Microsoft

MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Microsoft 365 for Public Sector in Switzerland

Version 1.1

Microsoft

Content

Tables

Figures

Disclaimer

This document contains a general presentation of questions that our customers often ask when using cloud computing solutions. The aim is to enable customers to understand better the technical and legal background of using a cloud computing solution. This document does not contain a case-by-case examination of individual legal relationships. Therefore, you must seek independent legal advice for an individual and conclusive legal assessment of the permissibility of the use of Microsoft cloud solutions in a specific application.

The information herein is for informational and discussion purposes only and represents the current view of Microsoft Corporation or any Microsoft Group affiliate as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment or binding offer or acceptance of any warranties, liabilities, wrongdoing etc. on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this document.

1 INTRODUCTION TO MICROSOFT PUBLIC SECTOR CLOUD DESIGN

With the rise of modern communication and collaboration and the so-called “new-work”, hybrid and remote work became a critical factor in the success of every authority. With the use of productivity solutions such as Microsoft 365 and, in particular, Microsoft Teams, cloud solutions are now widespread. Those easily accessible services have also become increasingly popular for public sector authorities.

While the benefits are apparent, there are challenges that authorities need to address: In a “cloud first” world, data resides with the cloud provider but remains under the authority's control. It is said that the so-called data processing is "outsourced" to the cloud provider. To ensure control over the outsourced data processing, customers must deal with the cloud provider’s standards and common regulations, particularly regarding information security.

Therefore, public sector customers need to know what assistance Microsoft can provide as a cloud service provider when they decide to use Microsoft 365 Online Services. Public sector customers need to identify the resulting risks and understand Microsoft's contractual, organizational and technical measures to ensure that online services can be used securely.

This document provides customers with an overview of the essential control targets and concrete measures based on Microsoft 365 technologies, focusing on the public sector.

1.1 CONTROL OF DATA AS A CORE TOPIC

Cloud solutions process data on technical infrastructures of specialized third-party providers such as Microsoft instead of the authority's on-premise infrastructure. Such data processing by third parties is legally permissible, provided that, in addition to compliance with the case-specific requirements, the data controller retains full control.

In this context, control refers to technical, organizational, and contractual measures taken to ensure that only authorized persons have access to the data and that the obligations under data protection law (security measures, reporting obligations, compliance with processing principles, etc.) are observed. Furthermore, it must be ensured that the third parties authorized to access the data do not use it without authorization, and data is permanently deleted when requested by the data controller. Finally, the control requirement also includes the requirement that the corresponding outsourcing is transferable back to the authority’s infrastructure or another infrastructure if necessary, all with a reasonable amount of time and effort.

The specific requirements depend on the circumstances and the nature of the data. For example, requirements are higher if data is unencrypted (although data transmission to Microsoft Services is generally always encrypted), or its exploitation could significantly impact the data subjects (e.g., highly confidential data or sensitive data).

The requirement of "control" is not explicitly stated in the law or a single superordinate legal provision. Implicitly, however, all enactments of federal and cantonal legislation relevant to information law aim to organize the control claims to information. Control as a duty is thus, to a certain extent, the abstract "distillate" that remains when the relevant individual legal norms are reduced mentally to the essentials.

The instruments for exercising and ensuring data control are also congruent for local IT infrastructures and cloud solutions, namely technical, organizational and contractual measures.

2 LEGAL CHALLENGES IN CLOUD DESIGN

2.1 OVERVIEW

Although the principle of "Cloud First" is already to be found in a "Cloud Computing Strategy of the Swiss Authorities" adopted almost ten years ago, there is still a certain reluctance on the part of the authorities today, which can probably be attributed to existing uncertainties in dealing with cloud solutions. In the Cloud Strategy 2020, eight years after the decision in favor of the "Cloud First" principle, there is still (or already) talk of a **paradigm shift towards "Cloud First"** (Cloud-Strategy 2020)[1].

The uncertainties can be observed among authorities at all federal levels, i.e., federal, cantonal, and municipal authorities. While the Data Protection Act and other federal decrees are of primary importance for federal authorities, cantonal authorities and municipal authorities must comply with data protection laws and, if applicable, other decrees of the respective canton. What applies to members of authorities at all levels is the official secrecy or the criminal liability of members of authorities in the event of a breach thereof.

2.1.1 Cloud computing as a distinct outsourcing situation

In the context of cloud solutions, data is processed on corresponding third-party IT infrastructures instead of on the company's local computers or servers and managed by a third-party personnel. Therefore, this is a so-called outsourcing situation within the meaning of data protection legislation.

Cloud solutions should, however, be distinguished from other classical outsourcing setups, which also qualify as outsourcing situations under the relevant data protection provisions. "Classical" outsourcing is typically understood as the case in which a service provider builds and controls specific business processes in the customer's place according to specific instructions from the customer and, in this context, receives access to and insight into data. In contrast, in a cloud model, the customer basically receives a **standardized service**. Therefore, the **lack of individuality** in the service relationship (technical and organizational level) is a central differentiation criterion between cloud computing and classical outsourcing. However, the transition between the two forms is blurring.

2.1.2 Abroad

If in the context of cloud solutions, personal data is processed in countries with a lower level of data protection than in Switzerland or the EU, or the EEA (this is referred to as "lack of equivalence" in so-called "insecure foreign countries"), the permissibility of the corresponding data processing is dependent on the fulfillment of additional conditions beyond the general requirement of control (e.g., the existence of contractual protection measures, see also 4.12).

1 https://www.newsd.admin.ch/newsd/message/attachments/64425.pdf

2.2 LEGAL REGULATIONS

2.2.1 General

Since the Confederation has no comprehensive authority to legislate in the area of data protection, the cantons are authorized by virtue of their right to organize themselves to regulate data protection independently insofar as the processing of personal data by cantonal authorities, municipalities, and administrative agencies are concerned. All cantons have general data protection decrees. These concretize the fundamental right to the protection of personality and the principles of the rule of law for the processing of personal data at the cantonal level by defining the prerequisites and general principles of data processing by cantonal and communal authorities as well as the rights of the persons concerned. If cantonal public bodies engage in private economic competition, this activity is not to be classified as the exercise of sovereign functions or the exercise of public duties under cantonal law (as is the case, for example, with cantonal banks).

The FADP and most cantonal data protection laws contain specific provisions for so-called mandated data processing. This is the case when the responsible public body entrusts a third party with the execution of a data processing operation.

In certain cantons, there are specific regulations on the conditions for outsourcing data processing operations to third parties (e.g., the agreement in a written contract, specific regulations on the involvement of subcontracted processors, etc.). However, most cantons do not establish any special specifications in this regard that go beyond the regulations in the FADP.

In general, it can be said that mandated data processing is generally permissible if there are no statutory or contractual confidentiality obligations to the contrary and compliance with data protection regulations is ensured. In this respect, the basic principle in the FADP and the cantonal data protection laws is comparable.

In principle, the public body awarding the contract remains responsible for compliance with data protection. Therefore, it must take appropriate measures to ensure an adequate level of data protection.

2.2.2 The most common specifications in detail

2.2.2.1 Contractual agreement

With third parties who take over outsourced data processing for a public authority (e.g., Microsoft), an outsourcing agreement must be concluded that regulates safeguards with regard to compliance with data protection and data security and the use of cloud services in the public sector.

Depending on the canton, there are legal regulations that specify the content of the contract with the order processor. In some cantons, there are also so-called general terms and conditions, which must be agreed upon as part of contracts for outsourcing IT services or processing personal data.[2] In the interest of a suitable solution, these requirements can be deviated from in principle, namely insofar as no compelling reasons arise from the legal situation to apply such general terms and conditions unchanged or where an examination shows that the requirements for sufficient contractual provisions regarding data protection and data security are also sufficiently taken into account based on the provider's contracts.

In line with the nature of a "cloud" with standardized offers for all customers, Microsoft uses standard contracts for the use of the cloud infrastructure. Considering individual requirements on a larger scale is difficult on the given highly standardized IT infrastructure and must be clarified on a case-by-case basis, for which Microsoft generally offers assistance.

2 E.g., Canton of Bern (General Terms and Conditions on Information Security and Data Protection in the Provision of IT Ser-vices); Canton of Zurich (General Terms and Conditions in the Outsourcing of Data Processing Using IT Services).

2.2.2.2 Processing according to instructions and in the interest of the public body

The commissioned processor may only carry out data processing in accordance with the instructions and the interests of the public body. Art. 10a para. 1 lit. a FADP, as well as various cantonal legislation, contain provisions in this regard that the data may only be processed as the public body itself would be permitted to do.

Microsoft's Data Protection Addendum (DPA)[3] states that. Microsoft, as a data processor, will process customer data (and, in particular, personal data) only as described in the DPA and in a limited manner (a) to provide the products and services to the customer in accordance with the customer's documented instructions and (b) for Microsoft's business operations incident to providing the products and services to the customer. In this regard, the customer's applicable agreement, together with the product documentation and the use and configuration of the functionality of the online services, collectively constitute the customer's complete and documented instructions vis-à-vis Microsoft for the processing of personal data.

In particular, customer data will not be used for the purposes of advertising, market research, or user profiling.

