Microsoft

Microsoft Cloud Compendium

Questions and Answers

Compliance in the Microsoft Enterprise Cloud

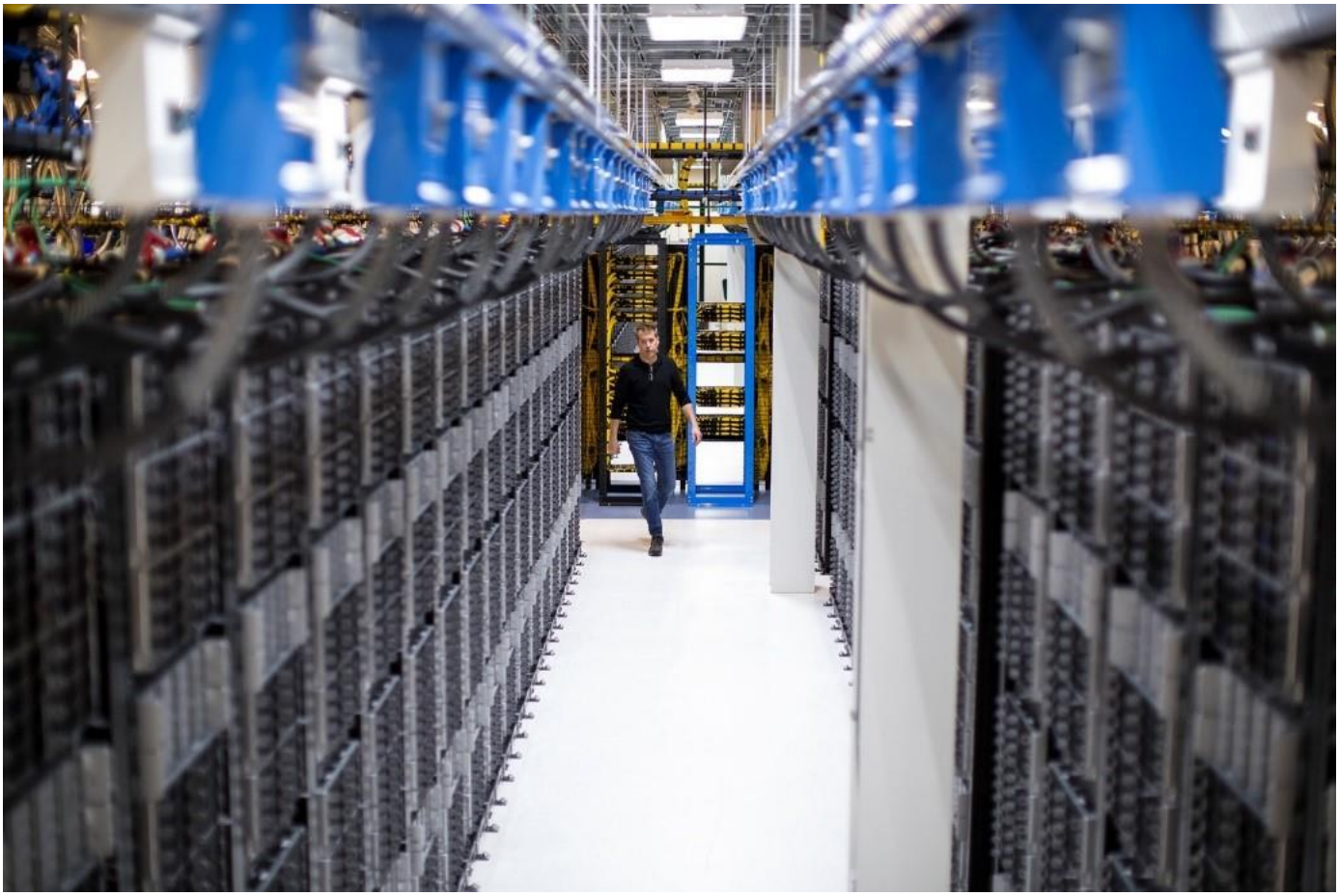
Published by Microsoft Corporate, External and Legal Affairs (CELA) Germany
Version: December 2020

Table of contents

Introduction

With this Cloud Compendium, we aim to provide answers to frequently asked questions about Microsoft Cloud Services and place them in the legal and regulatory framework.

