the processing? | Note: This may include reference to internal policies and documents as well as Microsoft’s privacy and service-related documents which may be shared by you with data subjects.  In relation to what information you may wish to share with individual data subjects, the following Microsoft guidance may be relevant:   * [***Microsoft 365 Data Subject Requests for the GDPR and CCPA***](https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365)***:*** This guide discusses how to use Microsoft online products, services, and administrative tools to help customers find and act on personal data to respond to data subject requests. Specifically, this includes how to find, access, and act on personal data or personal information that resides in Microsoft's cloud. * [***Microsoft Privacy Statement***](https://privacy.microsoft.com/en-gb/privacystatement#mainmicrosoftaccountmodule)***:*** Although applicable to interactions and processing of personal data by Microsoft vis-a-vis end users (and not enterprise customers), the privacy statement provides useful guidance on how Microsoft may process individual’s personal data. This may be considered by the customer when supplementing its own guidance, policies and privacy statements which may further capture data protection provisions in the OSTs. In addition, there is information in the Privacy Statement intended for users provided products by their organizations about how Microsoft processes data for our legitimate business operations. |
| 3.1.4 If processing is based on consent, how is this obtained/withdrawn? | Note: Different legal bases may be used for different categories of data and there may be multiple parts to this answer based on the categories of data being processed and how consent is obtained or withdrawn. |

## Purpose Limitation

|  |  |
| --- | --- |
| **Title** | **Description** |
| 3.2 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? | Note: Include necessary information in your DPIA as required, based on controls established in relation to compliance with the GDPR’s purpose limitation principle. |

## Data Accuracy and Data Minimization

|  |  |
| --- | --- |
| **Title** | **Description** |
| 3.3 What controls are in place to ensure (i) data quality and (ii) data minimization? | Note: ***Include necessary information based on existing technical and organizational measures implemented.***  ***Where appropriate, Microsoft applies de-identification and pseudonymization, in order to provide additional privacy safeguards for personal data.*** |

## Accountability

|  |  |
| --- | --- |
| **Title** | **Description** |
| 3.4 What measures do you have in place to demonstrate compliance with the GDPR principles | Note: Include necessary information in relation to the technical, organizational and other measures implemented to demonstrate compliance with the GDPR. It may also be helpful to cross-reference other provisions and sections in the DPIA.  Broad measures undertaken by Microsoft in relation to compliance with the GDPR are set out[***here***](https://privacy.microsoft.com/en-GB/)***,*** including Microsoft’s six privacy principles as listed below:   * Control: We will put you in control of your privacy with easy-to-use tools and clear choices. * Transparency: We will be transparent about data collection and use so that you can make informed decisions. * Security: We will protect the data that you entrust to us via strong security and encryption. * Strong legal protections: We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right. * No content-based targeting: We will not use your email, chat, files, or other personal content to target ads to you. * Benefits to you: When we do collect data, we will use it to benefit you and to make your experiences better.   Microsoft specific measures and documentation in this regard is set out (among others) in the [*Accountability Readiness Checklist*](https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-arc?view=o365-worldwide) which provides an overview of the documentation, controls and measures in relation to compliance with the GDPR.  Requirements for testing and evaluating the security of processing personal data may include technical tests such as penetration testing. Where the customer uses a third-party system or processor, they may wish to further understand what responsibilities they have for securing and testing the security (e.g. managing configurations to secure data and then testing those configuration settings).  How Microsoft services are tested security based on identified risks, including tests by third parties, and the types of technical tests and any available reports from the tests:   * Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance * For a listing of external certifications, see Microsoft Trust Center Compliance offerings * For more information about penetration testing your applications see FedRAMP Moderate FedRAMP System Security Plan (SSP), CA-8 Penetration Testing (M) (H) pp204 * Technical compliance review in[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Independent review of information security:  How Microsoft services test and assesses the effectiveness of technical and organizational measures to ensure the security of processing, including any audits by third parties:   * Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance * Office 365 ISMS Manual (see 9 Performance evaluation) * Independent review of information security in[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Additionally, information in relation to Microsoft’s EU Data Protection Officer including contact information is provided[***her******e***](https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-data-protection-officer)***.*** |
| What organizational measures (such as training) have you implemented |  |