2.2.2.3 Involvement of other data processors

The DPA describes how Microsoft deals with subprocessors and notifies customers of changes to the portfolio of subprocessors, etc., in the section "Notice and Controls on use of Subprocessors". This describes the requirements Microsoft places on subprocessors and that Microsoft is responsible for ensuring that subprocessors meet all requirements that are part of the DPA.

The Services Trust Center[4] maintains the list of subprocessors, including the services they provide, the location of their headquarters, and the scope and conditions under which they may access Customer Data: http://aka.ms/mscloudsubprocessors.

In Core Online Services, neither Microsoft nor subprocessors have permanent administrative access to customer data or customer solutions. Microsoft operates with "Zero standing ADMIN" also known as "Least Privilege", where administrative access is controlled by an authentication process (called "Lockbox"), e.g., in the case of customers who engage Microsoft to perform a support task that grants privileges to the employee in charge of the support case (which could allow temporary access to customer data). The assignment of administrative access must be done through multiple links, time boxes, and a full audit trail – and can include final approval by the customer, if the customer wishes, by setting up an enhanced "lockbox" process called "customer lockbox" (see Chapter 4.9).

2.2.2.4 Data security

The national and cantonal data protection and information security laws generally require the contractor to ensure appropriate data security in connection with outsourcing IT services or mandated data processing. Most cantonal decrees do not define any specific protective measures but lay down principles regarding the protective goals to be safeguarded – confidentiality, **availability, and integrity**. In particular, the following risks must be safeguarded:

– Unauthorized or accidental destruction

– Accidental loss

– Technical error

– Forgery, theft, or unlawful use

– Unauthorized modification, copying, accessing, or other unauthorized processing

Personal data must be protected against such risks by **appropriate technical and organizational measures**.

3 Privacy Addendum of Microsoft's Products and Services: https://aka.ms/dpa
4 https://servicetrust.microsoft.com/

Microsoft uses numerous encryptions at various levels in its online services and has published comprehensive documentation and white papers. On the one hand, various encryptions are applied to stored data ("data at rest"), both on the operating environments ("volume level") and the individual data files, thus preventing physical access to the data. Using self-administered keys can further enhance encryption protection, so-called BYOK ("Bring Your Own Key"). Microsoft also uses encryption techniques for data transmission ("data in-transit"). In addition, the online services allow the cloud customer to apply and manage various encryption techniques of their own.

Via the Microsoft Trust Center[5] as well as via the service review in the Security & Compliance Center[6], cloud customers can directly view certification and audit review reports as well as other comprehensive information about the data storage locations, access options to cloud customer data, security precautions and data protection precautions at any time. In this way, the cloud customer can convince itself of Microsoft's compliance with security obligations at any time.

2.2.2.5 Cross-border transfer

Federal and cantonal data protection laws impose special requirements when personal data is transferred abroad or accessed from abroad as part of processing in cloud environments.

In general, outsourcing to a country with a level of data protection equivalent to Switzerland is permitted without further measures. This includes, in particular, all EU/EEA countries.

Microsoft uses the data centers of the Switzerland region and parts of the Europe region (with data centers in Ireland, the Netherlands, Austria, and Finland) for SaaS online services for Swiss cloud customers by default. Customer data is stored in these data centers. The respective data storage locations can be accessed for each online service via the respective service check in the Security & Compliance Center.

The specific provision of the Online Services or Customer's individual configuration of the Online Services may require that some Customer Data be made available to Microsoft employees or subprocessors outside of this primary storage region. Likewise, those Microsoft employees with the most technical experience in addressing specific service issues may be located outside of this primary storage region and may need online access to systems or data to resolve an issue.

According to the DPA, Microsoft may therefore transfer, store, and process Customer Data that Microsoft processes on behalf of Cloud Customer to other countries in which Microsoft or its affiliates or subprocessors have facilities (sometimes including the United States). In doing so, Microsoft agrees to comply at all times with the requirements of Switzerland's data protection laws with respect to the collection, use, transfer, retention, and other processing of Personal Data from Switzerland.[7]

5 https://www.microsoft.com/en-us/trust-center
6 https://docs.microsoft.com/en-us/microsoft-365/compliance/service-assurance?view=o365-worldwide
7 https://aka.ms/dpa, «Data Transfer»

For such potential transfers of customer data, professional services data, and personal data from the EU/EEA and Switzerland to so-called unsafe third countries, Microsoft has concluded so-called standard contractual clauses (processor-to-processor) between Microsoft Ireland Operations Ltd. and Microsoft Corp. USA. The standard contractual clauses were adapted to Swiss conditions for data exports from Switzerland in accordance with the recommendations of the FDPIC.

On May 6, 2021, Microsoft announced that it would use the so-called EU Data Boundary to technically design the core online services Azure, Microsoft 365, Dynamics 365, and Power Platform in such a way that the core customer data is processed and stored within Europe and support is provided from the European region.[8] The stated completion target is the end of 2022.

Microsoft will also not disclose Customer Data to law enforcement authorities unless required by law. If law enforcement authorities contact Microsoft to request Customer Data, Microsoft will attempt to redirect the law enforcement authority to request such data directly from the Customer. If Microsoft is required to disclose or provide access to law enforcement authorities, Microsoft will promptly notify the Customer and provide a copy of the request unless prohibited by law. Microsoft takes a principled and rigorous approach to deal with government requests for access to Customer Data in Microsoft's custody.[9]

Microsoft publishes Law Enforcement Request Reports every six months to ensure transparency about the scope and nature of these incidents.[10] The reports are public and can be used to assist in conducting risk assessments. Microsoft interacts with customers and governments worldwide on a daily basis, actively shaping the international legal framework for these critical issues. Microsoft has published six principles that build on ongoing efforts to protect Microsoft customers' data and improve privacy to guide this work.[11] Microsoft believes that the principles articulated represent universal rights and basic minimum requirements that should govern law enforcement access to data in our modern era. Applying these principles may vary from country to country, but the underlying principles of checks and balances, accountability, and transparency should remain.

2.2.2.6 Authority access

Microsoft believes that customers have the right to be protected by their laws. Microsoft takes a principled and rigorous approach to deal with government requests for access to customer data in Microsoft's custody.[12] The key policies that Microsoft adheres to in all of its services are:

- Microsoft does not give any government direct and unfettered access to its customers' data and does not give any government the encryption keys or the ability to break the encryption.
- If a government wants customer data, it must follow applicable legal procedures. It must show a search warrant or court order for content data, a procedural order for subscription information, or other non-content data.
- All requests must refer to specific accounts and identifiers.
- Microsoft's Legal Compliance team reviews all requests to ensure they are valid, reject those that are not, and provide only the specified data.
- In addition, after the Schrems II ruling, Microsoft committed to challenging government requests for customer data from third parties legally.[13]

Part of Microsoft's work on government inquiries includes publishing "Law Enforcement Request Reports" every six months[14] to provide transparency on the scope and nature of these incidents.

8 https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/
9 The process is described in detail here: https://aka.ms/mslerh
10 Located here: https://aka.ms/mslerr
11 "Six Principles for International Agreements Governing Law Enforcement Access to Data": https://aka.ms/MS6dataaccessPrinciples
12 The process is described in detail here: https://aka.ms/mslerh
13 See also: https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/
14 https://aka.ms/mslerr

For an assessment of the risk of government access, it may be relevant to consider the actual scope figures from the Microsoft Law Enforcement Request Reports available at the link above. Well over 90% of government requests involve data from Microsoft consumer customers such as Hotmail or Skype.

It is clear from these figures that ...

– ... the probability that a particular corporate customer is the target of such a request is minimal,

– ... the probability that such a request will NOT be rejected or redirected is even lower, and

– ... the likelihood that such a request for data stored outside the country of origin of the request will NOT be rejected or redirected is even lower.