Microsoft believes that data protection and privacy are important fundamental rights and that the General Data Protection Regulation (GDPR) is an important step forward in clarifying and supporting individual rights.



1. To what extent is data protection law relevant for customers of Microsoft Enterprise Cloud Services?

Customers may only process personal data in the Cloud if there is a legal basis. Regarding Cloud Services, such legal basis is usually found in the so called "data processing" which is reflected in Microsoft agreements (see below).

Data protection law only applies to the processing of personal data. In short, "personal data" are all information relating to an identified or identifiable natural person, such as the date of birth of a natural person or his or her e-mail address. In practice, a lot of personal data can usually be found in the Microsoft Enterprise Cloud.

2. On what legal basis does Microsoft process personal data in its Enterprise Cloud Services?

The license agreements for the use of the respective Microsoft Technology form the basis for the use of the services. In Europe, these license agreements are concluded between the customer and Microsoft Ireland Operations Limited (hereinafter, "MIOL").

The license agreements are supplemented by the "Online Services Terms" (OST) and the "Data Protection Addendum for Microsoft Online Services", Data Protection Addendum (DPA) http://aka.ms/dpa. The DPA contains in the section "Data Protection Terms", among other things, information about the processing of data, the obligations of Microsoft as well as details about security measures taken.

Furthermore, the DPA includes as Attachment 2 the standard contractual clauses (also called "EU Standard Data Protection Clauses"), which are concluded between the customer and Microsoft Corporation. The standard contractual clauses were adopted by the EU Commission in 2010. By concluding the standard contractual clauses, Microsoft Corporation is obligated to comply with the EU data protection standards and also to impose these standards contractually on any sub-contractors.

3. What has changed for international data traffic as a result of the European Court of Justice ("ECJ") ruling in the "Schrems II" case on July 16, 2020?

According to the GDPR, a legal basis is required for the lawful transfer of data from the EU to so-called third countries (such as the USA). There are several possibilities for this, including the aforementioned EU standard contractual clauses. The EU-U.S. Privacy Shield could also legitimize data transfers to the USA. It is an adequacy decision based on an agreement between the EU and the U.S. government, under which U.S. companies can voluntarily commit to comply with the EU data protection standards set forth in the agreement. The European Court of Justice ("ECJ"), in its July 16, 2020 ruling in the "Schrems II" case, has declared the EU-US Privacy Shield invalid with immediate effect. As a result, all data transfers that continue to be conducted solely on the basis of the Privacy Shield are no longer permissible. However, according to the ECJ ruling, the EU standard contractual clauses continue to be valid. Nevertheless, the ECJ considers further measures in addition to the standard contractual clauses to be necessary, where appropriate, in order to establish an adequate level of data protection in the third country.

4. What has Microsoft done in response to the ECJ's ruling in the "Schrems II" case?

In response to the invalidity of the EU-US Privacy Shield resulting from the ruling, Microsoft has made adjustments to the DPA, subjecting all data flows therein to the standard contractual clauses. As further measures to protect personal data, Microsoft has already implemented encryption for data in transit and at rest and, in accordance with the provisions of the OST and the DPA, stores most customer data at rest in the region. In addition, Microsoft has already responded to the European Data Protection Board's November 11, 2020 recommendations for action with the following commitments: First, Microsoft commits to challenge any request by a government entity for enterprise or public sector customer data where there is a legal basis to do so. This comprehensive commitment goes beyond the proposed recommendations of the European Data Protection Board. Second, Microsoft will financially compensate customers' users if Microsoft is required to disclose their data in response to a request from a government agency in violation of the EU General Data Protection Regulation (EU GDPR). This commitment also goes beyond the recommendations of the European Data Protection Board. In doing so, Microsoft is demonstrating its confidence that it can protect the data of enterprise and public sector customers and will not expose them to inappropriate disclosure. Microsoft calls these protections "Defending Your Data". Microsoft will immediately begin including them in our contracts with enterprise and public sector customers.

