IT Infrastructure and use of **AWS at Personio**

Date: 24/02/2022

Table of Contents

Summary

Personio uses Amazon Web Services Europe (AWS) as its **hosting provider**.

The data centres of AWS are, among others, **DIN ISO/IEC 27001** and **DIN ISO/IEC 27018** certified and guarantee the highest level of data protection security.

All customer data is stored on **servers within the European Union**.

AWS not only meets **strict security and compliance requirements**, but also enables us to increase the **stability** and scalability of our infrastructure.

To ensure security, all data is encrypted at rest (**Encryption at rest**) and in transit over public networks (**Encryption in transit**).

Personio takes **additional technical and organisational measures** to ensure the security of processing

Introduction

As part of our preparations for the GDPR, we have already scrutinised all our processes, technical measures and conditions. We also reviewed our hosting concept with regard to data security, availability and scalability. With the involvement of various experts (including data protection officers and IT security consultants), we defined a series of measures to achieve an optimal solution for our customers in the long term.

The most important change we made in this context was the change of hosting provider to Amazon Web Services (AWS). This decision was made on the basis of a detailed analysis in which we compared different providers and models.
In addition to meeting strict security and compliance requirements, the associated increase in the stability and scalability of our infrastructure was decisive in the decision in favour of AWS.

AWS has since proven to be a reliable and secure partner for our company that can meet our high data security requirements in the best possible way. In addition to the technical precautions, we have also taken all necessary precautions with AWS on a legal / contractual level to ensure the best possible security of all your data.

This document is intended to provide transparency about our decision-making process as well as an insight into our legal and technical measures with which we protect our customer data. It is written primarily for the data protection and information security officer and the legal department of your company.

Compliance and legal aspects

We selected AWS on the basis of a careful selection process, taking into account legal, organisational and technical criteria. After intensive due diligence and corresponding negotiations, we chose AWS as our infrastructure partner because, in addition to first-class products and services, AWS also has an extremely professional compliance and security set-up.

Certifications to prove information security and data protection

The services offered in the AWS Frankfurt region and in the other European regions and used by us, such as RDS (database), S3 (document storage) or KMS (key management), have numerous internationally recognised certifications, which have been attested by independent and renowned consulting companies and demonstrate compliance with the highest security requirements.

The AWS Frankfurt region, other regions and corresponding services are certified both for IT security according to DIN ISO/IEC 27001 and for the protection of personal data in the cloud according to DIN ISO/IEC 27018. Furthermore, AWS is certified according to the internationally recognised Payment Card Industry Data Security Standard (PCI DSS). This standard is bindingly applied by credit card organisations and is considered one of the strictest security regulations worldwide.

Furthermore, AWS is the first company to have the security of its cloud environment certified by the German Federal Office for Information Security (BSI) on the basis of the Cloud Computing Compliance Controls Catalogue (C5). AWS is thus considered a pioneer for cloud security in Germany. An overview of all compliance programmes and certifications of AWS can be found here.

As part of the selection process for our new hosting provider, we worked intensively with our data protection officer from Bitkom Servicegesellschaft mbH.

We are therefore convinced that AWS is the best possible partner for our company in terms of data protection. You are welcome to convince yourself of AWS' compliance with the GDPR. You can find more information here.

Restriction of server locations to the EU area

To best ensure that data cannot be used or disclosed without authorisation, we have technically and contractually restricted the use of the services to the EU/EEA area and regulated access options accordingly.

We are aware of the concerns of some data protection experts regarding the possible disclosure of data based on requests from the US government. We are monitoring the corresponding developments in US legislation, such as the Cloud Act, as well as the EU's efforts to exchange electronic evidence in criminal cases, and welcome in principle the intention to create legal certainty. It should be noted that neither we nor AWS will hand over data without cause, as this is neither in the business interest of the two companies nor of our customers.

In order to protect our customers' data even in the unlikely event of a state claim for surrender and against "external attacks", we have developed a comprehensive data protection and IT security concept together with AWS. According to the "Shared Responsibility Model", we rely on the extensive security mechanisms of AWS ("Security of the Cloud") on the one hand and will additionally apply our own security measures. Further information on the "Shared Responsibility Model" of AWS can be found here, further information on the technical and organisational measures of AWS are listed here.

An essential core element of our security measures is encryption, which is also required by the GDPR. We use state-of-the-art encryption algorithms (see section "Encryption"), wherever possible AES-256, which is approved even in the USA for documents of the highest classification level and is considered indecipherable.

We use state-of-the-art encryption algorithms (see section “Encryption”), wherever possible AES-256, which is also approved in the USA for documents with the highest level of confidentiality and is considered indecipherable. This encryption ensures that even in the very unlikely event of data theft, the data is protected in the best possible way against unauthorised access.

Technical and organisational measures

In the following, we would like to go into more detail about our data protection and IT security concept in connection with the use of AWS. If you have any questions, please contact us at security@personio.de. Our security engineering team will be happy to assist you.

Database encryption (Encryption at rest)

The Amazon Web Services key management system (AWS KMS) is used to encrypt customer data. The encryption system is designed so that no one, including Personio staff and AWS staff, can access the plaintext encryption keys.

For more details, please refer to the AWS FAQ:

AWS KMS is built so that no one, including AWS employees, can retrieve your plaintext CMKs from the Service. AWS KMS uses hardware security modules (HSMs) that have been or are currently being validated in accordance with FIPS 140-2 to protect the confidentiality and integrity of your keys. Your keys are stored in these HSMs whether you use AWS KMS or AWS CloudHSM to create your keys or import key material into a CMK. Your plaintext CMKs never leave the HSMs, are never written to disk at any time, and are only used in the HSMs' temporary storage for the duration of the cryptographic operations you request. Updates to the software on the service hosts and the AWS KMS HSM firmware are controlled by a multi-party access control that is audited and verified by an independent group within Amazon and a NIST certified laboratory in accordance with FIPS 140-2.

