How to conduct

Transfer Impact Assessments

v. 01-2024

This document is for information purposes only. It summarizes information about the current product offerings of ATOSS Software AG and its affiliated companies (hereinafter "ATOSS"), which may be amended and updated from time to time. The current version of this document is available for download in our ATOSS customer web lounge (ATOSS customer web lounge) (see section "Data Protection").

The statements in this document do not constitute any binding commitments, assurances or warranties on the part of ATOSS and its sub-processors or licensors. Furthermore, they do not replace any (data protection) legal advice to the customer. The information in the contract documents relating to the specific ATOSS Product applies.

Notwithstanding the foregoing, ATOSS would like to draw the customer's attention to relevant information regarding the performance of a transfer impact assessment (hereinafter: "TIA") for ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services in light of the "Schrems II" ruling of the Court of Justice of the European Union and the recommendations of the European Data Protection Board (hereinafter: "EDPB"). See EDPB recommendations

Foreword - The responsibility for data transfers

The purpose of the General Data Protection Regulation ("GDPR") is to ensure a uniform level of data protection in the EU. Therefore, there are certain requirements that must be met if data is to be processed outside the EU.
In the case of data processing outside the EU (so-called third country transfers), a transfer impact assessment must be carried out in relation to the use of ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services that process personal data.

A transfer impact assessment identifies and evaluates the level of data protection and, if applicable, additional safeguards pursuant to Art. 46 GDPR, to the extent that an adequacy decision of the EU Commission is not available.

As summarized by the European Data Protection Board ("EDPB") (see EDPB recommendations), the right to data protection is a fundamental right of individuals, which provides for adequate safeguards to preserve the essence of this right. Data processing must therefore be appropriate, necessary and genuinely meet the general interest objectives recognized by the European Union or the need to protect the rights and freedoms of others. However, the right to the protection of personal data is not an absolute right. It must always be considered in relation to its function and weighed in accordance with the principle of proportionality.

As such assessments involve legal interpretations and analyses, ATOSS cannot offer its customers any legal advice in this regard. Notwithstanding this, we would like to offer our customers assistance in carrying out a transfer impact assessment for ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services in the light of the "Schrems II" ruling of the Court of Justice of the European Union and the recommendations of the EDPB and refer to relevant information in this whitepaper.

Following the recommendations of the EDPB, a transfer impact assessment can be conducted in the following six steps:

Step 1 Know your data transfers

In this step, all transfers of personal data of the customer shall be recorded. The mapping of where the personal data is transferred to is considered necessary to ensure that a substantially equivalent level of data protection is guaranteed wherever this personal data is processed.

Step 2 Identify the transfer tools you are relying on

A second step is to verify whether a transfer tool that constitutes an appropriate guarantee under Chapter V of the GDPR is in place.

Step 3 Assess whether the transfer tool is effective in light of all the circumstances of the transfer

The third step is to assess whether the applicable legislation and / or practices of the third country affect the effectiveness of the transfer tool used .

Step 4 Identify and adopt additional measures where necessary

A fourth step is the identification of additional safeguards and their necessity in order to raise the level of data protection of the personal data transferred to the applicable EU standard, where an adequacy decision of the EU Commission (Art. 45 GDPR) is not in place. This step is only necessary if your assessment shows that the third country's legislation and / or practices affect the effectiveness of a transfer tool under Art. 46 GDPR.

Step 5 Take formal procedural steps if you have identified additional measures

A fifth step is to take any formal procedural steps that you believe are necessary to obtain an adequate guarantee under Article 46 GDPR.

Step 6 Re-evaluate at appropriate intervals

The sixth and final step is to re-evaluate and monitor the level of data protection at appropriate intervals.

Step 1 Know your data transfers

In this step, all transfers of personal data of the customer shall be recorded. The recording of where the personal data is transferred to is considered necessary to ensure that a substantially equivalent level of data protection is guaranteed wherever this personal data is processed.

