WHITEPAPER

Transfer Impact Assessment

Version: 03/05/2025

This document is for information purposes only in relation to ATOSS Cloud Products and may change from time to time. The current version can be found on our website via https://www.atoss.com/en/security/data-residency

In detail, it contains information about
the ATOSS Cloud Core Services

- ATOSS Staff Efficiency (ASES) CLOUD24/7*
- ATOSS Startup Edition (ASE) CLOUD 24/7*
- ATOSS Staff Efficiency (ASES) Cloud Solution*
- ATOSS Startup Edition (ASE) Cloud Solution*
- ATOSS Time Control (ATC) CLOUD24/7
- ATOSS Time Control (ATC) Cloud Solution

**Explanations on the conclusion of an EU Data Boundary can be found on page 13 ff.*

the Cloud Dedicated Services

- Identity and Access management (IAM) Service
- Staff Center (Mobile) Security Gateway Service
- ATOSS Time Control (Mobile) Security Gateway Service

Details of the service levels and service descriptions can be found on our website: https://www.atoss.com/en/general-terms-and-conditions

It expressly does not contain any information relating to

- Crewmeister Products
- the ATOSS Connector for Workday
- the MODULE Workforce Analytics
- the ATOSS internal IT infrastructure

If you require product-specific information, please contact your Key Account Manager at any time.

Foreword

According to the GDPR, certain conditions apply to the processing of personal data outside the EU (so-called third country transfer).

Among other things, a Transfer Impact Assessment (TIA) is required for the use of cloud services. A TIA identifies and evaluates the level of data protection and, if necessary, additional guarantees in accordance with Art. 46 GDPR, if there is no adequacy decision by the EU Commission for the recipient in the third country. The **European Data Protection Board (EDPB)** also emphasizes that data protection should always be implemented proportionately. This means that the situation and legal interests must always be weighed up.

We would like to point out that the statements in this document do not constitute any binding promises, assurances or warranties for the licensed products. In this respect, only the information in the contractual documents relating to the respective Cloud Product applies. Furthermore, they do not replace (data protection) legal advice on the part of the customer. In case of doubt, please always consult your data protection officer.

ATOSS is also not permitted to offer you legal advice. At the same time, we support our customers to the best of our ability by publishing below relevant information for your own evaluation of our cloud services in the light of the "Schrems II" judgment of the Court of Justice of the European Union and the recommendations of the EDPB.

Transfer impact assessment in six steps

Step 1 Know your data transfers

According to the EDPB, companies should track which personal data they transfer to recipients in third countries to ensure that the level of data protection of these recipients complies with the GDPR.

Step 2 Identify the delivery tools you rely on

If there is a third country transfer, personal data may be transferred to recipients in third countries if the EU Commission has confirmed an adequate level of protection. If the third country does not have an adequacy decision, alternative transfer instruments, such as standard contractual clauses and additionally implemented security measures, must be evaluated in order to nevertheless be able to confirm an adequate level of data protection.

Step 3 Assess the effectiveness of the transmission tools in light of all the circumstances

In a third step, it should be examined whether the applicable legal provisions and/or practices of the third country impair the effectiveness of the transfer instruments used.

Step 4 Identify and add additional measures where necessary

Only if the previous assessment indicates an inadequate level of data protection must additional measures (either by the controller or processor) be considered. If no sufficient data security can be concluded despite additional security measures, the transfer must be suspended according to the EDPB in order to protect the legal interests concerned.

Step 5 Consider procedural steps when additional measures for effectiveness

The fifth step includes all necessary procedures to ensure an adequate guarantee in accordance with Art. 46 GDPR. Additional security measures must therefore be GDPR-compliant and, if necessary, coordinated with data protection officers and data protection authorities.

Step 6 Re-evaluate at appropriate intervals

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

Step 1 Know your data transfers

According to the EDPB, companies should track which personal data they transfer to recipients in third countries to ensure that the level of data protection of these recipients complies with the GDPR.