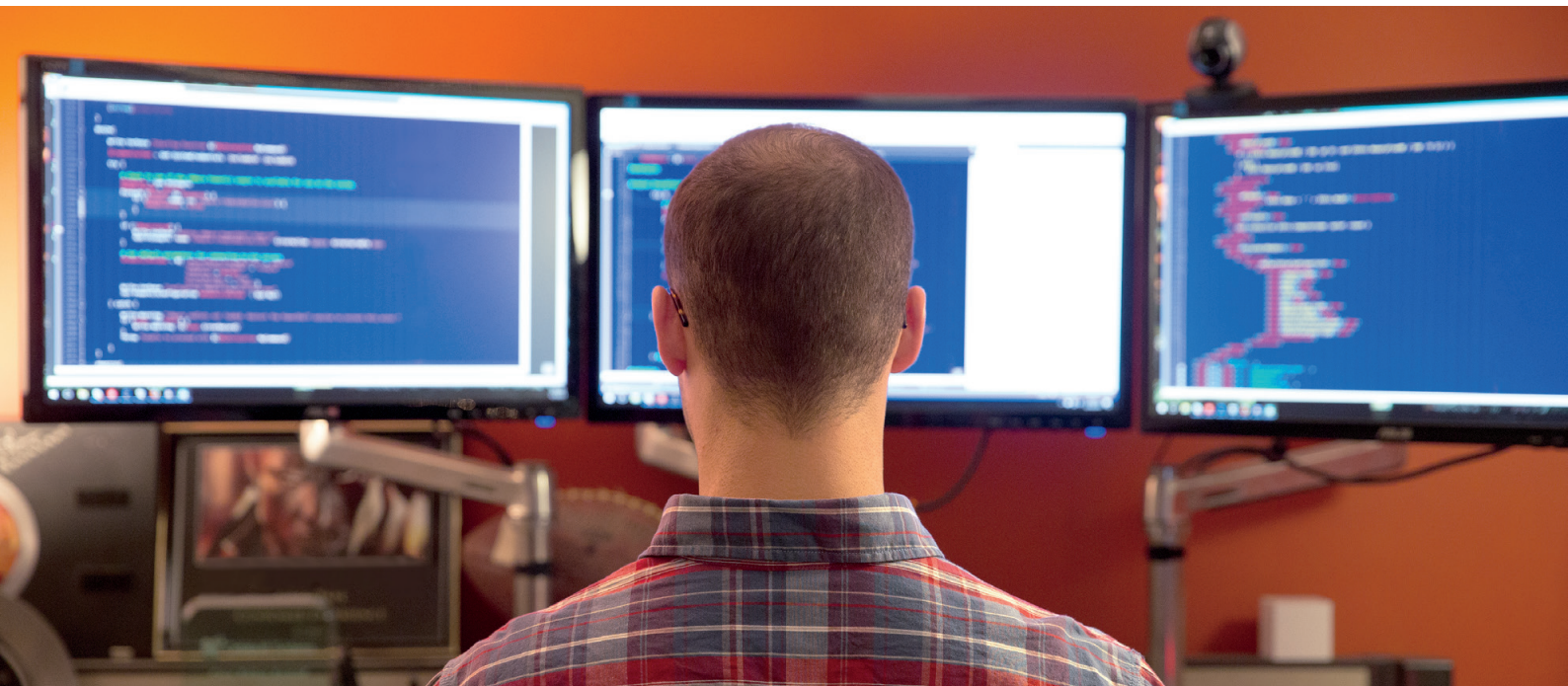
Based on these reports, an understanding of Microsoft's principled process and history of protecting customers' privacy rights, it should be possible for customers to conduct a risk assessment showing that the likelihood, and therefore the overall risk, from third country law enforcement requests, is absolutely minimal to virtually non-existent.

Note further that the numerical difference between requests for consumer accounts and corporate accounts also reflects formal guidance[15] from the U.S. Department of Justice's Computer Crime and Intellectual Property Section, which advises prosecutors to go directly to companies for access to their data when it is practical and does not otherwise compromise the investigation, rather than trying to go through cloud service providers.

2.2.2.7 Critical data

With regard to very specific information that should not fall into the hands of third parties due to the public interest, for example, because of a special security connection to critical infrastructures of the community, there could be an explicit or implicit restriction on the use of a cloud service. In this respect, the community would be obliged to use suitable information classifications to delimit those data not to be included in a cloud project. Such aspects must be specially planned in each case, and appropriate measures must be taken.

15 https://aka.ms/USDoJSeekingEnterpriseData



2.3 INFORMATION PROTECTION ORDINANCE (IPO)

The Ordinance on the Protection of Federal Information (Information Protection Ordinance, IPO, 2015)[16] regulates the protection of federal and armed forces information insofar as this is required in the country's interests. In particular, it defines its classification and processing. At the heart of the ordinance is the assignment of classification levels to information according to the degree to which it merits protection. Measures are proposed or can be derived from this. The ordinance recognizes the following 3 classification levels: SECRET, CONFIDENTIAL, INTERNAL.

The following table summarizes all electronically applicable information handling measures per classification level.

Class / Machining specification	**INTERNAL (RESTRICTED[17])**	**CONFIDENTIAL**	**SECRET**
Classification note (label)	Note INTERNAL	Note CONFIDENTIAL	Note SECRET
Storage or retention	Access protected	Encrypted on workstation systems or removable media	Only on approved funds or encrypted on workstation systems or removable media
Data transmission	Protected transmission path (e.g., federal network)	Encryption or protected transmission path	Encryption or protected transmission path
Editing with computer tools	Permitted	Only with means approved by the coordination office (exception: army) and using security software according to federal standard	Only with means approved by the coordination office and using security software in accordance with the federal standard
Carriage from permanent location	Permitted	Restricted permissible	Restricted permissible
Withdrawal and obligation to return	None	Mandatory	Mandatory
Destruction or deletion	Restricted permissible	Restricted permissible	Only by author

Table 1 – Matrix classification levels and measures according to IPO

The Ordinance also applies to organizations and persons under public or private law and federal and cantonal courts that process classified information, insofar as this is provided for in federal law or has been agreed accordingly.

16 https://www.fedlex.admin.ch/eli/cc/2007/414/en
17 Information from abroad classified as "RESTRICTED" or equivalent is processed in the same way as information classified as INTERNAL

3 CONTROL OBJECTIVES AND RISKS

As in other areas, there is no law or regulation that either completely prohibits or per se permits cloud use. Therefore, data protection officers of public bodies must carry out a risk analysis based on the applicable legal situation, the type of data, its form of processing, and possible protection and control measures and decide whether the step into the cloud is reasonable.

Awareness and documentation regarding the classification of data and information (cf. chapter 2.3) are of central importance for the selection of appropriate measures. It also forms the basis for configuring and monitoring the technologies and resources behind the measures. Based on the provisions of the Information Protection Ordinance (cf. chap. 2.3), each organization should provide specific measures to protect the respective classes of data. These include contractual, organizational, as well as technical measures. For example, an authority might have the following protective measures and control targets:

- **Secret data**
  As a first step, secret data is not stored in the cloud but locally. To benefit as much as possible from the features of Microsoft's 365, a hybrid deployment for Exchange and SharePoint provides an end-to-end user experience while ensuring the highest possible data protection.
- **Confidential data**
  Confidential data may be stored encrypted in the cloud. Microsoft Purview Information Protection (MIP) is suitable for this, either with its own key (BYOK) or using Double Key Encryption.
- **Data Subject Request**
  Companies may need to respond to formal requests by a data subject. Microsoft 365 provides the necessary tools to provide copies of personal data, request corrections, transferring or erasing with respect to the data subject's personal data.

The following chapters refrain from assigning measures to specific classification levels. The aim is rather to suggest the possible control objectives and risks to be dealt with, which should be considered and dealt with as part of a decision for a public cloud. The measures to be taken can then be determined depending on the type, structure, and information of the data.

3.1 CONTROL TARGETS

The widely used Information Security Triad model can be used as a foundation and classification basis for risks and measures. It focuses on the three main areas of information security: confidentiality, integrity, and availability. The main aim is to achieve the following overarching control objectives and to be able to answer the corresponding questions.

ID	Area	Aim and description	Basics
KZ1	C	**Access control** Are the data in the processor's area of responsibility adequately protected against unauthorized physical access (e.g., confidentiality protection)	Information security best practice (e.g., ICT minimum standard of the FCA) | Art. 7 and Art. 10a para. 2 FADP, Art. 8 and Art. 9 para. 1 lit. a DPO (Ordinance to the Federal Act on Data Protection) | Art. 8 para. 1-2 and Art. 9 para. 2 nFADP
KZ2	C	**Access control** Is electronic access authorization sufficiently regulated?	Information security best practice (e.g., ICT minimum standard of the FCA) | Art. 7 and Art. 10a para. 2 FADP, Art. 8 and Art. 9 para. 1 lit. g DPO (Ordinance to the Federal Act on Data Protection) | Art. 8 para. 1–2 and Art. 9 para. 2 nFADP

KZ3	C	**Usage control** Are individuals with standing or temporary data access sufficiently controlled so that the risk of unauthorized data use is minimized and breaches can be tracked?	Information security best practice (e.g., ICT minimum standard of the FCA) | Art. 7 and Art. 10a para. 2 FADP, Art. 8 and Art. 9 para. 1 lit. d and h DPO (Ordinance to the Federal Act on Data Protection) | Art. 8 para. 1–2 and Art. 9 para. 2 nFADP
KZ4	C	**Deletion control** Is it ensured that the processor deletes the data when the outsourcing ends?	Art. 10a para. 1 it. a DSG | Art. 9 para. 1 lit. a nFADP
KZ5	I	**Integrity control** What precautions are in place to prevent the processor or other third party from manipulating the data?	Information Security Best Practice | Art. 7 and Art. 10a para. 2 FADP | Art. 8 para. 1–2 and Art. 9 para. 2 nFADP
KZ6	A	**Availability control** How is the availability of the data ensured?	Information security best practice (e.g., ICT minimum standard of the FCA) | Art. 7 and Art. 10a para. 2 FADP | Art. 8 para. 1–2 and Art. 9 para. 2 nFADP
KZ7	A	**Recoverability** How is the recoverability of data ensured in case of loss or errors?	Information Security Best Practice | Art. 10a para. 1 lit. a FADP | Art. 9 para. 1 lit. a nFADP

Table 2 – Information security control objectives

3.2 RISK ANALYSIS

The following risk list with the contractual, organizational, and technical measures derived in the following chapter can be evaluated by decision-makers in public bodies and used as a basis for decision-making. The list of risks can be expanded if necessary in the case of additional regulations (e.g., canton or municipality). The risks are derived from the control objectives according to chapter 3.1 and are also classified according to the general **C-I-A** method. Some of the risks only have a reference to the legal or regulatory basis (**Law**), as they can only be indirectly assigned to one of the main areas of information security. The risks are deliberately focused on the customer's relationship with the processor. Nevertheless, in most risk areas, the customer can take additional technical protection and security measures in addition to the contractual and organizational measures surrounding the relationship with the processor itself to address the corresponding risk. This applies to both the processor and potentially unauthorized third parties. The additional question that must be asked per risk is as follows: "How and with which measures can and should I, as a customer, address this risk in addition to the measures taken by the processor?".