Stakeholders and roles in data processing

What role does the customer have in connection with the processing of his personal data to ATOSS?	For the purposes of the GDPR, the customer is the "**controller**". To the extent that the customer permits its affiliates to use the licensed ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services, its affiliates shall also become "controllers" for their personal data when using the ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services. Pursuant to the ATOSS contract, the customer shall remain the sole contractual party and thus the sole contact person for ATOSS. This shall apply not only to the customer's own interests but also to those of its affiliates, which may also use ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services for their personal data in accordance with the respective contract. Further details can be found in the preamble of the ATOSS DPA, which is available for download on our website.
What is the role of ATOSS and the companies commissioned by ATOSS in connection with the processing and transmission of the customer's personal data?	ATOSS and the companies commissioned by ATOSS are "**processors**" of the customer. The same shall apply with respect to the affiliates of the customer if they also use the ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services for their personal data. In this context, ATOSS is the direct contractual party of the customer and thus a **first-level processor**. In addition, ATOSS is authorized to use further companies to provide ancillary services in the case of an ATOSS Cloud Service. These companies commissioned by ATOSS are **sub-processors of ATOSS** and thus **second-level processors.** ATOSS shall be responsible for the use and careful selection of its sub-processors. The list of ATOSS' sub-processors can be found in the DPA-Exhibit III of the DPA, which is available for download on our website.

Additional information to the list of ATOSS sub-processors

As a European provider of HR workforce management solutions, ATOSS relies on reputable sub-processors to provide ancillary services in the case of an ATOSS Cloud Service. The use of these sub-processors serves to ensure the ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services in the light of GDPR compliance, in accordance with the state of the art and a best-of-breed approach and to reduce vendor lock-in as part of a multi-scaler strategy for our customers. By multi-scale, we mean that ATOSS may select and switch between the sub processors listed in this DPA-Exhibit III, as the sub processors are already authorized by the customer during the period of processing of personal data. ATOSS reserves the right not to use each of the sub processors listed in DPA-Exhibit III for the processing of personal data.

What is the advantage of the ATOSS multi-scaler strategy for ATOSS Cloud customers?

- This enables the establishment and operation of a state-of-the-art IT cloud infrastructure consisting of modern application servers & container orchestration clusters, geo-redundant backup and disaster recovery services as well as server management & system monitoring by IT experts and specialists.
- This allows certified high-security data centers to be used in accordance with international standards (e.g. DIN EN ISO/IEC 9001, DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27017, DIN EN ISO/IEC 27018).

Does ATOSS transfer personal data of the customer to a sub-processor directly commissioned by ATOSS with a registered office outside the EU?	As you can see from the DPA-Exhibit III, all ATOSS companies and all sub-processors with which ATOSS has concluded sub-contracts currently have their registered office within the EU or Switzerland. You will find the DPA-Exhibit III in our DPA, which is available for download on our website. In particular, the sub-processors commissioned by ATOSS to provide ancillary services in the case of an ATOSS Cloud Service either have their registered office within the EU and are thus directly subject to the scope of the GDPR and the supervision of the European data protection authorities or are subject to the reformed Swiss Data Protection Act.
Are all ATOSS sub-processors listed in the DPA used for the customer?	By conclusion of the ATOSS contract, the customer grants ATOSS a general permission to use all sub-processors listed in DPA-Exhibit III. At the same time, ATOSS reserves the right not to use each of the sub-processors listed therein for the processing of personal data. Taking into account capacity and resource planning, ATOSS limits the use of the sub-processors to the extent necessary for the performance of the services. Consequently, ATOSS may select and switch between the sub processors listed in this DPA-Exhibit III.