## Data Subject Rights

|  |  |
| --- | --- |
| **Title** | **Description** |
| 3.5 How will the rights of the data subjects impacted by this be supported? | Note: Include necessary information from your perspective in your DPIA as required based on internal processes and policies. Illustrative and Microsoft supportive information in this regard is set out below.  Rights of individuals relating to the processing of their personal data may include things such as access, correction, objection, and erasure. 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 Microsoft 365 Security & Compliance Center to manage data subject requests).  In most cases Microsoft’s processing for its legitimate business operations constitutes processing or generating aggregate data that is not unique to customers or natural persons, such as reporting on revenue at the level of a service in a geography. Accordingly, expectations may be set with data subjects that Microsoft’s processing for its legitimate business operations should not be expected to result in data in scope for data subject requests, because the data retained or processed is not personal data  To the extent a data subject has requests that pertain to Microsoft’s processing for legitimate business operations as an independent controller, the data subject may contact Microsoft via the [*Privacy Response Center*](https://privacy.microsoft.com/en-US/privacy-questions) intake mechanism.  Additionally, Microsoft provides customers access to several resources and features which they can use to help data subjects (such as employees or customers) exercise their data subject rights under the GDPR. These include the following:   * [Responding to DSRs for Customer Data](https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-dsr-office365#part-1-responding-to-dsrs-for-customer-data) * [Responding to DSRs with Respect to Insights Generated by Office 365](https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-dsr-office365#part-2-responding-to-dsrs-with-respect-to-insights-generated-by-office-365) * [Responding to DSRs for system-generated Logs](https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-dsr-office365#part-3-responding-to-dsrs-for-system-generated-logs) * [Additional resources](https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-dsr-office365#part-4-additional-resources-to-assist-you-with-dsrs) |

# Data Security

***The data protection principles lie at the core of the GDPR and are correspondingly critical considerations when conducting a DPIA. T***his section sets out information in relation to key security obligations and considerations connected with the envisaged processing activity.

