Microsoft

Microsoft Cloud Compendium

Questions and Answers

Compliance in the Microsoft Enterprise Cloud

Revision: January 2016

Compliance in the Microsoft Enterprise Cloud

Published by Microsoft Switzerland Ltd Liab. Co
Revision: January 2016

Where does the Microsoft Enterprise Cloud store its data?

By default, the core customer data of the Microsoft Enterprise Services (Microsoft Office 365, Microsoft Azure, Microsoft Dynamics CRM Online, Microsoft Intune) for Swiss customers are stored in the Microsoft data centres in Dublin and Amsterdam. As far as the data centres are concerned, Microsoft pursues a strategy that is aligned with the regions. The country or region of the customer that the administrator enters when setting up the services for the first time determines the primary storage location for the customer's data. Further information is available under the following link:
https://www.microsoft.com/enus/TrustCenter/Privacy/You-are-in-control-of-yourdata#_You_know_where

In individual cases, the requirements for the provision of the services may require certain data to be made accessible to employees or suppliers of Microsoft outside the primary storage region. Moreover, the employees with the greatest technical experience in handling special service problems may be based at locations other than the primary location, and these employees may need access to systems or data in order to solve a particular problem.

To what extent is data protection law relevant to customers of Microsoft Enterprise Cloud Services?

Customers may only process personal data in the cloud if legal permission exists to do so. For Cloud Services, a permission is usually derived from the external data processing as specified in Microsoft's contracts (see below).

Data protection law only applies to the processing of personal data. In summary, this includes all details of an identified or identifiable natural or legal person, e.g. the name/company of a person or its e-mail address. Usually, the Microsoft Enterprise Cloud contains a lot of personal data. However, there are also cases in which hardly any personal data or none at all are processed, e.g. design data of a fashion manufacturer that are stored in Azure.

Currently, Microsoft does not have any data centre in Switzerland. Can a Swiss customer still use Microsoft Enterprise Cloud Service in compliance with data protection regulations?

Yes. In terms of data protection law, data centres in EU countries correspond to those in Switzerland, as these countries ensure an adequate data protection level. From the data protection perspective, it is thus irrelevant whether a data centre is located in Switzerland or in the EU. As far as data protection law is concerned, a data centre in Switzerland does not provide greater advantages than a data centre in the EU. Microsoft offers its customers the EU standard contractual clauses for the portion of the services that Microsoft performs outside the EU. The Federal Data Protection and Information Commissioner (FDPIC) is of the opinion that these clauses represent an adequate data protection solution for this purpose.

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

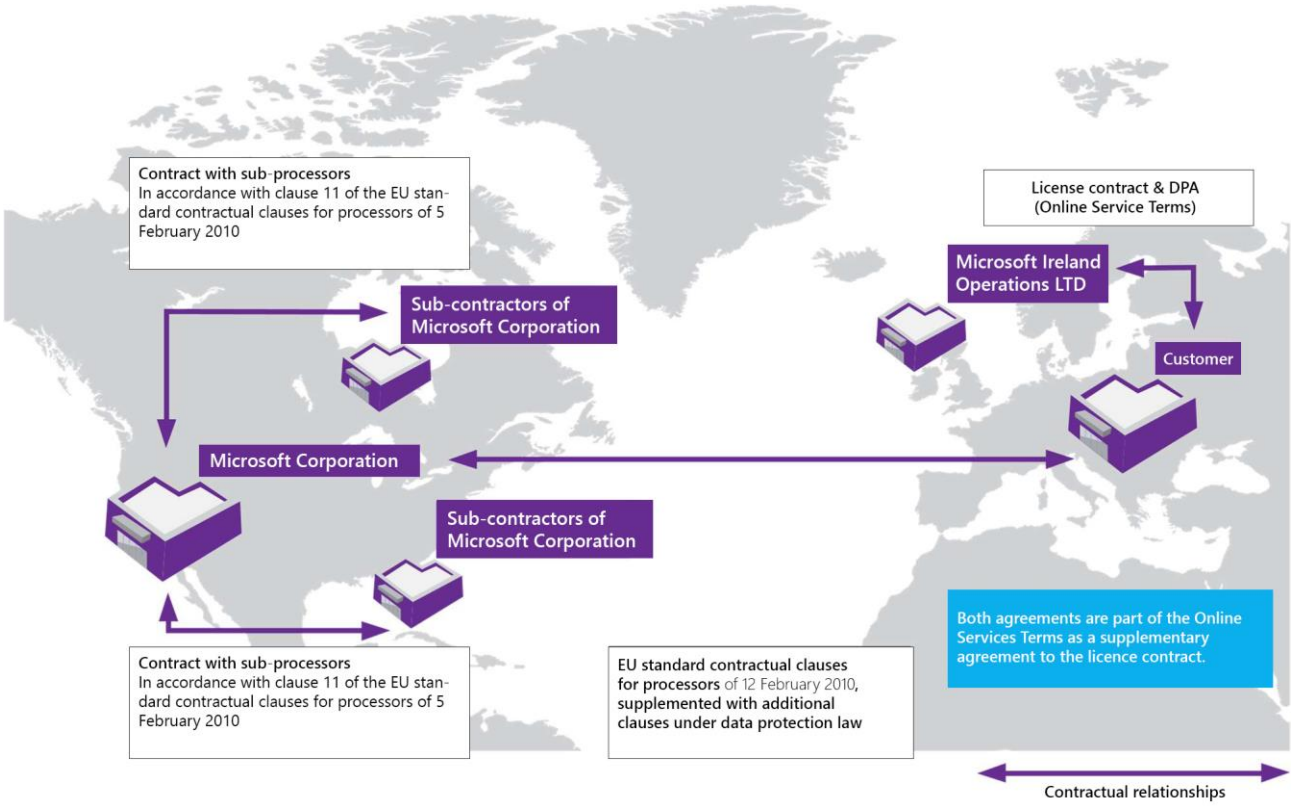
The service relationship is based on the licence contracts for the use of the respective Microsoft technology. These agreements are concluded between the customer and Microsoft Ireland Operations Limited (hereinafter referred to as "MIOL"). The licence contracts are supplemented by the Online Services Terms (OST) (current version: http://aka.ms/Wkcowi). Among other things, the "Data Processing Terms" section of the OST contains the statutory regulations for external data processing (pursuant to Art. 10a of the Federal Act on Data Processing of 19 June 1992 (hereinafter referred to as "DSG")).