Checkpoints at a glance:

- ✓ Controller and processor
- ✓ Data exporter: Name and description of the organization (either a controller or a (sub)processor) that directly carries out the data transfer to the third country
- ✓ Data importer: Name and description of the organization and details of any subcontractors located outside the European Economic Area (EEA) that receive personal data from a data exporter.
- ✓ Categories of data subjects and data
- ✓ Processing purposes

Controller and processor

The GDPR defines two relevant roles in data processing: the controller and the processor (Chapter 4 GDPR). Any transfer of personal data is only permitted if the controller and processor comply with the general principles of data transfer - including for transfers to third countries (Art. 44 GDPR)

What role does the customer have in relation to data transfers of their personal customer data in the ATOSS Cloud Products?

In relation to the Cloud Service Agreement, the customer is the "**controller**" of its personal customer data. If the customer allows its affiliated companies to use the licensed Cloud Products, these affiliated companies also become "controllers" of their personal company data. However, the customer remains the sole contractual partner and is therefore the sole contact for ATOSS. Further details on the case constellations can be found in the preamble to the ATOSS DPA, which you can access on our website.

What role does ATOSS play regarding data transfers of its personal customer data in the ATOSS Cloud Products?

In relation to the Cloud Service Agreement, ATOSS, including the companies affiliated with ATOSS, and the companies commissioned by ATOSS are together "**processors**" of the Customer. The same applies in relation to the Customer's co-using affiliated companies.

- The contracting ATOSS company (ATOSS) is the customer's contractual partner, i.e. the only direct contact and therefore the first-level processor. **processor at the first level**.
- The companies affiliated with ATOSS and contracted companies are **sub-processors of ATOSS** and thus **second-level processors**. ATOSS is responsible for the deployment and careful selection of its sub-processors. The list of ATOSS sub-processors can be found in the DPA on our website.

Is a data processing agreement ("AVV" for short) concluded between the customer and ATOSS?

Through explicit inclusion, the DPA always forms an integral part of the ATOSS offer or the cloud service contract between the contracting ATOSS company and the customer

If ATOSS commissions a sub-processor to carry out certain data processing activities, ATOSS shall oblige this sub-processor to essentially the same data protection obligations as those that apply to ATOSS in the customer relationship. ATOSS shall ensure that the sub-processor fulfills the obligations to which ATOSS is subject in accordance with this DPA and the GDPR.

How does ATOSS select its sub-processors?

ATOSS attaches great importance to ensuring that all sub-processors of ATOSS guarantee the agreed level of data protection equally in relation to their specific processing activities. This generally includes implemented security measures according to best industry practices, such as encrypted data transmission and access secured by standard security mechanisms per access level, as well as the inclusion of confidentiality clauses, including proof of international certificates.

Are all ATOSS sub-processors listed in the DPA engaged for the customer?

Upon conclusion of the DPA, ATOSS has the Customer's general permission to use and change all sub-processors listed in DPA-Exhibit III during the term of the contract (multi-scale strategy). ATOSS reserves the right not to use every sub-processor listed therein for the Customer. This approach enables ATOSS to plan capacity and resources efficiently and at short notice and offers advantages for business continuity and resilience strategies. At the same time, ATOSS will limit the use of sub-processors to the extent necessary for the provision of services

Please also note that configuration and parameterization services within a customer cloud instance can only be provided if the customer activates a user account for this purpose. User and access management is therefore controlled solely by the customer.

Can the customer restrict the list of approved sub-processors to an individual selection of sub-processors?

Deletion or restriction to certain sub-processors is not possible for individual customers. This is because ATOSS must always be able to design its services in the best possible way for the customer, which includes not only efficient resource and capacity management, but also the avoidance of security risks such as vendor lock-in or service outages. In the interests of our customers, ATOSS endeavors to maintain a high level of innovation and to continuously expand it in the light of a best-of-breed approach in favor of service quality. Regarding this service quality and our contractual promise of continuous modifications, ATOSS therefore needs the flexibility to select state-of-the-art technologies and establish effective cloud processes in order to offer its customers outstanding services.