Can the customer limit the list of approved sub-processors to an individual selection of sub-processors?	A deletion or restriction to certain sub-processors of ATOSS by the customer is not possible. ATOSS always wants to design its ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services in the best possible way for the customer, which includes - not only in the interest of resource and capacity planning - but also the avoidance of alleged security risks such as vendor lock-in. At the same time, ATOSS can only maintain and expand its high innovative strength if ATOSS aligns its products and services to the best-of-breed approach and cooperates with various sub-processors who supply ATOSS with selected technologies over the entire term of the customer's contract. With a view to service quality and our contractual promise of continuous adjustments, ATOSS therefore needs the flexibility to be able to offer its customers outstanding services at all times.
How does ATOSS select its sub processors?	Prior to commencement of the data processing activities, each sub-processor of ATOSS shall be obliged in writing to comply with the same data protection obligations, i.e. at least equivalent in terms of content, as agreed with the customer in the ATOSS DPA. In this context, the subcontracting agreement must at least guarantee the level of data protection required in the DPA between ATOSS and the customer. ATOSS also attaches great importance to ensuring that all sub-processors of ATOSS guarantee appropriate security and data protection criteria for their specific processing activities. As a rule, this includes security measures such as encrypted data transmission and access secured by standard security mechanisms per access depth, as well as the inclusion of confidentiality clauses and proof of international certificates.
Where does ATOSS process and store the customer's personal data in the event that ATOSS Cloud Services are used?	ATOSS stores and processes the customer's personal data in the geographical regions indicated on our website. Link - Data residency

Is ATOSS aware that ATOSS sub processors providing ancillary services in connection with an ATOSS Cloud Service may transfer personal data of the customer to other (sub-)processors outside the EU / EEA?

ATOSS regularly reviews the agreements with its sub processors. With regard to further data processing activities, the following can be summarized:

Telekom Deutschland GmbH:

ATOSS has commissioned Telekom Deutschland GmbH ("Telekom") as a hosting service provider with the provision and operation of cloud infrastructures and associated support services. According to the data processing agreement with Telekom, the data processing activities of Telekom and its (sub)processors do not take place in third countries, i.e. outside the EU.

In addition, please refer to Telekom's various certificates and audit reports related to cloud privacy and information security.

Link - https://geschaeftskunden.telekom.de/hilfe-und-service/downloads/zertifikate
Link - https://www.qbeyond.de/auszeichnungen-zertifikate/

UMB AG:

ATOSS has commissioned UMB AG ("UMB") as a hosting service provider with the provision and operation of cloud infrastructures and associated support services. According to the data processing agreement with UMB, the data processing activities of UMB and its (sub)processors do not take place in third countries, i.e. outside the EU, or the EEA or Switzerland.

Upon request, we can provide corresponding certificates for Swiss customers at any time.

Is ATOSS aware that ATOSS sub processors providing ancillary services in connection with an ATOSS Cloud Service may transfer personal data of the customer to other (sub-)processors outside the EU / EEA?

Google Ireland Ltd.:

When licensing our ATOSS Mobile Apps - ATOSS Staff Center (Mobile) and ATOSS Time Control (Mobile) – a technology is included that shall ensure that Google Ireland Ltd. no longer carries out data processing activities in relation to personal data, even if ATOSS continues to use certain cloud services of Google Ireland Ltd. for the provision of the ATOSS (Mobile) Push Notification Service.

The ATOSS (Mobile) Push Notification Service allows the customer to send an automatic push notification to their users of the ATOSS mobile apps, e.g. "A new leave request is awaiting approval". This service must be explicitly set up by the customer. If this ATOSS (Mobile) Push Notification Service is not set up by the customer, no push message will be sent. In addition, the receipt of push messages can be allowed or blocked by the individual user of the mobile device at any time. The information contained in such push messages is transmitted exclusively via a secure connection (https) using an additional symmetric encryption method between the ATOSS mobile app on the user's end device and the ATOSS Staff Efficiency Suite/ATOSS Startup Edition or ATOSS Time Control.

This means that Google Ireland Ltd. is not involved in the transfer of personal data contained in the push messages. Nonetheless, the ATOSS Staff Efficiency Suite/ATOSS Startup Edition or ATOSS Time Control needs to authenticate to a messaging backend server in order to send push notification requests to mobile devices. Through a special technical implementation, ATOSS was able to ensure that no personal data is processed during the required authentication when using the Google Firebase Cloud Messaging. Authentication takes place by means of an individual token/key (Firebase token), which is generated by integrating Google Firebase Cloud Messaging. This Firebase token exclusively acts as a signal/trigger to the ATOSS Mobile App in order to query the latest push message status directly via the database of the ATOSS Staff Efficiency Suite/ATOSS Startup Edition or ATOSS Time Control.