A proposal for mapping the corresponding measures is also shown in the following risk table. These are measures taken by the order processor (contract, documentation) as well as measures that the customer can take.

ID	Area (C-I-A), Law	Risk	Measure ID	Risk impact according to measure	Probability of occurrence according to measure	Risk assessment	Residual risk mitigated?
R1	Law	**Subprocessors** Is it ensured that the processor informs the customer about the use of subprocessors and grants the customer a right of objection in the event of replacement or before new subprocessors are brought in (Art. 9 para. 3 nFADP)? Are the subprocessors subject to the same legal and regulatory basis as the processor?	M12				
R2	Law	**Insufficient data security** Is it ensured that the processor adequately protects the confidentiality, integrity, and availability of the customer's personal data (Art. 10a para. 2 FADP, | Art. 9 para. 2 nFADP)? Is auditing of compliance with the relevant security procedures and security guidelines ensured and documented in a comprehensible manner?	M2 M4 M6 M8 M12 M14				
R3	Law	**Unreported data security breach** Is it ensured that the processor reports data security breaches to the customer (Art. 10a para. 2 FADP | Art. 9 para. 2 and Art. 24 para. 3 nFADP)? Does the processor monitor the services with regard to security breaches and proactively carry out optimizations?	M1 M2 M12 M13				
R4	Law	**Own purposes of the processor** Is it ensured that the processor uses the processed personal data only on behalf of and for the purposes of the customer and not for his own purposes (Art. 10a para. 1 it. a FADP, | Art. 9 para. 1 lit. a nFADP)? How are the ownership relationships around the data regulated? How are the roles and responsibilities divided between the customer and the order processor?	M12 M13				
R5	Law	**Cross-border disclosure** Are suitable safeguards (e.g., EU standard contractual clauses) implemented to ensure appropriate data protection when personal data are transferred to countries without an adequate level of data protection (Art. 6 and Art. 10a para. 1 lit. a FADP | Art. 16 and Art. 9 para. 1 lit. a nFADP)?	M11 M12				
R6	C Law	**Disclosure of secret facts** Is information subject to official or professional secrecy adequately protected from plaintext access by the order processor or third parties (Art. 320 StGB, Art. 321 StGB)? Is the data processing by the processor subject to appropriate confidentiality obligations?	M2 M3 M9 M10 M12 M13				
R7	Law	**Governmental access** Does the processor provide sufficient insight into its processes and policies regarding governmental access to data that allows the customer to make an informed decision on this issue (best practice)?	M4 M12 M13 M14				

R8	CIA Law	**Lack of governance** Has the processor given the customer sufficient insight into its own internal control system (ICS) (best practice)? Is auditing of compliance with the relevant security procedures and security guidelines ensured and documented in a comprehensible manner?	M1 M4 M8 M12 M13 M14
R9	I Law	**Lack of reporting** Does the processor provide sufficient reports on outsourced activities and services (best practice)? Is auditing of compliance with the relevant security procedures and security guidelines ensured and documented in a comprehensible manner?	M4 M12 M13 M14
R10	C	**Unauthorized access to data (KZ1)** Is there transparency regarding the technical and organizational measures taken by the processor to protect customer data from unauthorized access and physical access, encryption during transmission, malware protection, confidentiality, authentication, and operational guidelines for its employees?	M3 M9 M10 M12 M13
R11	C	**Unauthorized access to data (KZ2)** Is the processor able to identify access policies to components and data, and is it visible that appropriate security procedures and security policies are applied? Are procedures in place to ensure access to data even after failures?	M3 M5 M12 M13
R12	C, I	**Unauthorized use of data (KZ3)** Is it ensured and shown that the processor either does not have access to the customer's data or can only view it within the scope of the mandated order processing? Is there a log of any data access? Are there confidentiality obligations on the part of the processor within the scope of the required functions?	M9 M10 M11 M12
R13	C	**Non-compliant deletion of data (KZ4)** Does the processor have clear guidelines on how to handle the cancellation of a subscription or the deletion of data by the customer? Are hardware components disposed of in accordance with industry standards? Is the data portable? Is it ensured that there is a contractual right of inquiry on this subject?	M1 M6 M7 M12
R14	I	**Data integrity at risk (KZ5)** Does the processor ensure that its employees are trained on appropriate security procedures, and security policies (e.g., handling of administration sessions or passwords) and actively follow them?	M1 M12 M13
R15	A	**Reduced availability and recoverability of data (KZ6 & KZ7).** Does the processor provide documentation of the SLA and guarantees based on it per service? Has the processor implemented business continuity management? Is it transparent what happens when individual services are discontinued by the processor? Have appropriate recovery procedures and their testing been implemented on the basis of the platform? Are the customer's responsibilities in this context clear?	M7 M12 M13

Table 3 – Risk analysis based on legal basis and basics of information security

4 MEASURES AND COMPONENT DESCRIPTION

This chapter provides a list and in-depth explanation of the possible measures to counter the risks listed above. The order of the measures does not indicate their priority.

Measure ID	Area	Measure	Measures type
M1	C, I, A	ISO 27001	Organizational, Contractual
M2	C	Microsoft Secure Score & Security Compliance Toolkit	Technical, Organizational
M3	C	Microsoft Purview Information Protection	Technical, Organizational
M4	C, I, A	Data Protection Impact Assessments (DPIA)	Organizational
M5	C	Microsoft 365 IAM & Privileged access management	Technical, Organizational
M6	C	Microsoft Purview Compliance Manager	Technical, Organizational
M7	C	Data Subject Request	Technical, Organizational
M8	C, I, A	Microsoft Public Sector Cloud Design Training	Organizational
M9	C, I	Microsoft Purview Customer Lockbox	Technical, Organizational
M10	C, I	Encryption	Technical, Organizational
M11	C, I	Microsoft 365 Hybrid with Exchange and SharePoint	Technical, Organizational
M12	C, I, A	Contract	Contractual
M13	C, I, A	Shared Responsibility Model	Organizational, Contractual
M14	C, I, A	Privacy Management for Microsoft 365	Technical, Organizational

Table 4 – List of measures

4.1 M1 – ISO 27001

ISO/IEC 27001 is the international standard for implementing an information security management system (ISMS) and outlines control targets and measures that help maintain the security of information assets.

An ISMS describes the necessary methods used and evidence associated with requirements essential for the reliable management of information asset security in any type of organization.

It's important to understand Microsoft is ISO 27001 audited and certified. A list of ISO 27001-certified cloud services, including Microsoft 365 and Office 365, is available in the official documentation[18]. Existing customers can find ISO 27001 audit reports inside the Microsoft Trust Center[19].

18 https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001#microsoft-in-scope-cloud-platforms--services
19 https://servicetrust.microsoft.com/

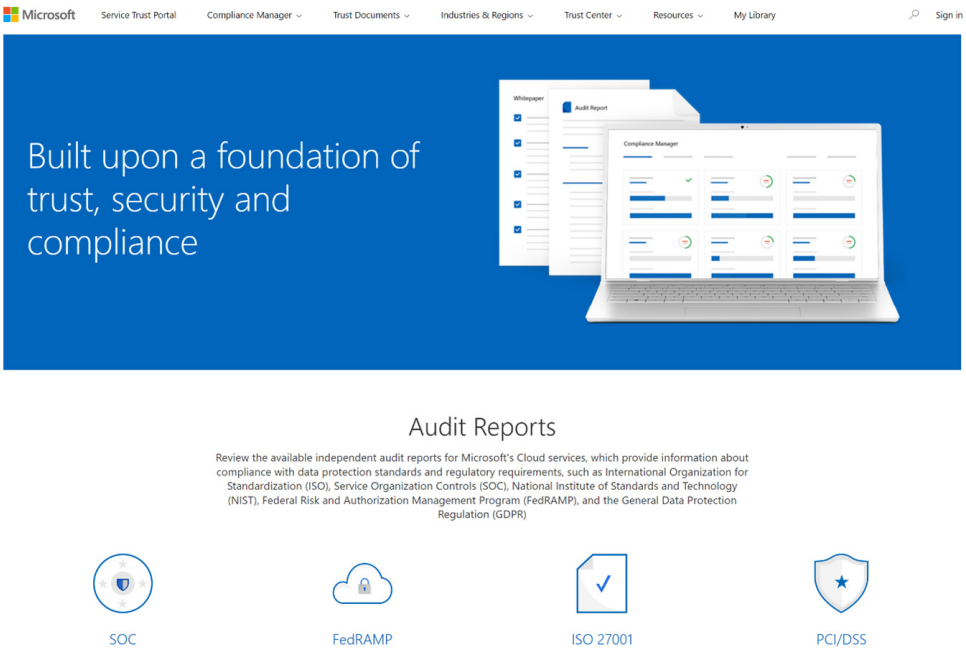


Figure 1 – Microsoft Service Trust Portal

In addition to its compliance with the ISO 27001 standard, Microsoft provides Customers with a list of top priorities for the first 30 days, 90 days, and beyond[20] to meet their requirements of ISO/IEC 27001. Please read the guide on **Cloud Governance & Security for Public Sector in Switzerland** to better understand all available options.