Data exporter and data importer

The terms **data importer** and **data exporter** do not originate from the GDPR, but from the **Standard Contractual Clauses (SCC)** of the European Commission. These roles are intended to describe the transferor and recipient of personal data to a third country in more detail. The EDPB has even defined criteria to specifically determine a so-called international transfer.

It can be stated: If a company transfers personal data outside the EU/EEA, the transferring company is a data exporter and the recipient in the third country is the data importer.

According to the EDPB, mere remote access to personal data from a third country is also relevant data processing, i.e. no storage of data in this third country is required. At the same time, the EDPB emphasizes that the mere risk that persons from third countries can remotely access data stored in the EU/EEA does not constitute an onward transfer in accordance with Chapter V GDPR.

Information from the EDPB is available online on the EU Commission's website: https://www.edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en

Does the licensing of ATOSS Cloud Products lead to a transfer of personal data to a recipient in a country outside the EU/EEA?

As a cloud service provider of workforce management solutions, ATOSS has established itself as one of the leading providers in Germany and Europe as well as internationally. ATOSS customers include German and European public authorities, as well as European and international financial, retail, logistics and industrial companies, and companies in the healthcare and service sectors.

These customer expectations must be considered when compiling our license offers and designing our cloud services. ATOSS successfully relies on selected modern cloud technologies and renowned hosting service providers (hyperscalers) with globally available services. It is a strategic concern of ours to utilize the innovation opportunities available on the market and global developments in new technologies for our cloud services and customers. Assuming this is the case, international transfers cannot be completely ruled out.

We describe the background and overall circumstances below:

ATOSS and its affiliated companies

The parent company, ATOSS Software SE, is a Bavarian company (Munich, Germany) that specializes in the development and sale of cloud and software solutions for working time management and personnel resource planning. The ATOSS Group includes other subsidiaries within the EU with which our customers can conclude cloud service contracts in accordance with local law (then contracting ATOSS company) or which act as processors (e.g. support hotline). (e.g. support hotline, consulting) under the cloud service contract with the customer.

- ATOSS companies based in the EU that are directly subject to EU data protection law

ATOSS customers

EU data protection law applies directly to EU **customers**. Since no international transfers take place in the direct relationship between ATOSS and the EU customer, the AVV provisions apply to onward transfers in the (sub)processor chain.

If an **EU customer** allows **its affiliated company in a third country (third country company)** to use ATOSS Cloud Products (e.g. client-based), please inform us at an early stage. This is because the third country company is then a data importer and ATOSS is a data exporter. This international transfer should be legitimized by a privacy addendum based on standard contractual clauses and a specific third country legal review.

Since our **international contract customers with registered offices in third countries** also qualify as data importers and ATOSS as data exporters, ATOSS and the customer should review these international transfers in the direct relationship and legitimize them by means of a privacy addendum based on standard contractual clauses and taking into account the law in the third country.

ATOSS sub-processors

For our EU customers, therefore, only the assessment of an international (onward) transfer in the light of the subprocessing chain is relevant

Sub-processors that use modern cloud technologies to provide their services on a subcontracted basis are eligible.

Which ATOSS sub-processors qualify as data importers? Which are not and how is this to be justified in each case?

Our Cloud Product portfolio follows a multi-scale approach. This also includes the simultaneous use of different service hosting providers for our cloud services and service components.

In detail:

Telekom Deutschland GmbH

ATOSS has commissioned Telekom Deutschland GmbH ("Telekom" for short) as a hosting service provider for the provision and operation of cloud infrastructures and related support services. To our knowledge, Telekom is not to be classified as a data importer in the present case.

Data Hosting
Data hosting takes place in data centers of Telekom and its sub-processors, EU. Telekom reserves the right to change the locations of its data centers at any time within the EU region.