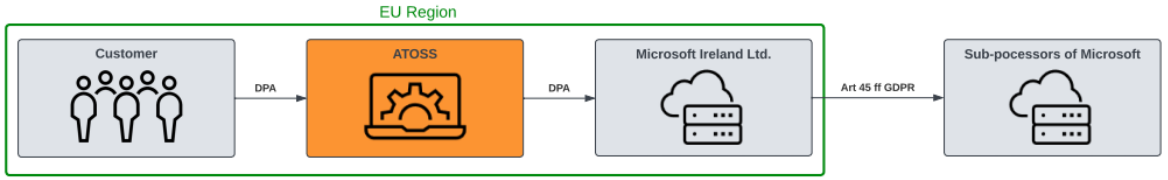
Further information can be found in an audit report done an independent security consulting company which performed the test explicitly for the ATOSS Staff Center (Mobile) Push Notification Service. For the ATOSS Time Control (Mobile) Push Notification Service an audit was not performed, as the implementation and use of Google Cloud Messaging is identical. The audit report for the ATOSS Staff Center (Mobile) Push Notification Service is available to our ATOSS Staff Efficiency and ATOSS Startup Edition customers on the ATOSS web lounge or can be sent to you at any time on request.

Microsoft Ireland Ltd.

ATOSS has commissioned Microsoft Ireland Ltd ("Microsoft") as a hosting service provider with the provision and operation of cloud infrastructures and associated support services. In this regard, it must known that Microsoft offers data centers in selectable regions worldwide. In line with GDPR compliance, ATOSS can use data centers in different regions for the benefit of its customers. When selecting data centers for customers, ATOSS takes into account the current circumstances (e.g. the existence of an adequacy decision or other) and generally selects data center regions that are close to the customer's destination and which shall thus ensure performance and service quality. According to current information from Microsoft, data processing activities outside the EU may be carried out by (sub)processors that are commissioned directly by Microsoft (see Figure 1).

Link - Microsoft General - List of sub-processors for online services

Figure 1



Special ATOSS supplementary agreement <EU Data Boundary> possible on customer's request

Upon customer's request, ATOSS is able to pass on the benefits from the Microsoft <EU Data Boundary> concept to the customer licensing the ATOSS CLOUD24/7. The <EU Data Boundary> is defined by Microsoft as a geographically defined boundary within which Microsoft has committed to store and process data, subject to limited circumstances where data will continue to be transferred outside the EU Data Boundary.

See statements and documentation provided by Microsoft about the EU Data Boundary.

Key facts according to ATOSS CLOUD24/7 offerings with EU Data Boundary supplementary agreement:

To the extend supplementarily agreed, ATOSS will offer cloud hosting and cloud operation services within the scope of the Microsoft EU Data Boundary as follows:

- **ATOSS selects Microsoft data centers regions located in <Europe> by default.** Consequently, personal customer data is stored in Europe. Microsoft may replicate this data to other data centers in Europe to improve data resilience. However, Microsoft does not store or transfer this customer data outside of Europe.

  See statements and additional information provided by Microsoft about data residency in azure.

- **ATOSS has enabled the additional access control named "Microsoft Customer Lockbox" for Microsoft Azure support services.** As a rule, most operations, support, and troubleshooting surrounding standard operating procedures performed by Microsoft personnel and its sub processors do not require access on personal data that is processed on the ATOSS customer cloud application instance and associated technical services. However, Microsoft is not able to exclude the occurrence of special circumstance where a Microsoft engineer needs to access data, whether in response to a support ticket initiated by ATOSS cloud experts or a problem identified by Microsoft. In such cases the Microsoft Customer Lockbox provides an interface to review and approve or reject data access requests from Microsoft personnel. For auditing purposes, the actions taken by Microsoft personnel are logged in the activity logs through the Microsoft Customer Lockbox.