4.2 M2 – MICROSOFT SECURE SCORE & SECURITY COMPLIANCE TOOLKIT

A high level of basic IT security is required to meet regulatory requirements. The Microsoft Secure Score measures the security level of the business and provides guidance on improving based on best practices. In addition to that, Microsoft also provides the Security Compliance Toolkit for administrators to control and apply those recommended security configurations.

Microsoft Secure Score
Microsoft Secure Score is a tool that provides metrics, recommendations, and guidance to improve the security of your organization's Microsoft 365-related assets. Secure Score evaluates the security status of identities, devices, information, apps, and infrastructure and displays the results in a score. A concrete list of prioritized improvement actions provides details about why and how it should be improved.

The Microsoft Secure Score dashboard is the central place where organizations can control and manage security configurations in their tenant against the most current best practices. The improvement actions would be measured regularly, so customers get informed in time when a configuration does no longer meet the requirement. This could result from a configuration change or an updated best practice. Secure Score also allows authorities to accept and document risks based on their risk appetite.

20 https://docs.microsoft.com/en-us/compliance/regulatory/iso-action-plan

The Secure Score is affected by:

– How recommended security measures are configured

– How security-related tasks are performed

– Whether improvement actions have been taken using alternative solutions from third-party vendors

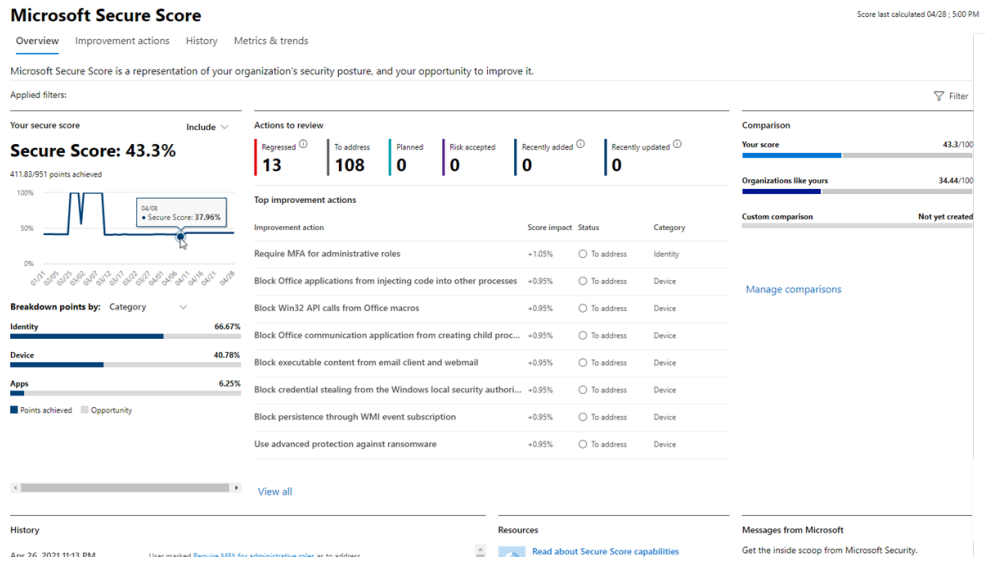


Figure 2 – Microsoft Secure Score

Security Compliance Toolkit

The Security Compliance Toolkit (SCT) is a tool that enables IT security administrators to implement recommended configuration baselines offered by Microsoft.

SCT makes it easier for IT administrators to manage the organization's Active Directory Group Policies (GPOs). Existing GPOs can be compared against Microsoft's recommended baselines and applied broadly via Active Directory, Microsoft MDM policies, or individually via local policies.

The following baselines are available:

– Windows 10 security baselines

– Windows Server security baselines

– Microsoft Office security baseline

– Microsoft Edge security baseline

4.3 M3 – MICROSOFT PURVIEW INFORMATION PROTECTION

Microsoft Purview Information Protection helps organizations classify, label, and protect data based on sensitivity.

Organizations use labels to support the following activities:

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

– Users understand the importance of information that is being handled

– Compliance officers in discovering where sensitive information lives

– Security administrators deploy data access and data loss prevention (DLP) policies based on rich label information

Microsoft Purview Information Protection (MIP) is a framework that includes several technical solutions to maintain an effective classification system to protect sensitive data across the enterprise. MIP provides a unified set of capabilities to identify the data, protect the data, and help prevent data loss across Microsoft 365 apps (e.g., Word, PowerPoint, Excel, Outlook) and services (e.g., Teams, SharePoint, and Exchange).

Azure Information Protection (AIP) is one of the components of MIP. AIP is used for information classification via labels. With AIP as the foundation, organizations can control access and use information inside and outside the enterprise.

The Microsoft Purview Information Protection components help meet regulations where data may need to be handled differently depending on its classification.

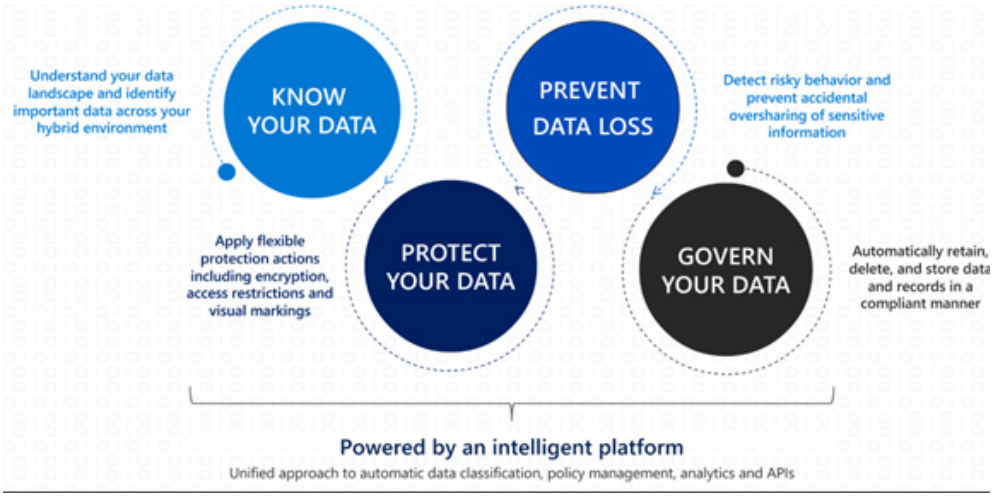


Figure 3 – Azure Key Vault

When used in combination with conditional access[21], MIP also provides opportunities to:

- Block access to sensitive content when there is a likelihood of a risky-sign in (i.e., a sign-in attempt was not performed by the legitimate owner of a user account).
- Require multi-factor login to open protected documents.
- When accessing sensitive information, devices must comply with corporate policies, such as meeting the minimum version of an operating system, being part of the domain, or meeting specific PIN or password policies.

4.4 M4 – DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

In certain situations, data protection legislation requires carrying out a Data Protection Impact Assessment (DPIA) to process data that is "likely to result in a high risk to the rights and freedoms of natural persons" (exemplary, from GDPR). Whether a DPIA is needed is a matter of how an organization uses Microsoft 365 and what kind of personal data will be processed.

Drafting a Data Protection Impact Assessment (DPIA) can be time-consuming. Although each customer's DPIA will differ based on how the organization configures and uses Microsoft 365, the customizable DPIA template[22] may save you time.

21 https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
22 https://www.microsoft.com/en-us/download/details.aspx?id=102398

Contents

Figure 4 – Template for Data Protection Impact Assessments (DPIA)

Customers can find additional information for a Microsoft 365 specific DPIA in the official documentation[23].

4.5 M5 – MICROSOFT 365 IAM & PRIVILEGED ACCESS MANAGEMENT

Having standing access by some users to sensitive information in Microsoft 365 Online Services is a potential risk for compromised accounts or internal threat activities, also called insider risk. Privileged access management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings.

Instead of administrators having constant access, just-in-time access rules are implemented for tasks requiring elevated permissions. Enabling Privileged Access Management (PAM) in Microsoft 365 allows your organization to operate with zero standing privileges and provides a layer of defense against standing administrative access vulnerabilities. Privileged Access Management requires users to request just-in-time access to complete elevated and privileged tasks through a highly scoped and time-bounded approval workflow.

Moreover, different mechanisms exist to analyze user behaviors and determine whenever a user is at risk based on previous activities, e.g., simultaneously accessing services from two distant locations. These mechanisms are part of the so-called "Identity Protection", which supports the organization in recognizing suspicious user and logon behavior, preventing unwanted access to data, and investigating accesses that pose a high risk. In this way, "Identity Protection" can contribute to compliance with certain regulations.