|  |  |
| --- | --- |
| **Title** | **Description** |
| 4. What controls are in place to ensure the security of the personal data? | Note: Include necessary information in relation to security measures implemented to demonstrate compliance with the GDPR. It may be helpful to reference industry standards and measures may include, for example, encryption, access management, breach detection, and data loss prevention. Consider what IT systems are being used to host the personal data. e.g. Corporate managed systems; managed BI Reporting tools; Local Access/EXCEL database; external archiving, cloud. Additionally, relevant Microsoft information and a sample set of applicable controls are found below. Microsoft has implemented and will continue to maintain an Information Security Management System to protect Microsoft Online Service, Customer Data, security commitments are outlined in the DPA (including the GDPR Terms).  Guidance including Microsoft's recommendations for discovering, classifying, protecting, and monitoring personal data contextualized for the GDPR is also provided in the [***Microsoft 365 Information Protection for GDPR guide***](https://docs.microsoft.com/en-gb/microsoft-365/compliance/office-365-information-protection-for-gdpr)***.***  ***In connection with Online Services, Microsoft is obligated to maintain adherence to security and compliance frameworks or standards as set forth in the OST and DPA. Considerations on discrete topics appear below.***  Secure Log-on  You can utilize mechanisms provided in the service to ensure secure log on capabilities for their users where necessary. Information in relation to how Microsoft services support internal access control policies related to personal data can be found[***here***](https://www.microsoft.com/en-us/trust-center/privacy/data-access)and within Microsoft 365 Compliance Center (See Secure log-on procedures in[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)for more information).  Information in relation to Microsoft’s access controls which customersmay be able to use to protect user and device access to Microsoft 365 services is provided [***he******re***](https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-access-to-data-and-services)***.***  Cryptography  You may want to determine which data may need to be encrypted and utilize encryption as needed, using the tools available to them. The Microsoft Compliance Score can be utilized to assess cryptography practices and group the actions necessary to meet the requirements of a standard, regulation, or law (See Cryptography in[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score) for more information).  What Microsoft implements to manage cryptography:   * FedRAMP Moderate FedRAMP System Security Plans (SSP) see Cosmos pp29 * Cryptography in Compliance Score   Clear Desk and clear screen policies  You may want to consider risks around hardcopy material that displays personal data, and potentially restrict the creation of such material. Where the system in use provides the capability to restrict this (e.g., settings to prevent printing or copying/pasting of sensitive data), a customer may wish to consider the need to utilize those capabilities.  What Microsoft implements to manage hardcopy data:   * Microsoft maintains these controls internally (i.e. for data that it stores and processes), see Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability * Clear desk and clear screen policy in [***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)***.***   Separation of development, testing, and operational environments  How Microsoft ensures that personal data is protected in development and test environments:   * Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability * Separation of development, testing and operational environments in[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Information Backup  How Microsoft ensures the availability of data that may include personal data, how accuracy of restored data is ensured, and the tools and procedures Microsoft services provide to allow you to back up and restore data:   * FedRAMP Moderate FedRAMP System Security Plan (see 10.9 Availability) * Information Backup in[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Protection of log information  You may want to consider requirements for protecting log information that may contain personal data or that may contain records related to personal data processing. Where the system in use provides capabilities to protect logs, a customer may want to utilize these capabilities where necessary.  How Microsoft protects logs that may contain personal data:   * Search the audit log in Office 365 Security and Compliance Center * Protection of log information in [***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Information transfer policies and procedures  You may want to have procedures for cases where personal data may be transferred on physical media (such as a hard drive being moved between servers or facilities). These procedures may include logs, authorizations, and tracking.  How Microsoft services transfer physical media that may contain personal data, including the circumstances when transfer might occur, and the protective measures taken to protect the data:   * FedRAMP Moderate FedRAMP System Security Plan (see 13.10 Media Protection (MP)) * Information transfer policies and procedures in [***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Confidentiality or non-disclosure agreements  Microsoft Online Services access and confidentiality management:   * SOC 2 Type 2 Audit Report (see CC1.4 pp33) * Confidentiality or non-disclosure agreements 6.10.2 in [***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Securing application services on public networks  Descriptions of the measures Microsoft Online Services take to protect data in transit, including encryption of the data, and how Microsoft services protect data that may contain personal data as it passes through public data networks, including any encryption measures:   * Encryption in the Microsoft Cloud (see Encryption of Office 365 customer data in transit) * Securing application services on public networks in [***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Secure system engineering principles  How Microsoft services include personal data protection principles as a mandatory part of our secure design/engineering principles:   * SOC 2 Type 2 Audit Report (see Security Development Lifecycle pp23, CC7.1 pp45) * Secure system engineering principles in[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Management of information security incidents and improvements  How Microsoft services determine if a security incident is a breach of personal data, and how we communicate the breach:   * Office 365 and Breach Notification Under the GDPR * Management of information security incidents and improvements in [***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Responsibilities and procedures (during information security incidents)  How to notify Microsoft services in the case a security incident or breach is detected of personal data:   * Office 365 and Breach Notification Under the GDPR * Responsibilities and procedures in[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Response to information security incidents  Descriptions of the information Microsoft online services provide to help a customer decide if a breach of personal data has occurred.   * Office 365 and Breach Notification Under the GDPR * Response to information security incidents in[***Compliance Score***](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score)   Protection of records  How Microsoft services store records relating to the processing of personal data:   * Search the audit log in Office 365 Security and Compliance Center * Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability (see A.18.1.3) * Office 365 ISMS Manual (see 9 Performance evaluation) |

# Data Processors and International Transfers

This section covers the use and sharing of data as part of the envisaged processing activity outside your organization. You (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. It may be helpful to reference and make connections to Section 2.2 of this document where the data narrative describes processing.