Data processing
In accordance with the data processing agreement with Telekom, data processing does not take place outside the EU.

Certificates and measures
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" for short) as a hosting service provider for the provision and operation of cloud infrastructures and related support services. To our knowledge, UMB is not to be classified as a data importer in the present case.

Data Hosting
Data hosting takes place in data centers of UMB and its sub-processors, Switzerland. UMB reserves the right to change the locations of its data centers at any time within the Switzerland region.

Data processing
In accordance with the data processing agreement with UMB, data processing does not take place outside Switzerland, the EU and the EEA.

Certificates and security measures
Link: https://www.umb.ch/en/company/vision-mission
On request, we can provide copies of the security certificates for Swiss customers at any time.

Google Ireland Ltd.

When licensing our new ATOSS Mobile Apps, ATOSS Staff Center (Mobile) and ATOSS Time Control (Mobile) includes technology designed to ensure that Google Ireland Ltd. ("Google") does not carry out any data processing activities in relation to personal data, even if ATOSS continues to use certain Google cloud services to provide the ATOSS (Mobile) Push Notification Service. To our knowledge, Google is not to be classified as a data importer in the present case.

The ATOSS (Mobile) Push Notification Service enables the customer to send an automatic push notification to the users of the ATOSS Mobile Apps, e.g. "A new vacation request is waiting for 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 permitted 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) with an additional symmetric encryption procedure 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 is not involved in the transmission of the personal data contained in the push messages. Nevertheless, the ATOSS Staff Efficiency Suite/ATOSS Startup Edition or ATOSS Time Control must authenticate itself 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 using Google Firebase Cloud Messaging. Authentication is carried out using an individual token/key (Firebase Token), which is generated by the integration of Google Firebase Cloud Messaging. This Firebase token serves exclusively as a signal/trigger to the ATOSS Mobile App to query the current status of the push message directly via the database of the ATOSS Staff Efficiency Suite/ATOSS Startup Edition or ATOSS Time Control.

Your key account manager can provide you with further information on request in an audit report from an independent security consultancy.

Note: No audit was performed for the ATOSS Time Control (Mobile) Push Notification Service, as the implementation and use of Google Cloud Messaging is identical.

Microsoft Ireland Ltd.

ATOSS has engaged Microsoft Ireland Ltd ("Microsoft") as a hosting service provider for the provision and operation of cloud infrastructures and related support services. To our knowledge, Microsoft is to be classified as a data importer.

Data Hosting

Microsoft offers data centers in selectable regions worldwide. When selecting data centers for customers, ATOSS takes into account the specific circumstances (e.g. the existence of an adequacy decision or similar) and prefers to select data center regions that are close to the customer's location in order to ensure performance and service quality. For EU customers (without affiliated third country companies), we therefore select reasonably referenced and generally available geo-redundant MS Azure regions within the EU/EEA and Switzerland. Microsoft reserves the right to change the specific locations of its data centers at any time within the agreed MS Azure regions.
Information on the MS Azure data center regions can be found here: What are Azure regions?

Certificates and security measures

Link: https://learn.microsoft.com/en-us/compliance/regulatory/offering-C5-Germany?view=o365-worldwide

Link:

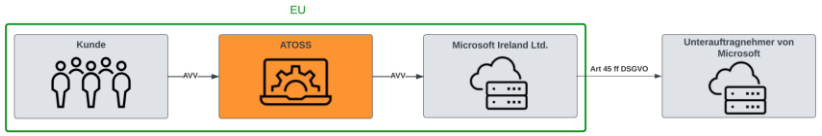
https://servicetrust.microsoft.com/ViewPage/AllDocumentsA

Data processing

In accordance with the data processing agreement with Microsoft, the Microsoft Products and Service Data Protection Addendum (DPA) applies, publicly available here: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

According to current information from Microsoft, certain data processing activities outside the EU may therefore also be carried out by (sub)sub-processors of Microsoft.