Attachment 3 to the Online Services Terms contains the EU standard contractual clauses, which are concluded between the customer and Microsoft Corporation.

EU standard contractual clauses were adopted by the European Commission and are recognised by the Federal Data Protection and Information Commissioner (FDPIC). Additionally, Microsoft submitted the Online Service Terms (OST) for review by the FDPIC. The OST were deemed as satisfactory contractual guaranties for the forwarding of data abroad (acc. Art 6 §2 lit. a DSG).

If these clauses are used without modification, the forwarding of personal data to other countries, including but not limited to the USA, is permitted under data protection law. In this way, Microsoft Corporation is under the obligation to comply with EU data protection standards and to contractually impose them upon any sub-contractors.

The contractual concept is structured as follows:



Does anything change in the contractual relationship if the cloud services are used by different group companies of the customer?
The services can also be used by a central group company, e.g. by the group's IT service company. The licence contract is concluded between this group company and MIOL.

What is the content of the contractual relationship when companies use a Microsoft platform such as Microsoft Azure and offers services to their customers on this basis?
In the case of a Platform as a Service (PaaS), the contract details depend on the individual situation. If the Microsoft partner wants to offer the applications developed by him as a service, the performance obligations that he promises in his contractual terms should not exceed those agreed with Microsoft.

Have Microsoft's Enterprise Cloud contracts been coordinated with the authorities responsible for supervising the data protection?
As Microsoft makes use of the EU standard contractual clauses when forwarding personal data to countries outside Switzerland and the EU, an appropriate data protection level is always on hand. However, the customer must generally inform the FDPIC of the use of such EU standard contractual clauses.

What role does the Safe Harbour certification by the Microsoft Corporation play for Swiss customers?
On 6 October 2015, the European Court of Justice declared the EU-US Safe Harbour certification to be invalid for the EU. Therefore, no appropriate data protection level for the data protection-compliant transmission of personal data to the USA currently exists. The FDPIC has also adopted this view in principle. For this reason, Microsoft makes use of the EU standard contractual clauses for the transfer of personal data to countries outside Switzerland and the EU.

Can US authorities access the data of the customers in the Microsoft Cloud?
Microsoft does not grant any government authority direct or unlimited access to customer data, except under a judicial decision. Furthermore, Microsoft will, whenever possible, first refer the requesting authority to the customer.

Microsoft has announced that it will exhaust all legal remedies should a US authority demand direct surrender of the content data stored in the data centres in the EU.

Until the preparation of this document, Microsoft has never been under the obligation to disclose the data of a Swiss enterprise customer by virtue of a U.S. National Security Order.

Moreover, Microsoft only transmits data between its data centres in encrypted form.

Details are available here:

http://blogs.microsoft.com/on-the-issues/2015/04/09/our-legal-challenge-to-a-us-government-search-warrant/

http://digitalconstitution.com/

May sensitive data (e.g. health data) be processed?