|  |  |
| --- | --- |
| **Title** | **Description** |
| 5.1 Specify the jurisdiction(s) where the processing activity(s) will take place (will the processing take place in data centers in specific locations or cloud services hosted from specific locations? E.g. Data capture in Europe, data review in India, data storage in the USA, data backup in Australia) | Note: Include necessary information from your perspective depending on the specific geographical location and mode of deployment that is applicable. Additional information from Microsoft in this regard may be located in the OSTs and/or the DPA and additionally described in the [***Trust Center data location guidance***](https://www.microsoft.com/en-us/trust-center/privacy/data-location). |
| 5.2 Could personal data be shared/transferred outside of the EEA? If so, explain where to, how data is transferred and by whom? |  |
| 5.3 Will a contract be put in place with third parties containing customer’s GDPR clauses?    If a contract is already in place, provide details of the person (solicitor or procurement) who has verified it contains the customer’s GDPR clauses – attach a copy of the contract if possible. [Where personal data is transferred outside of the EEA, adequate safeguards should be in place e.g. Model Clauses, or to an Adequate Country] | Note: Include necessary information from your perspective as required, based on your assessment.  As related to Microsoft, per the terms of the Microsoft OST/DPA and how data is transferred, shared, and stored. This content may already be described in section 2.2 of this document. |
| 5.4 State how you will monitor data processor’s compliance with Data Protection requirements e.g. 3rd party audits | Note: Include necessary information from your perspective in your DPIA as required, based on your assessment.  Microsoft provides access to a range of compliance resources including 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 General Data Protection Regulation (GDPR). These are provided through its [***Service Trust Portal***](https://servicetrust.microsoft.com/)***.***  Additionally, the DPA and OST contains the following relevant Microsoft obligations for illustrative purposes please see the expanded details on the contractual terms themselves:  Data Subject Rights; Assistance with Requests  Auditing Compliance  Security Incident Notification |
| 5.5 Is there any EDPB approved code of conduct or certification scheme? | Note: Codes of conduct are mechanisms which can be used to assist an organization in demonstrating their GDPR compliance and may be not applicable in all situations but worth identifying if they exist. |

# Stakeholder engagement

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** |
| 6.1 Customer stakeholders involved in completing this DPIA  Please include all key stakeholders involved, e.g.   * DPO / Office of DPO * Risk and compliance * Legal * Product/Project Manager * Internal Data Protection SME   NIST/Cybersecurity  In addition to those who have supported the completion of this DPIA are they any other internal stakeholders who need to be made aware? | ***Note: An indicative list of stakeholders who may be involved in the DPIA process is set out in the column to the left. However, note that this list is likely to vary on a customer by customer basis.*** |
| 6.2 Document any Customer Data Protection subject matter experts (SME) consulted during the completion of the DPIA, or external stakeholders with whom you need to liaise about this, e.g. works councils.  Describe when and how you will seek the views of those whose personal data will be processed as a result of this activity – or justify why it is not appropriate to do so. | Note: Include necessary information from your perspective. Depending on the deployment context, you may consult with Microsoft on specific open questions that you may have in relation to deploying a service. Additionally, in the event that residual high risks are presented as part of this assessment, you may need to formally consult the data protection supervisor in relation to the envisaged processing activity.  With regard to Microsoft, information in relation to support Microsoft provides for customer DPIAs is also provided in[***Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Office 365***](https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-dpia-office365) |
| 6.3 Is there a need to ask data processors or any other third parties to assist in stakeholder engagement? | Note: Include necessary information from your perspective in your DPIA as required. |

# Diagram of Personal Data Flows

|  |
| --- |
| This section should capture a visual representation of how Personal Data flows. This should align to the written narrative described in Section 2.2. Below is a very simple sample for things that might be considered.  This image is a very simple sample of how Personal Data flows between Data Collection, Data Storage & Processing through to Data Transfer. |

# Data Protection Risk Identification, Assessment and Mitigation

***Note: Risk identification, assessment and mitigation are important aspects to the work being done in a DPIA. The assessment must be conducted by you and there are many different industry standards that might be helpful for you to use in implementing this step of a DPIA.***

***These might include but are not limited to:***

* ***NIST SP 800-30 COSO ERM framework***
* ***ISO 31000 International Standard for Risk Management***

***You may wish to consider particularly whether the processing could possibly result in risks relating to:***

* ***Inability of individuals to exercise their GDPR rights***
* ***Inability to access services or opportunities***
* ***Loss of control over personal data***
* ***Discrimination***
* ***Identity theft or fraud***
* ***Financial loss***
* ***Reputational damage***
* ***Physical harm***
* ***Loss of confidentiality***
* ***Any other significant economic or social disadvantage***
* ***Requests not to receive marketing are not observed***
* ***Tracking without the individual’s knowledge or consent***
* ***Special characteristics are gathered in a non-compliant way***
* ***The individual’s data is used in ways they had not been told about or would reasonably expect***
* ***The individual’s data has been shared with other organizations without their knowledge***
* ***The individual’s data has been retained for far longer than they would have anticipated***
* ***Data has not been kept secure***
* ***More data than is strictly necessary has been gathered***