  See statements and additional information provided by Microsoft about Customer Lockbox for Microsoft Azure.

Description of the data processing operations

What does "processing of personal data" mean within the meaning of the GDPR?	Data processing first describes the general use of any data. However, in order to interpret the GDPR, the term "**processing of personal data**" must be considered. The GDPR does not apply to all data, but only to the special category: "**personal data**". The GDPR understands the term "processing of personal data" very broadly, so that in principle any use of personal data is also a "processing of personal data" in the legal sense. In this sense, for example, data storage and transfer between different systems and applications in a cloud environment technically administered by ATOSS or its sub processors is a "processing of personal data". At the same time, this also refers to real-time remote access (e.g. in support situations).
What categories of personal data does ATOSS process in connection with ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services?	The DPA-Exhibit I contains the relevant information on the data categories of personal data, which ATOSS may process and transmit. The list of data categories contains the exemplary data categories that are processed typically insofar as the customer uses the ATOSS Cloud Services within the standard functions and within the scope of the typical business purposes. This includes in particular business uses for the performance of time and attendance management, shift management and personnel planning. Whether a listed data category is actually processed depends on the customer's individual selection of modules and its own configurations. Please note that the customer can change his configurations independently at any time and thus has full control over which data categories are actually processed. The DPA-Exhibit I can be found in our DPA, which is available for download on our website.

Does ATOSS process sensitive personal data within the meaning of Art 9 GDPR?	As ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services are in principle highly parameterizable by the customer, the selection of data categories and their nature depends on the customer's choice of individual configurations - cf. question before. Example: When configuring the settings, the customer can decide to process "information about planned and actual absences". Whether this information becomes sensitive health data depends on whether the customer creates buttons or service-related messages, e.g. with the name "illness", instead of simple "absence messages", or whether he creates links between the personal absence and other data, such as the certificate of incapacity for work due to illness or similar. In general, our ATOSS consultants always recommend the customer to clarify the configurations with his internal or external data protection officer. In the standard functions of the ATOSS modules in the ATOSS Staff Efficiency Suite/ATOSS Startup Edition (ASE/S), the customer can decide on the configuration of so-called absence codes. These absence codes, which can be freely selected by the customer, can be mapped with the codes already defined in the customer's accounting system. Should you require product-specific and commercial information on our ATOSS Cloud Services, please feel free to contact your responsible Account Manager at any time.
For what purposes are personal data of the customer transmitted?	Relevant information on the purposes of the data processing activities within ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services can be found in DPA-Exhibit I. This is part of our DPA, which is available for download on our website.
Is a data processing agreement ("DPA") concluded for the usage of ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services?	A DPA in accordance with the GDPR is always part of an ATOSS contract concluded in writing (also in electronic form as part of the ATOSS offer) between the contracting ATOSS company and the customer. Our current DPA is available for download on our website.

Step 2 Identify the transfer tools you are relying on

A second step is to check whether there is a transfer tool that constitutes an appropriate guarantee under Chapter V (Art. 44 - 50) of the GDPR.

The following transfer tools come into consideration with regard to the ATOSS Cloud Services:

Adequacy decision of the EU Commission (Art. 45 GDPR)	**Standard contractual clauses (Art. 46 para. 2 lit c GDPR)**	**Binding corporate data protection regulations (Art. 47 GDPR)**
☒	☒	☐
Consent of the data subject (Art. 49 lit a GDPR)	**Other extraordinary accruals (Art. 49 GDPR)**	**More:**
☐	☐	☐

Do adequacy decisions of the EU Commission (Art. 45 GDPR) come into consideration for data processing operations?

The EU Commission is authorized to decide on the basis of Art. 45 GDPR whether a country outside the EU (= third country) offers an adequate level of data protection. The corresponding mechanism for this is the issuance of an adequacy decision. If the EU Commission has issued an adequacy decision, no additional appropriate safeguards (Art. 46 GDPR) are required with regard to data processing in that country.

Please refer to the list of adequacy decisions of the EU Commission. This current list is available for download on the website of the EU Commission, where you can also find out about changes.