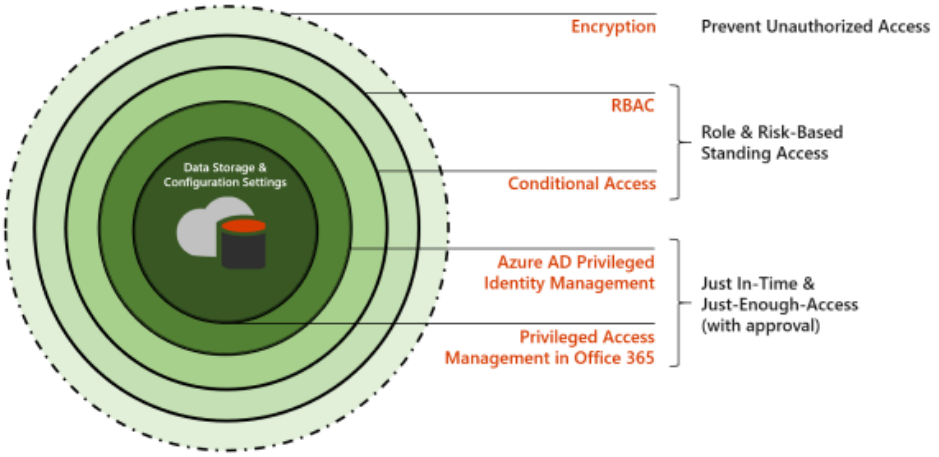


Figure 5 – Privileged Access Management in Microsoft 365

23 https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365

4.6 M6 – MICROSOFT PURVIEW COMPLIANCE MANAGER

The Microsoft Purview Compliance Manager helps simplify how you manage compliance by recommending actions to comply with industry regulations and standards, such as data protection regulations. In addition, Compliance Manager offers the following functionality:

– Assign compliance activities and track and record them

– Evaluation and prioritization of control targets

– It is a secure repository for documentation and other artifacts

– Generates detailed reports that can be provided to auditors, regulators, or other stakeholders

By providing pre-built assessments, detailed step-by-step guidance on suggested improvement actions, and a risk-based compliance score, the Compliance Manager is helping to know the compliance situation, continuously improve it, and measure the progress.

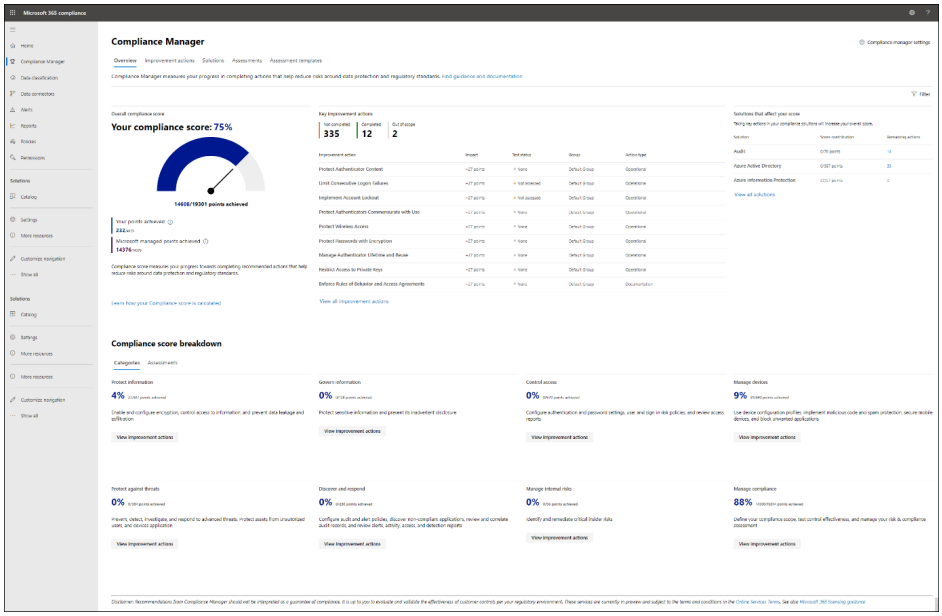


Figure 6 – Microsoft 365 Purview Compliance manager

For organizations that need to comply with multiple regulations, it can be overwhelming to know where to start. The Compliance Manager provides a comprehensive set of templates for creating assessments. These templates can help organizations comply with national, regional, and industry-specific requirements governing the collection and use of data. By using Compliance Manager, it can be seen how existing compliance meets specific regulatory requirements.

New templates are added to Compliance Manager as new laws and regulations are enacted. Compliance Manag-er also updates its templates when the underlying laws or regulations change and help with the following activities:

– Built-in assessments for industry standards and regulations

– Custom assessments to meet unique compliance needs

– Workflow functions that help the organization carry out risk assessments

– Detailed step-by-step guidance for improvement actions

– Risk-based compliance score

Customers can find a full list of assessment templates[24] in the official documentation.

The use of cloud services creates shared responsibilities between the authority and the cloud provider, known as the "shared responsibility model" (see chapter 4.13). Compliance Manager helps clarify which controls are managed by Microsoft and which lie in the customer's responsibility.

24 https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-list?view=o365-worldwide#overview

4.7 M7 – DATA SUBJECT REQUEST

Certain data protection legislation grants individuals (data subjects) who can be identified via an identifier (e.g., name, ID number, etc.) rights with respect to their personal data, such as requesting copies of personal data, requesting corrections, restricting processing, erasing data, or receiving personal data in electronic format. A formal request to take action on personal data is called a Data Subject Request (DSR). Microsoft 365 provides built-in tools for complying with a DSR.

The first step in responding to a DSR is identifying the personal data that is the subject of the request. This is done by searching the requested personal data using the Subject Rights Requests functionality in Microsoft 365.

In addition to responding to a DSR with the built-in Microsoft 365 tools, Microsoft Priva[25] offers additional complementary functionality related to investigating and servicing a DSR, such as identifying critical privacy risks and conflicts, automating privacy operations, and empowering employees to make smart personal data handling decisions.

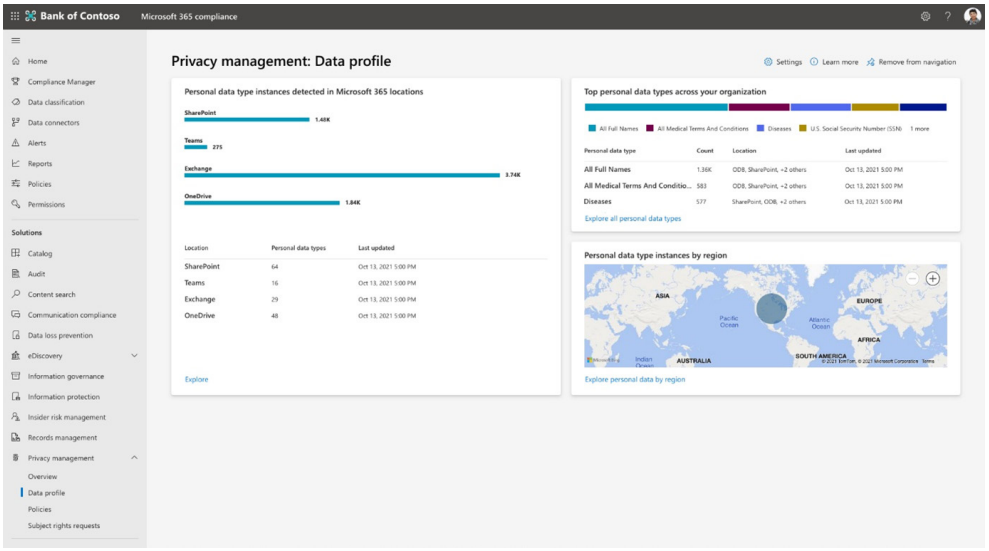


Figure 7 – Microsoft 365 Priva Dashboard

4.8 M8 – MICROSOFT PUBLIC SECTOR CLOUD DESIGN TRAINING

As a basis for the effective use of Microsoft 365 as a cloud platform, including the components and concepts presented in this guide, training measures must be provided for all involved employees.

Regardless of role in the organization (e.g., CISO or IT administrator), Microsoft Public Sector Cloud Design training provides the opportunity to drive the adoption of cloud services while working toward compliance.

In addition to deepening your knowledge of Microsoft 365 features, specialized training clarifies what implementing a software-as-a-service model means for authorities.

Figure 8 – Structure of the Microsoft Public Sector Cloud Design Training

25 https://www.microsoft.com/en-ww/security/business/privacy/privacy-management-software

Some Microsoft partners offer an introduction to Microsoft Public Cloud Design for the public sector, as well as additional training on the legal principles, specific technology capabilities of the Microsoft 365 ecosystem, and the targeted operating model. This is primarily technical support, not replacing any necessary legal review.

Foundation	Technology	Operation
– Introduction Cloud Design – Data Protection Act (nFADP) – Information Protection Ordinance (ISchV) – Information Security (ISO 27001) – Information classification	– Microsoft Purview Information Protection – Microsoft Purview Compliance Manager – Microsoft 365 Hybrid deployments – Privacy Management for Microsoft 365	– Blueprint Deployment – Conformance Analysis – Create guidelines – Set up environment – Continuous Review – Monitoring

Figure 9 – Microsoft Public Sector Cloud Design Training

This measure supports the following targets:

– Preventing incorrect manipulation

– Ensuring operational continuity

– Increase IT departments' understanding of the technologies, risks, and opportunities.

4.9 M9 – MICROSOFT PURVIEW CUSTOMER LOCKBOX

For each Microsoft 365 service, authorized administrators can use the Microsoft 365 Admin Center to submit online support requests to resolve issues. The Microsoft 365 support team fixes these issues only at the customer's request and only as long as the support ticket is open.