5. Why are there still references to the Privacy Shield in the DPA?

References to the EU-US Privacy Shield remain in the DPA, but Microsoft no longer relies on the Privacy Shield as a legal basis for transferring data to third countries in light of the "Schrems II" ruling. The U.S. Department of Commerce has announced that it will maintain the Privacy Shield regime in the United States. Microsoft has made a commitment to the U.S. Department of Commerce to comply with the Privacy Shield terms and will therefore continue to operate in a Privacy Shield-compliant manner - in addition to the standard contractual clauses - although this transfer mechanism will no longer serve as the legal basis for data transfers.

6. Do the contractual relationships change if the Cloud Services are used by different group companies of the customer?

The Enterprise Cloud Services may be procured by a central group company, e.g. by the IT-service company of the corporate group. The license agreement will be concluded between this group company and MIOL. On customer's side, the Data Processing Agreement and the EU standard contractual clauses should be signed by all group companies which are using the services. From the viewpoint of the data protection authorities, these group companies are the responsible "data controllers" which must have a direct contractual relationship with the non-EU-domiciled Microsoft Corporation. Microsoft offers a supplemental agreement for this purpose.

7. What is the content of the contractual relationships when enterprises, particularly Microsoft Partner, use a Microsoft platform such as Microsoft Azure and offer the services to their customers based on such platform?

Within the so called "platform as a service" (PaaS), the structure of the agreement depends on the specific case. If the Microsoft Partner plans to offer applications, which are developed by the Partner as a service, the Partner may

want to consider not to incorporate any performance obligations in its contractual terms that exceed those the Partner has agreed with Microsoft.

8. Where is data stored in the Microsoft Enterprise Cloud?

Microsoft is continuously developing its cloud strategy and offers a comprehensive range of its global cloud solutions made up of local cloud data center regions. The geographic area (so-called Geo) that the administrator first chooses when initially setting up the services determines the storage location for the resting customer data ("data at rest").

You may find further information at: https://www.microsoft.com/en-us/trust-center/privacy/data-location, resp. https://www.microsoft.com/en-us/trust-center/privacy/customer-data-definitions.

9. Is there any communication between Microsoft and the data protection authorities?

Yes. Microsoft has sought dialogue with the national data protection authorities of the EU member states long before the GDPR came into force. There continues to be an ongoing exchange.

10. Does Microsoft disclose customer data to US authorities?

In case Microsoft receives an order to disclose data, Microsoft will not provide any data to the authorities but will directly refer the requesting authority to the customer. However, should the authority still require Microsoft to disclose data, Microsoft will comprehensively examine this request for disclosure from a legal point of view and, if legally required, comply with the request (see also Microsoft's protective measures "Defending Your Data" under section 4 of the Cloud Compendium).

11. What is the relevance of the American CLOUD Act?

Under the "Clarifying Lawful Overseas Use of Data Act" ("CLOUD Act"), U.S. law enforcement agencies can obtain information from U.S. service providers and their subsidiaries on the basis of investigation orders.

The CLOUD Act serves the investigation of crimes and in principle, does not change the processes and requirements for requests for information from law enforcement agencies. It provides a legal framework for resolving conflicts of law by enabling the United States and encouraging foreign governments to conclude bilateral agreements on dealing with requests in cross-border investigations.

Whereas the CLOUD Act creates new rights under new international treaties, the cloud service providers still have the right to go to court in the event of a conflict of laws to verify the legality of search warrants. If cloud service providers challenge investigation orders on the legal ground of a violation of a state's national laws, this may lead to the repeal of the investigation order. Nevertheless, the CLOUD Act states to the competent US courts that the violation of foreign law alone does not lead to annulment. Rather, the courts must make an overall assessment, which

in consequence can lead to the prosecution authority's prevailing interest in the (unchanged) maintenance of the investigation order.

Further details on the CLOUD Act can be found here: https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow.