We would like to emphasize at this point that ATOSS and all of the sub processors which ATOSS commissions directly (cf. DPA-Exhibit III), have their registered office within the EU or Switzerland.

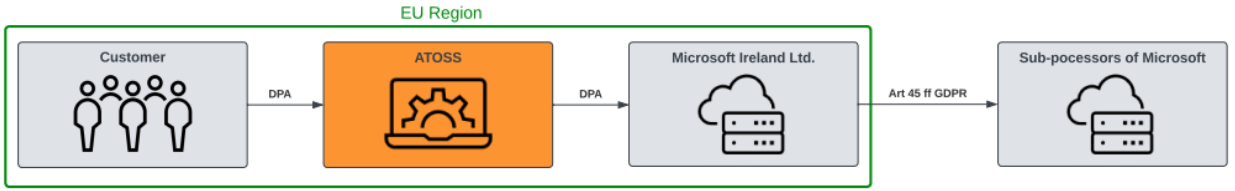
Although Switzerland is not a member of the European Union, the EU Commission has issued an adequacy decision for Switzerland.

The further transfer impact assessment is limited to Microsoft.

According to current information from Microsoft, data processing activities outside the EU may be carried out by (sub)processors that are commissioned directly by Microsoft.

Link - Microsoft General - List of sub-processors for online services

Figure 1



New assessment related to data processing operations to the U.S.:

With regard to the U.S., **an adequacy decision - the EU-U.S. Data Privacy Framework -** was issued on July 10, 2023.
With this adequacy decision, the EU Commission has certified an adequate level of data protection for the U.S..
In order for the adequacy decision to apply to U.S. companies, they must certify themselves in accordance with the requirements of the EU-U.S. Data Privacy Framework.
The companies that are certified, can be viewed at this official link.

The EU-U.S. Data Privacy Framework has come into force and essentially has the following effects:

- No additional guarantees required under Art. 46 GDPR for certified U.S. companies
- No standard contractual clauses ("SCC" for short) with U.S. companies necessary
- No need to conduct a comprehensive transfer impact assessment regarding data transfers to the U.S.

The new adequacy decision for the U.S. provides the long-awaited legal certainty. This provides a further building block of trust in ATOSS Cloud Services and the security strategy ATOSS has put in place to protect and securely process your data with technical, contractual and organizational measures.

Can other transfer tools (Art. 46 GDPR) be considered for the data processing activities?	For cases where no adequacy decision is in place, Art. 46 GDPR lists several instruments as so-called "**adequate safeguards**" that can be also used for the transfer of personal data outside the EU. In accordance with the legal situation, ATOSS and Microsoft have already concluded the applicable **SCC** prior to the enactment of the EU-U.S. Data Privacy Framework. Thus, the decision of the EU Commission with regard to the direct subcontracting relationship between ATOSS and Microsoft results in a **double security** for ATOSS, as the standard contractual clauses still remain valid. At the same time, Microsoft remains obliged to enter into SCC when using additional Microsoft sub processors for data processing activities outside the EU. • Please refer to the SCC available online from Microsoft - link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Step 3 Assess whether the transfer tool is effective in light of all the circumstances of the transfer

The third step is to assess whether the applicable laws and / or practices of the third country affect the effectiveness of the transfer tools. The scope of this assessment should be limited to the regulations and practices relevant to the protection of the specific personal data being transferred. In the present case, it must focus on HR workforce management information, such as employee data.

At this point we would like to refer you to the further information published by Microsoft.