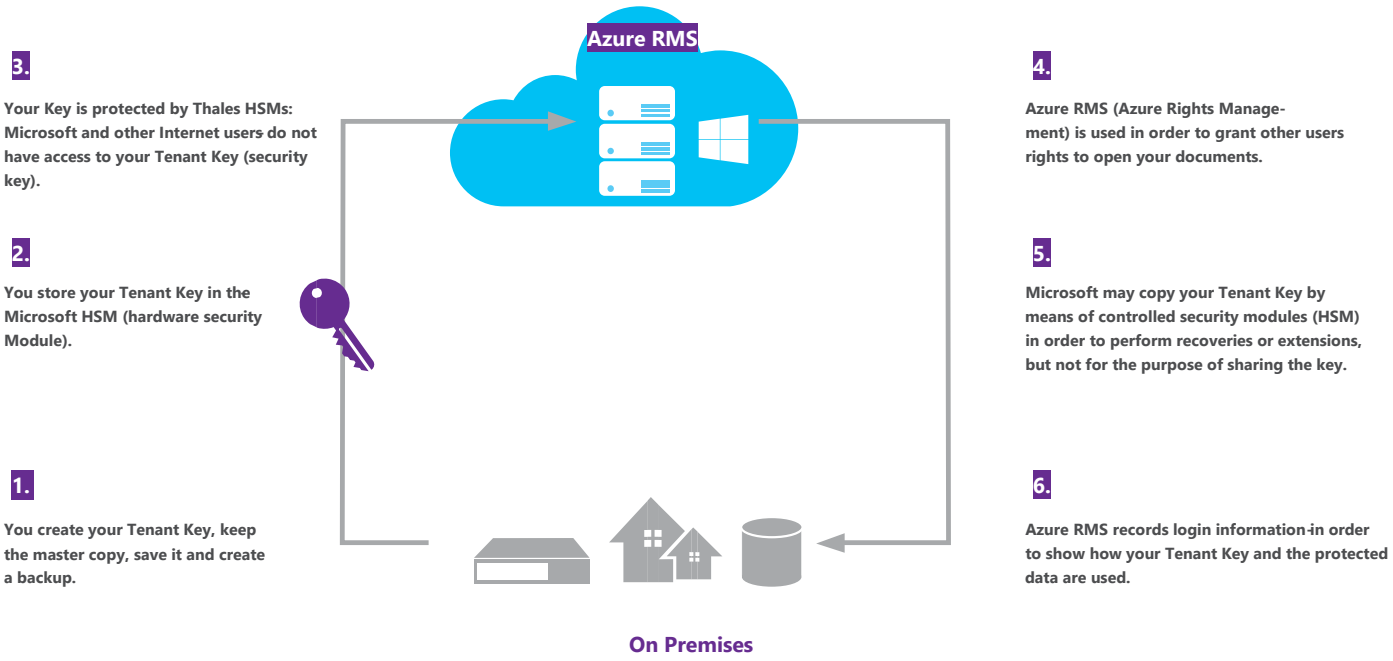
Yes. According to Art. 3 lit. c of the Federal Act on Data Protection (FADP), sensitive data are data on religious, ideological, political or trade union-related views or activities, health, the intimate sphere or the racial origin, social security measures and administrative or criminal proceedings and sanctions. These are subject to special protection and may, as a matter of principle, only be processed and forwarded or forwarded for the purpose of external data processing with the consent of the subject. This applies even if the service provider is active outside the EU. Apart from the fact that the service provider must have an appropriate data protection level, the FADP does not make any distinction between the requirements for the commissioning of service providers in Switzerland and the EU and those outside Switzerland and the EU. However, in addition to a data processing agreement for the forwarding of personal data to countries outside Switzerland and the EU, contractual guarantees must exist for an appropriate data protection level. To do this, Microsoft makes use of the EU standard contractual clauses for processors, which are recognised by the FDPIC.

Can the applicability of data protection law be excluded through encryption?

This mainly depends on the type of encryption. If encryption is applied both on the transport route between the customer and Microsoft and to the data stored in the cloud, and the customer alone has the key, no transmission of personal data is on hand. Thus, Microsoft enables its customers to use their own key for the encryption of data in Windows Azure Rights Management. In this context, the key is protected by a Thales hardware security module (HSM), so that Microsoft cannot export and share the key. Such encryption would exclude the personal reference of data, but might limit the functionality, e.g. the search function.

However, as there will always be non-encryptable data such as the admin data and the metadata, data protection law must be observed. In any case, encryption represents a type of protection that is approved under data protection law.

When the customer uses his own key, the protection works as follows:



Graphic presentation of the protection mechanism when using your own customer key

How can customers comply with their obligation to ensure observance of all technical and organisational measures according to the FADP?