12. What are the consequences of the CLOUD Act for Microsoft?

To continue to protect the privacy of its business customers in the future, Microsoft complies with the following five principles:

- Microsoft will continue to refer US authorities to the respective business customers instead of providing data to the authorities by choice.
- Microsoft will continue to go to court to defend the local rights of our customers if their rights are violated by the U.S. government.
- Microsoft will continue to push for new international agreements that strengthen the rights of our customers.
- Microsoft will continue to be transparent about the number of international search warrants we receive.
- Microsoft will continue to offer our customers several options for storing their data.

13. How many requests for data does Microsoft receive from investigating authorities?

Microsoft informs half-yearly about the number of world-wide official investigation requests on its website since many years. You can find these so-called Trust Reports under the category "Digital Trust Reports" here https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report. In this context, it is also worth mentioning the FAQs, which deal in more detail with the number of investigation requests relating to "Enterprise Cloud Customers". You can find them under the above-mentioned link.

14. Can Microsoft Cloud Services be used by persons subject to professional secrecy?

Yes. Section 203 of the German Criminal Code permits the disclosure of secrets entrusted to persons subject to professional secrecy (e.g. doctors, psychologists or lawyers) to other persons involved, e.g. external IT service providers. However, this shall apply only if no more professional secrets are disclosed than necessary for the use of the service provider and the service provider was obligated to maintain secrecy. An organizational integration into the sphere of the person who is subject to professional secrecy is not necessary.

This allows the use of supporting IT services, such as the provision and support of IT systems and applications, as well as the use of cloud applications by persons subject to professional secrecy. Microsoft offers an additional agreement for this purpose.

15. How does Microsoft deal with encryption?

In answer to reports on the access to data lines by the intelligence services of various countries, Microsoft transfers data between its data centers exclusively in an encrypted way. Microsoft also implemented the encryption of data on its servers for particular Enterprise Cloud Services in late 2014. Microsoft complies with the Cloud Computing Requirements Catalog (C5) of the German Federal Office for Information Security (BSI), which addresses the topic of cryptography and key management in detail. A link to the requirements catalog and further information on the topic can be found at: https://news.microsoft.com/de-de/microsoft-erfuellt-den-anforderungskatalog-cloud-computing-c5-des-bsi-fuer-mehr-als-100-seiner-weltweiten-rechenzentren/

16. How can customers fulfill their obligation to assess the compliance with all agreed technical and organizational measures?

Customers are obligated by data protection law to assess the implementation of the technical and organizational measures for the protection of personal data by the order processor when conducting an order processing. Customers can meet this obligation by having presented certificates from independent third parties. Therefore, Microsoft is audited by third parties every year. Such audits are conducted by internationally recognized auditors, who check whether Microsoft is ensuring the policies and procedures for security, data protection, continuity and conformity. This is based on the ISO 27001 standard, which is one of the world's best security-comparison-benchmarks. Microsoft provides its customers with audit reports in accordance with ISO 27001 upon request.

Moreover, Microsoft has been certified in accordance with the international ISO/IEC 27018 standard for data protection in the Cloud, as the first leading provider of Cloud services.

The ISO/IEC 27018 standard, which is an extension of the previously mentioned ISO 27001 standard, was developed by the International Organization for Standardization (ISO) to create a uniform and internationally valid concept to protect personal data stored in the Cloud. The British Standards Institution (BSI) has independently verified that Microsoft Azure, Office 365 and Dynamics 365 are in compliance with the "Codes of Practice" for the protection of personal data in Public Clouds. In addition, this test was conducted for Microsoft Intune by Bureau Veritas.

These certificates are stipulated contractually in the Microsoft Online Services Terms (for the ISO/IEC 27018 standard since April 2015), but do not alter the rights given by the EU standard contractual clauses or the GDPR. You can find an overview of the ISO standards and other certifications, including different SOC control standards for the Microsoft Cloud at https://www.microsoft.com/de-de/cloud/iso-standards-und-zertifikate.aspx and https://docs.microsoft.com/en-us/compliance/regulatory/offering-SOC

17. How can the customer store data securely for revisions?

Microsoft stores data geo-redundantly in several locations in various data centers. Accordingly, no back-ups are necessary in order to restore lost data. If the customer requires a reproduction of historical data, the customer must use an archiving solution in addition to the Microsoft Cloud Service. The customer can adjust the archiving functions in the respective product to his needs and set and configure them himself.