What information has Microsoft published regarding the hosting and operation of cloud infrastructures?	The following examples include the Microsoft Privacy Principles and other data protection procedures: • Please refer to the Privacy Principles available online from Microsoft - link: Data Protection with Microsoft Privacy Principles | Microsoft Trust Center • Please refer to the white paper available online from Microsoft - Compliance with EU transfer requirements - link: Working white paper remake 029 FNL (microsoft.com) • Please refer to the privacy policy for Azure customers available online from Microsoft – link: https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data • Please refer to the Defending your Data Initiative available from Microsoft online -link: https://news.microsoft.com/de-de/datenschutz-wie-wir-unsere-kundendaten-nach-dem-schrems-ii-urteil-schuetzen/ • Microsoft confirms to all customers that it has conducted a Transfer Impact Assessment and that the result of that assessment is positive. Thereafter, Microsoft has no reason to believe that applicable laws, including in each country to which it transfers personal data, prevent it from fulfilling customer's obligations under the service agreement and the SCC. Section 6 "Notice of Change" of Appendix C of the Microsoft Products and Services Privacy Addendum - link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Step 4 Identify and adopt additional measures where necessary

A fourth step is to identify and add additional measures as necessary to raise the level of data protection of the personal data transferred to the applicable EU standard.

Additional technical and organizational measures done by ATOSS

What additional measures are in place in connection with the data processing of the customer's personal data done by ATOSS?	According to the DPA, ATOSS is obliged to take **appropriate technical and organizational measures** to ensure the confidentiality, integrity and availability of the customer's personal data. Please refer to our DPA-Exhibit II in the ATOSS DPA, which is available for download on our website. The **provision and operation of ATOSS Cloud Services** are regularly reviewed for compliance with security practices and information security policies. In order to meet the expectations of our customers ATOSS regards the operation of an information security management system in accordance with the international standard DIN EN ISO/IEC 27001 for ATOSS Cloud Services as a substantial obligation of its own. A copy of the certificate is available on the website at any time. In this context, ATOSS also conducts regular tests and security scans itself and through external security service providers. In addition, external audits are regularly conducted from a data protection perspective. Further information is available for download in our ATOSS customer web lounge (see section "Data Protection").
What encryption does ATOSS use to protect the customer's personal data from unauthorized access?	ATOSS and its hyperscalers use encryption methods according to the technical guidelines of the German Federal Office for Information Security (BSI) and the international standard ISO/IEC 27001 according to the ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services. **Encryption methods for data at rest** Personal data from our cloud customers is automatically encrypted at rest (256-bit AES encryption). Further information on the encryption of data at rest, for example in connection encryption of data at rest with Microsoft Azure SQL databases, is available on the Microsoft website. **Encryption methods for data in transit** The transmission of data from or to ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services is generally encrypted and secured. If the ATOSS Cloud Core Services and ATOSS Cloud Dedicated Services are natively capable of encrypting the exchanged data, the encryption standards HTTPS/SFTP/LDAPS/SMTPS are used. All HTTPS communications are protected via TLS using the recommended state of the art technology. File transfers are encrypted using Secure File Transfer Protocol (SFTP). Terminal data is transferred securely via HTTP2/TLS. If the terminals do not support HTTPS connection, a secure VPN tunnel must be implemented for communication. For the message digest algorithm, SHA512 is used if possible.

Additional technical and organizational measures done by Microsoft

What additional measures are in place in connection with the data processing of the customer's personal data done by Microsoft?

Microsoft is contractually obliged under the DPA to take **appropriate technical and organizational measures** to ensure the confidentiality, integrity, and availability of customer's personal data.

- Please refer to the technical and organizational measures published online by Microsoft - link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
- Please also refer to Microsoft's various certificates and audit reports related to cloud privacy or information security such as DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27017, DIN EN 27018 and the C5 certificate - link: https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-c5-germany?view=o365-worldwide

  Further link:
  https://servicetrust.microsoft.com/ViewPage/AllDocuments

Step 5 Take formal procedural steps if you have identified additional measures

A fifth step is to take any formal procedural steps necessary for the adoption of your additional measure(s) depending on the transfer tool under Art. 46 GDPR on which you rely. Based on the above information, ATOSS considers that no additional measures are required in the present case.

Step 6 Re-evaluate at appropriate intervals

The sixth and final step is to reassess the level of data protection of the personal data transferred at appropriate intervals. ATOSS will regularly review the information in this document to ensure that our customers are able to effectively conduct their Transfer Impact Assessments. We therefore reserve the right to change this content from time to time and to update any changes.

ATOSS.COM