Figure 1



Link - Microsoft General - List of subprocessors for online services

As a rule, most cloud operations, support and troubleshooting under standard operating procedures performed by Microsoft personnel and its subprocessors do not require access to personal data processed on the customer's cloud instance and associated technical services.

However, Microsoft cannot rule out the possibility that in special circumstances a Microsoft support technician may need to access data remotely, whether in response to a support ticket initiated by ATOSS Cloud experts or to a problem identified by Microsoft.

For such cases, the "Customer Lockbox for Microsoft Azure" offers a special feature to check and approve or reject data access requests from Microsoft personnel by our ATOSS Cloud experts. For monitoring purposes, the access requests as well as the actions performed by Microsoft personnel are logged in the activity logs via this customer lockbox. Please refer to Microsoft's explanations and additional information on the **Customer Lockbox for Microsoft Azure**.

Has ATOSS activated the " Customer Lockbox for Microsoft Azure " by default?

Yes, that is true. Consequently, all ATOSS Cloud customers benefit from this additional access monitoring in relation to Microsoft data processing.

ATOSS Supplementary Agreement <EU Data Boundary>

For EU customers (without affiliated third country companies), ATOSS offers a so-called EU data limit for data hosting by contract addendum on request. The so-called <EU Data Boundary> is defined by Microsoft as a geographical boundary within which Microsoft has undertaken to store and process personal data, whereby under special circumstances data may also be processed outside the EU Data Boundary. Please refer to Microsoft's explanations and additional information on the **EU Data Boundary**.

In our ATOSS contract addendum to the EU Data Boundary, we provide you with contractual confirmation that we only select data center regions according to the Microsoft EU Data Boundary and that the customer lockbox for Microsoft Azure is activated by default. We offer the "EU Data Boundary" option for the following Cloud Products; ATOSS Time Control Cloud Products are excluded:

- ATOSS Staff Efficiency (ASES) CLOUD 24/7
- ATOSS Startup Edition (ASE) CLOUD 24/7
- ATOSS Staff Efficiency (ASES) Cloud Solution
- ATOSS Startup Edition (ASE) Cloud Solution
- Identity and Access management (IAM) Service

Please discuss the details and any additional license costs with your Key Account Manager

Categories of data subjects and data

The GDPR only applies to personal data and therefore only affects natural persons. In workforce management, these are employees, civil servants, candidates of the federal states, tariff employees, trainees and other users of the Cloud Products authorized by the customer.

What specific categories of personal data are processed in the ATOSS Cloud Products?

Our DPA contains in DPA-Exhibit I, a very detailed list of the categories of data typically to be processed that customers can have processed when using the Cloud Products within the standard functions and within the scope of the typical business purposes for time and attendance management, shift management and personnel planning.

Note: Our flexibly configurable solutions allow customers to control which data categories are processed themselves via their key users - depending on the module selection and the customer-specific configurations
All functions are described in the technical documentation. This documentation is supplied via technical online help and is kept up to date by ATOSS.

Does ATOSS process sensitive personal data within the meaning of Art. 9 GDPR?

As explained above, the selection and sensitivity of the data categories depends largely on the customer configuration. Our security precautions enable the processing of sensitive data (see DPA-Exhibit I).

If you require product-specific information, please contact your Key Account Manager at any time.

For what purposes is the customer's personal data processed?

Our DPA contains the description of the purposes for the commissioned data processing in DPA-Exhibit I.

Step 2 Identify the transmission tools, you rely on

If there is a third country transfer, personal data may be transferred to recipients in third countries if the EU Commission has confirmed an adequate level of protection. If the third country does not have an adequacy decision, alternative transfer instruments, such as standard contractual clauses and additionally implemented security measures, must be examined in order to nevertheless be able to confirm an adequate level of data protection.

Checkpoints at a glance:

- ✓ Adequacy decisions of the EU Commission
- ✓ Inclusion of standard contractual clauses
- ✓ Additional security measures implemented

Does ATOSS take into account the adequacy decisions of the EU Commission and the inclusion of standard contractual clauses?