In the case of external data processing, customers are under the obligation imposed by data protection law to verify the implementation of the agreed and statutory technical and organisational measures for the protection of the personal data. Generally, customers can comply with this obligation by requesting certificates of independent third parties. For this reason, Microsoft submits to yearly third-party audits. These audits are conducted by internationally accredited auditors, who check whether Microsoft observes applicable security, data protection, continuity and compliance guidelines and procedures. This is done on the basis of the ISO 27001 standard, one of the best global security reference benchmarks. On request, Microsoft provides its customers with a summary of the audit report according to ISO 27001.

Microsoft also complies with the ISO/IEC 27018 standard for data protection in the cloud.

The ISO/IEC 27018 standard, an extension to the above-mentioned ISO 27001 standard, was developed by the International Organization for Standardization (ISO) for the purpose of establishing a uniform, internationally valid concept for the protection of personal data stored in the cloud.

The British Standards Institution (BSI) has independently verified that Microsoft Azure, Microsoft Office 365 and Microsoft Dynamics CRM Online comply with the code of practice for protection of personally identifiable information (PII) in public clouds. Additionally, Bureau Veritas has conducted this test for Microsoft Intune.

The audits are contractually agreed in the Microsoft Online Services Terms (OST), but do not modify the rights under the EU standard contractual clauses.

http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/

How can the customer store his data in an audit-proof manner?

Microsoft stores the data geo-redundantly in several places in two different data centres. Accordingly, no backups are required for recovery purposes in the event of loss of data. If the customer needs a copy of historical data, he must use an archiving solution in addition to the Microsoft Cloud Service.

Which other regulatory requirements may apply apart from data protection law?

It is impossible to provide an exhaustive list of requirements in this document. Hence, the following explanations do not claim to give a complete overview.

For example, sector-specific requirements may apply, e.g. in the financial service or health industry. In particular, any statutory confidentiality obligations must be observed in these areas. Nevertheless, neither professional secrecy nor the various special secrecy obligations (e.g. bank client secrecy or the non-disclosure obligation in the field of social security and health insurance) render the storage in the cloud categorically impossible. Rather, the customer is responsible for evaluating, considering and ensuring compliance with the required detailed statutory and regulatory conditions for the storage in the cloud in his industry.

In the field of financial services, the Swiss Financial Market Supervisory Authority (hereinafter referred to as "FINMA") has issued a circular outlining principles for the outsourcing of business areas, which also includes the external storage of data. Especially when outsourcing overseas, it must be ensured that the customer's audit firm under banking and stock exchange law and the FINMA can exercise their audit rights. Furthermore, different requirements must be fulfilled depending on the customer's confidentiality obligations. Microsoft provides various solutions in order to accommodate the customer's confidentiality obligations, e.g. encryption as already described above.

The situation is similar in the insurance field, which is also subject to a statutory non-disclosure obligation. In contracts with Microsoft, the non-disclosure obligations are thus expanded to include the employees of Microsoft. In conjunction with other contractual components (such as the EU standard contractual clauses), the data can thus be stored externally in compliance with data protection law. Moreover, the customer can encrypt the data in such a way that only the customer has access to them.

From the perspective of data protection law, it is possible to store health data in the cloud. However, specific confidentiality obligations must be considered for the health sector (e.g. professional secrecy obligation), and different solutions may be appropriate depending on the statutory regulations. Microsoft enables the encryption of patient data in such a way that only the customer has access to such, thereby preventing the risk of disclosure in breach of the statutory confidentiality obligations and the Federal Act on Data Protection (FADP).

According to the general accounting principles of commercial and tax law, accounts and records may be kept electronically. In this connection, the only exceptions are the annual report and the audit report, which must be kept in writing and signed. Moreover, the Federal Tax Administration is of the opinion that VAT-relevant documents may be kept in electronic form, but must in this case be signed with an electronic signature.

Further topical information is available here:

- Microsoft Trust Centre for all services
  https://www.microsoft.com/en-us/TrustCenter/default.aspx

- Microsoft Office 365 Trust Center
  https://products.office.com/en-us/business/office-365-trust-center-welcome

- Microsoft Azure Trust Center
  https://azure.microsoft.com/en-us/support/trust-center/

- Microsoft Dynamics Trust Center
  https://www.microsoft.com/en-us/trustcenter/CloudServices/Dynamics

- Microsoft's Challenge to U.S. Search Warrant /NSA
  https://blogs.technet.microsoft.com/microsoft_on_the_issues/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction/

  http://blogs.microsoft.com/on-the-issues/2014/06/04/unfinished-business-on-government-surveillance-reform/#sm.00003eynio15l9fsjt0rko0291oyg

  http://blogs.microsoft.com/blog/2014/12/15/business-media-civil-society-speak-key-privacy-case/#sm.00003eynio15l9fsjt0rko0291oyg

This overview does not claim to be complete. It does not represent legal or tax advice.

Image sources: Own images, shutterstock_78032764, bartzuza