Almost all troubleshooting in Microsoft 365 is automated and does not require access to customer data. However, should access to the organisation's cloud environment or data be required, any Microsoft staff must follow a robust process to gain approval for access during a support case.

The additional Customer Lockbox feature for Microsoft 365 allows organizations to review and approve/reject those requests from Microsoft to access your cloud environment or data. It is also possible to assess whether the information to be shared during a support request is confidential and whether it may be viewed or not.

Access is only granted for a short time window. Afterward, it is automatically withdrawn regardless of whether the problem has been solved.

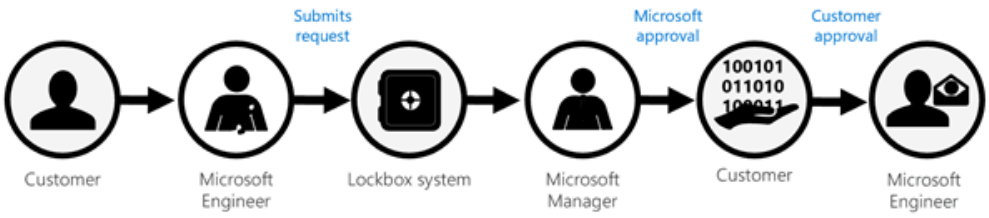


Figure 10 – Customer lockbox process

In addition, Customer Lockbox requests are saved in an audit log. This makes it possible to track when this type of request was made and whether it was accepted or refused. Through the audit log search in the Security & Compliance Center, these logs can be retrieved as needed.

This measure supports the following targets:

– Maintain confidentiality of customer data

4.10 M10 – ENCRYPTION

Encryption is an important part of the file protection and information protection strategy. Enterprises create, share, and store sensitive data on-premises, in the cloud, or across multiple clouds. Due to the nature of business and to meet regulatory requirements, sensitive data should always be securely stored and encrypted. Microsoft 365 provides solutions for encrypting disks, files, databases, and mailboxes in Office 365, both at rest and in transit.

Due to different business requirements and regulations, companies have various methods to encrypt data in the Microsoft Cloud Platform.

With Microsoft 365, multiple layers and kinds of encryption can work together to secure your data. For example, you can encrypt email messages and the communication channels through your email flows. Data is encrypted at rest and in transit, using several strong encryption protocols such as TLS/SSL, IPSec, and Advanced Encryption Standard (AES).

Per the shared responsibility model guidance, enterprise CISOs and Data Owners have the ultimate accountability to choose and implement the right encryption option to secure their data.

When an organization has any of the following requirements, it may be appropriate to use a combination of different encryption types and technologies, such as Microsoft Purview Information Protection (MIP) (see Chapter 4.3), to protect sensitive or highly sensitive information:

– Only authorized persons should be able to decrypt highly sensitive content

– Microsoft must not have access to highly sensitive data

– When keys must stay within a geographical boundary and under your control.

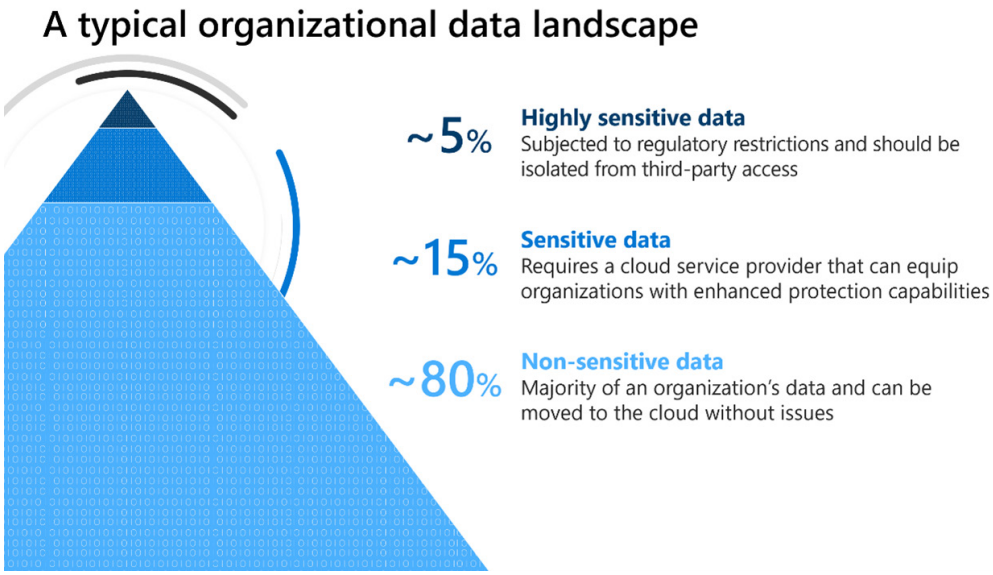


Figure 11 – Typical organizational data landscape

For this, Microsoft provides the following encryption solutions:

– Microsoft Managed Key (MMK)

– Bring Your Own Key (BYOK)

– Double Key Encryption (DKE)

These encryption solutions can help address issues related to third-country transfers, foreign legislation, or disclosure of data in criminal investigations.

Also, encryption keys can also be stored in special hardware (HSM) where Microsoft cannot access the keys. Thus, the keys can also be stored outside the cloud service itself, for example, through Double Key Encryption (DKE. DKE can be useful for handling extremely sensitive data.

However, depending on the encryption key option, the functionality of some Microsoft services may be limited (e.g., Indexing of documents or Maleware analysis). An impact assessment for each type of encryption should always be carried out before choosing.

For a full comparison[26] of the various encryption types, refer to the official Microsoft blog.

4.11 M11 – MICROSOFT 365 HYBRID WITH EXCHANGE AND SHAREPOINT

A Hybrid deployment provides organizations with an end-to-end user experience and holistic administration of on-premises services and the cloud. In addition, a hybrid deployment can serve as an intermediate step to moving completely to Office 365.

With a hybrid environment for Exchange and SharePoint, data that should not be stored in the cloud can be stored locally while still providing a seamless user experience.

Using classification and Data Loss Prevention (DLP) rules can prevent certain information from being stored in the cloud. Instead, users are directed to save that information in a local SharePoint environment.

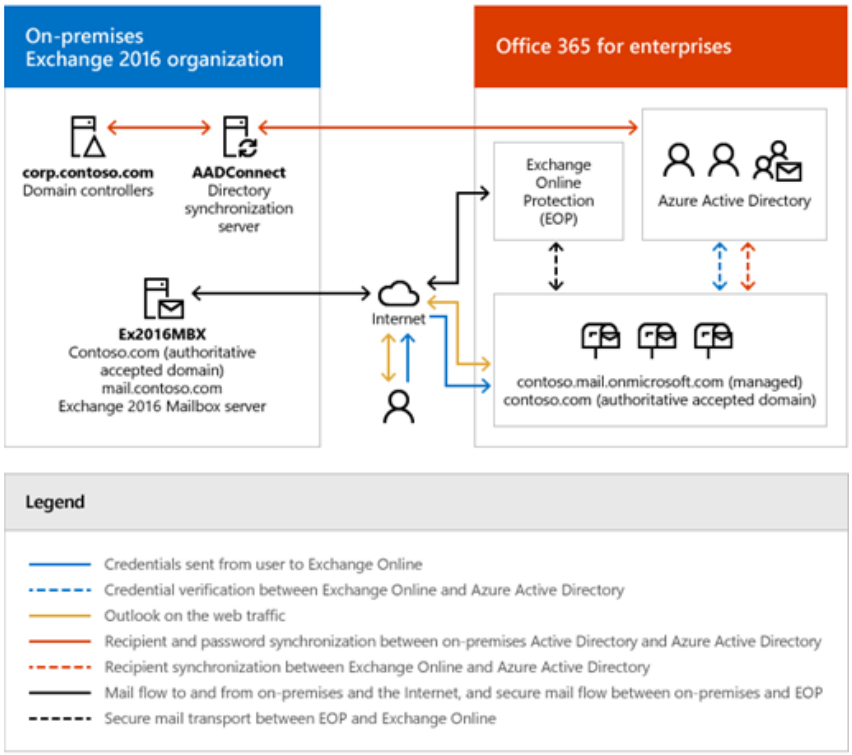


Figure 12 – Microsoft 365 Hybrid configuration for Exchange

26 https://techcommunity.microsoft.com/t5/security-compliance-and-identity/understanding-microsoft-information-protection-encryption-key/ba-p/2214589

4.12 M12 – CONTRACT

To gain the necessary understanding and insight that forms the starting point for proving this control, it is essential to know the overall structure of Microsoft cloud agreements, documentation, guidance, and, last but not least, certifications and audit reports. Here, the so-called Microsoft Assurance Framework provides the necessary overview and guidance for the audit process to be followed:

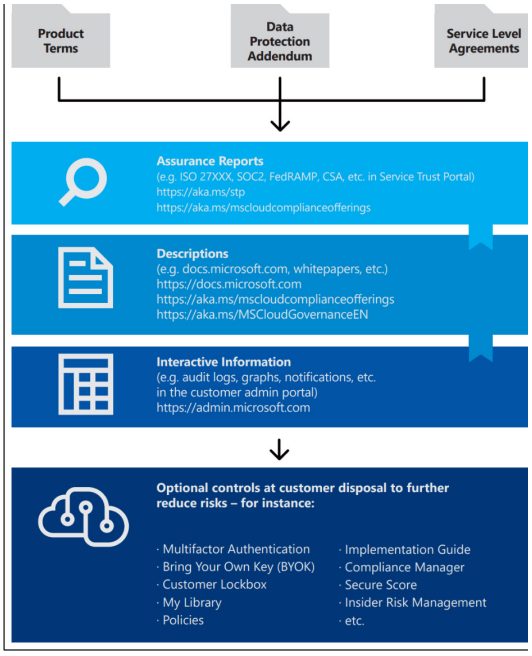


Figure 13 – Microsoft Assurance Framework

– The top level is the **contract** to be concluded **with Microsoft**. This includes, among other things, the **License Terms, which** contain the data processing agreement (for Microsoft Cloud called **Data Protection Addendum**).