18. For what purposes does Microsoft process data to pursue legitimate business activities of Microsoft??

Microsoft acts as a processor for the majority of data processing activities. To a limited extent, Microsoft also processes data as an independent data controller.

Microsoft processes data for legitimate business activities as an independent data controller solely for the following six purposes as defined in the DPA: (1) billing and account management; (2) remuneration (e.g. calculating employee commissions and partner incentives); (3) internal reporting and modeling (e.g. forecasting, revenue, capacity planning, product strategy); (4) combating fraud, cybercrime, or cyberattacks that may affect Microsoft or Microsoft products; (5) improving core functionality related to accessibility, data protection, or energy efficiency; and (6) financial reporting and compliance with legal obligations (subject to the disclosure limitations described in the DPA).

19. Does Microsoft also process data for advertising when processing for legitimate business activities?

No, when processing data for legitimate business activities as an independent data controller, Microsoft does not process data for user profiling, advertising, or similar commercial purposes. Data is processed solely for the purposes set out in the answer to question 18.

20. Why is Microsoft an independent data controller when processing data for legitimate business purposes?

When processing data for legitimate business purposes, Microsoft determines both the means and the purposes of the data processing. Thus, Microsoft is solely responsible for compliance with all applicable laws as well as the fulfillment of its obligations as a data controller for such data processing.

21. What other regulatory requirements can be applicable in addition to the data protection law?

Other regulatory requirements cannot be conclusively listed here. In practice, for example, sector-specific requirements such as in the financial services sector can apply. In accordance with the general bookkeeping principles under commercial and tax law, proper treatment of electronic documents and orderly access to data are particularly required (German Principles for Orderly Management and Storage of Books, Records and Documents in Electronic Form and for Data Access; GoBD). A crucial point in this regard is the internal controlling system ("Internes Kontrollsystem" "ICS").

To document a functioning ICS, which detects developments that could jeopardize an enterprise at an early stage, Microsoft offers customers, respectively their independent auditors, a certificate in accordance with the internationally accepted audit standard ISAE 3402. If a customer stores data, relevant for tax purposes, exclusively in Microsoft's Enterprise Cloud at data centers within the EU, the customer must also have an approval for this by the competent German tax authority.

Further up-to-date information

- Microsoft Trust Center
  https://www.microsoft.com/en-us/trust-center
- New measures to protect your data, blog post of November 20, 2020
- Encryption in the Microsoft Cloud
  Encryption in the Microsoft Cloud - Microsoft 365 Compliance | Microsoft Docs
- Overview of Azure encryption und Azure Backup Service
  Azure encryption overview | Microsoft Docs
  What is Azure Backup? - Azure Backup | Microsoft Docs
- Data protection and Compliance
  https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview

  https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview
- Data protection with Windows 10 and Microsoft 365 White Paper
  aka.ms/DatenschutzMicrosoft365
- Trust Center
  https://www.microsoft.com/de-de/trustcenter/CloudServices/office365/default.aspx
- Diagnostic data
  https://blogs.microsoft.com/on-the-issues/2019/04/30/increasing-transparency-and-customer-control-over-data/
- Microsoft Azure Trust Center

  Trust your cloud | Microsoft Azure
- Dynamics Trust Center
  https://www.microsoft.com/de-de/trustcenter/privacy/dynamics365-operations-location
- Transparency reports
  https://www.microsoft.com/en-us/corporate-responsibility/reports-hub
- Navigating your Way to the Cloud in Europe – A compliance guide for cloud decision makers
  https://www.microsoft.com/en-ie/lcc_cloud/default.aspx

Legal Note

This compendium contains a general overview of questions that our customers frequently ask while using Cloud Computing Solutions. It shall enable you to better understand the legal background of using cloud computing solutions. This compendium is not to be understood as a case-by-case examination of individual legal matters. You must therefore seek separate legal advice for an individual and conclusive legal assessment of the permissibility of the use of Microsoft cloud solutions in a specific case.

Microsoft Deutschland GmbH, Walter-Gropius-Str. 5, 80807 München

Photo sources: own