The EU Commission can classify third countries as compliant with data protection regulations by means of an adequacy decision (Art. 45 GDPR). Additional guarantees (Art. 46 (2) lit. c) GDPR) are then not necessary. The current list of decisions can be found on the EU Commission's website.

Switzerland (UMB AG)

According to the Commission decision, an adequate level of protection is ensured in Switzerland and personal data can be transferred and stored there without the need for additional safeguards. The decision is relevant for data hosting and data processing by UMB AG.

USA (Microsoft Ireland Ltd)

Since July 10, 2023, the EU-U.S. Data Privacy Framework certifies that the U.S. has an adequate level of data protection, provided that U.S. companies have certified themselves accordingly. Microsoft US entities covered by the Data Privacy Framework certification can be found on the Microsoft website: https://www.microsoft.com/en-us/privacy/entity-list-adhering-to-privacy-shield

You can find the active company certificates for Microsoft on the Data Privacy Framework list: https://www.dataprivacyframework.gov/list

Worldwide (Microsoft Ireland Ltd.)

Our Cloud Products contain a wide range of components, some of which are configured regionally or globally and some of which are configured differently. For key cloud components, such as databases and NetAPP files, we use geo-redundant storage (GRS) within Microsoft Azure. This protects your customer data from local site failures and data backup can be combined with the high requirements for cloud availability, information security and disaster recovery. Please refer to the Microsoft information available online - Link: https://learn.microsoft.com/en-us/azure/storage/files/files-redundancy#redundancy-in-a-secondary-region

In accordance with the legal situation, ATOSS and Microsoft have concluded the applicable standard contractual clauses (SCC). At the same time, Microsoft has also undertaken to conclude these SCCs for processing activities outside the EU if further sub-processors are used. The Microsoft SCCs available online can be found at the link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Explanations of the certificates and additionally implemented security measures can be found in the previous sections on pages 12 ff.

Step 3 Evaluate whether the instrument of transfer is effective in light of all the circumstances of the transfer

The third step is to examine whether the applicable legal provisions and/or practices of the third country impair the effectiveness of the transfer instrument used. International data centers, the global service components and international onward transfers from Microsoft are relevant here.

In detail:

Worldwide (Microsoft Ireland Ltd.)

Please refer to the Microsoft Defending your Data Initiative link available online: https://news.microsoft.com/de-de/datenschutz-wie-wir-unsere-kundendaten-nach-dem-schrems-ii-urteil-schuetzen/

Please refer to the Microsoft DPA available online with Appendix C (additional safeguards). Microsoft confirms a positive Transfer Impact Assessment and sees no legal obstacles to the fulfillment of the contractual obligations and SCC. - Link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Please refer to the Microsoft Privacy Principles available online - Link: Data Protection with Microsoft Privacy Principles | Microsoft Trust Center

Please refer to the Microsoft Whitepaper - Compliance with EU transfer requirements - Link: Working white paper remake 029 FNL (microsoft.com)

Please note the Microsoft Security Fundamentals for Azure customers available online: https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data

Step 4 Identify and add additional measures where necessary

Additional measures are only required if the assessment reveals an inadequate level of data protection. If these are not sufficient, the transfer must be suspended according to the EDPB.

Following a comprehensive internal assessment by ATOSS, the existing security measures guarantee an appropriate level of protection from our subjective point of view, which is also objectively proven by security certificates and independent test reports.

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

The fifth step includes all necessary procedures to ensure an adequate guarantee in accordance with Art. 46 GDPR. Additional security measures must therefore be GDPR-compliant

You can download the ATOSS ISO27001 certificate for cloud services from our https://www.atoss.com/en/security. At the same time, your key account manager can send you a GDPR report on request.
The active U.S. company certificates from Microsoft can be found on the Data Privacy Framework list:
https://www.dataprivacyframework.gov/list.

Step 6 Re-evaluate at appropriate intervals

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