– Microsoft's contractual obligations as defined in the contract can be verified using the second-level documents called **assurance reports**. In addition, customers can access all **third-party audit reports, standards compliance certificates**, etc.

– The third level comprises more detailed descriptive documentation, in which Microsoft provides **instructions and descriptions of** specific functions, features, processes, and the like. Also available are several topics- or sector-specific **white papers**, such as this document.

– Finally, customers have access to ongoing documentation and information specific to the use of Microsoft cloud services, available through a customized **cloud service management portal**.

For all these four levels, additional functions, services, and processes can be implemented for the individual customer. These can be deployed based on the overall risk assessment of the solution and data flows and thus can be included in a mitigation plan related to the identified risks that the customer wishes to mitigate.

The Microsoft Assurance Framework thus plays a critical role in creating controls at the customer site. The connection is shown in the following process model:

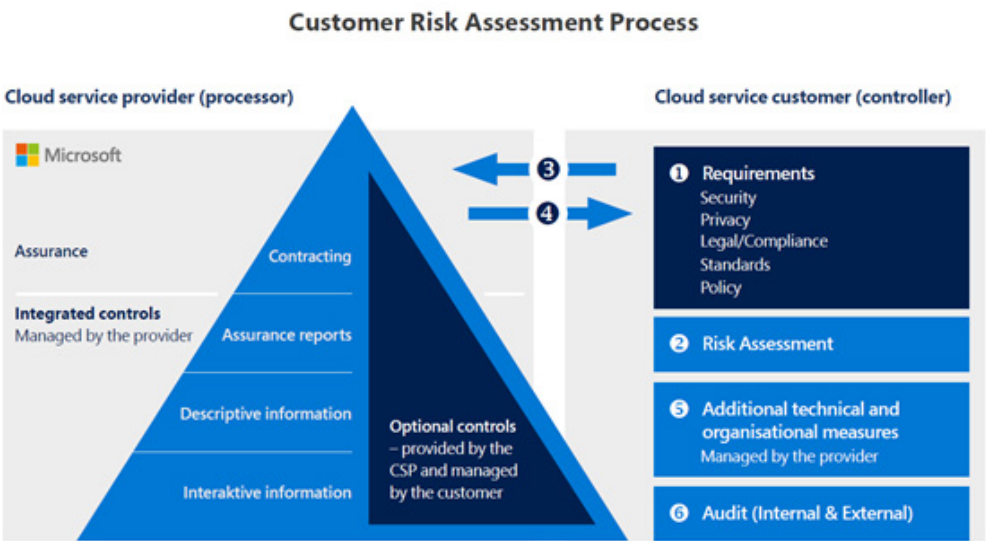


Figure 14 – Customer Risk Assessment Process

This measure supports the following targets:

– Ensuring compliance

– Restrictions on risks through guidelines

4.13 M13 – SHARED RESPONSIBILITY MODEL

The "mix" of control and interaction between the various instruments differs depending on the level of integration of the cloud solutions used. This is also reflected in the distribution of responsibility and the costs for establishing appropriate protection against certain risks (especially data protection and security).

In a cloud environment, unlike an on-premises IT infrastructure, the responsibility for implementing and maintaining security controls for IT applications is shared between the customer and the cloud provider. This is similar to a classic outsourcing scenario. However, the customer's ultimate responsibility for the processed data always remains.

In principle, modern cloud solutions follow a shared responsibility model. This divides responsibility between the customer and the cloud provider along the virtualization boundaries so that one party is primarily responsible for a particular aspect.

Figure 15 – Shared Responsibility Model

In the case of cloud solutions, there is a certain shift in the control function to the effect that the organizational/operational aspects of control become more important. Since, for example, an authority in a cloud environment has only limited ability to implement technical measures against unauthorized data access itself (because the cloud provider provides the relevant technology), the authority must fulfill its responsibility through suitable other measures. In addition to a careful evaluation of the cloud provider, regular monitoring of the effectiveness of the data protection provided by the provider could, for example, be an appropriate measure to ensure control (e.g., ongoing monitoring of accesses and access attempts via the corresponding evaluation of event logs).

To ensure the quality of the part of the shared responsibility model for which the cloud provider is responsible, Microsoft has conducted numerous security-, industry- and country-specific audits for Microsoft 365 to certify security compliance in the operation of the cloud platform by third parties. The security standards include ISO and SOC, whose audit reports are available in the Service Trust Portal.[27]

This measure supports the following targets:

– Regulate responsibilities between provider and customer

– Support for risk assessment

27 https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide

4.14 M14 – PRIVACY MANAGEMENT FOR MICROSOFT 365

An exponential increase in hybrid and remote work has caused employees to fluidly transition between work and personal activities. As a result, personal data is becoming more "mobile" and accessed across various devices and clouds, making the data susceptible to sophisticated attacks. Consequently, there are growing concerns over trust in technologies and organizations that handle personal data. Legislatures respond to such concerns by enacting regulations that protect personal data and provide consumers the right to their data, compelling organizations to make data privacy central to their business.

To respond to these challenges, Privacy Management for Microsoft 365 enables automatic and continuous identification of personal data in the customers' Microsoft 365 environment by leveraging data classification and other user information. As a result, organizations gain an overall view of their privacy situation, including the volumes, category, location, and movement of personal data within Microsoft 365 environments.

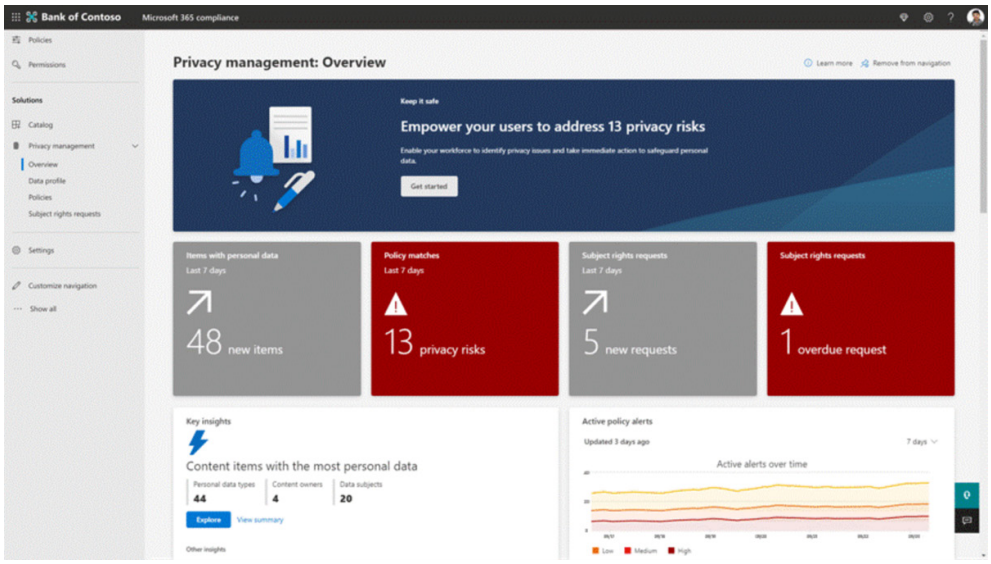


Figure 16 – Privacy Management Dashboard for Microsoft 365

Privacy Management for Microsoft 365 allows organizations to:

- Identify critical privacy risks and conflicts
- Automate privacy operations and respond to subject rights requests
- Empower employees to make informed data handling decisions

Microsoft

APPENDIX : IMPORTANT CONTRACT BASICS AND LINKS

The following table lists the main sources of transparency information related to this document.

Document or subject area	References
Microsoft Privacy Policy	https://privacy.microsoft.com/de-de/privacystatement
Data Protection Addendum for Products and Services (DPA)	https://aka.ms/dpa
Universal License Terms for Online Services	https://www.microsoft.com/licensing/terms/product/ForOnlineServices
Microsoft Business and Services Agreement (MBSA) or Microsoft Customer Agreement, or other programs depending on circumstances	MBSA: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4f5aA Customer Agreement: https://www.microsoft.com/licensing/docs/customeragreement
Technical documentation of Microsoft 365 Services	https://docs.microsoft.com/de-ch/
Microsoft Trust Center (Compliance & Security Documentations)	https://www.microsoft.com/fr-ch/trust-center
SLA documentation of all Microsoft Online Services	https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services

Table 5 – Compilation of important sources of information

Microsoft

Merci
Danke
Grazie
Engraziel