All customer data stored by Personio uses encryption at rest. This is done using the AWS KMS and applies to all AWS services that store data, such as RDS, S3 or EBS. This process ensures that unauthorised third parties cannot gain access to unencrypted data. All cryptographic keys are automatically rotated once a year.

The use of AWS KMS at Personio

AWS KMS is a managed service that simplifies the creation and control of encryption keys for data encryption. The Customer Master Key (CMK) in AWS KMS is protected by FIPS 140-2 validated cryptographic modules.

The following functions are generally supported by AWS KMS:

- Creating, describing and listing the Master Key.
- Enabling and disabling Master Keys
- Create and view permissions and access control policies for the Master Key.
- Enable and disable automatic rotation of cryptographic material in a Master Key
- Import cryptographic material into an AWS KMS Master Key
- Marking Master Keys for easy identification, categorisation and tracking
- Deleting Master Keys to complete the life cycle of keys.

The following cryptographic functions are supported by AWS KMS:

- Encrypt, decrypt and re-encrypt data.
- Generating keys for encrypting data (Data Encryption Keys)
- Generating random numbers for cryptographic applications

Monitoring

Every access and use of AWS KMS keys is monitored and recorded. This allows Personio GmbH to ensure that there are no unauthorised accesses to the keys used to encrypt the data. Access to the key management system is audited and manually reviewed by Personio's security engineering team if a security incident is suspected. In addition, AWS KMS key rotation events are monitored in CloudTrail.

Data separation in the context of encryption

Just as Personio ensures that data is strictly separated between different AWS accounts (Development, Staging, Testing, and Production), the Encryption keys used for the different AWS accounts are also strictly separated. A key is used only in the AWS account for which it was created. A KMS key from one AWS account cannot be used to encrypt or decrypt data in another account.

Transport encryption (Encryption in transit)

Personio systems use transport encryption whenever data needs to be transferred over an insecure or public network (e.g. outside the Virtual Private Cloud).

The transport encryption used depends, among other things, on the encryption requested by the client system. Only secure transport encryption is used within the company. The client is responsible for ensuring that its client system supports the corresponding transport encryption according to the state of the art and prefers it accordingly.

HTTPS

The web interface and API of the Personio application are only accessible via HTTPS connections. Client systems must use at least **TLS 1.2** to access the Personio system.

Administrative access

Access to Personio systems for administrative purposes is only via secure and authenticated connections.

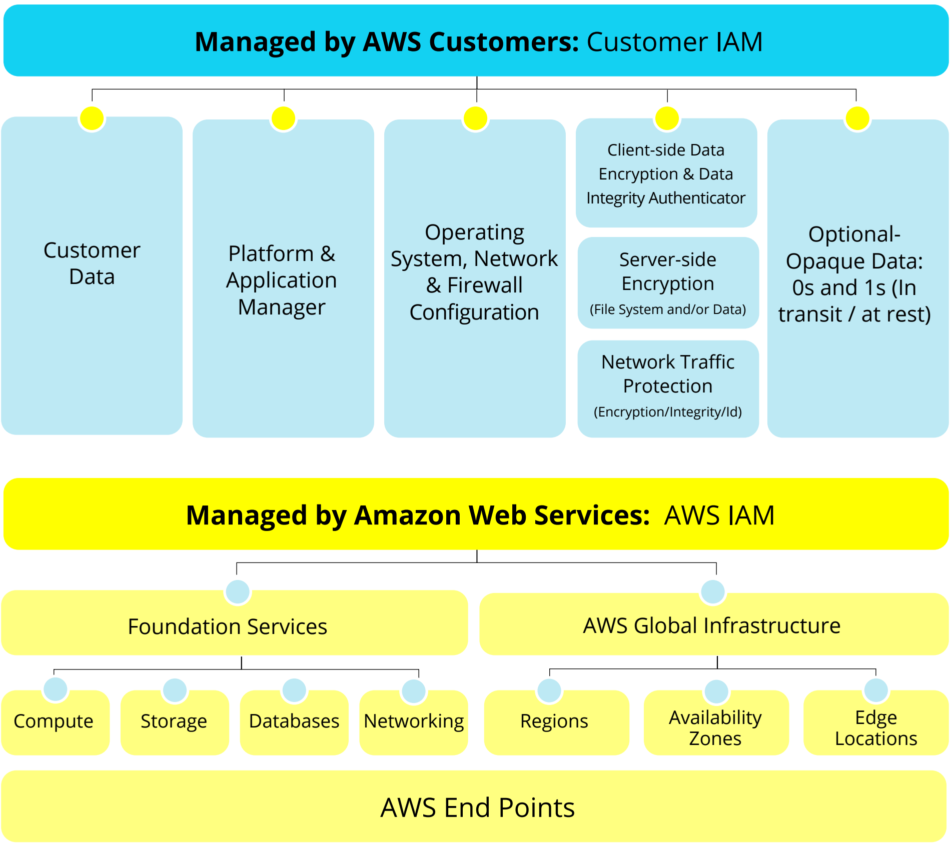
Data protection responsibilities

Personio shares its data protection responsibilities with AWS. The following assets fall to AWS:

- Facilities (data centres, air conditioning, etc.)
- Physical security of hardware
- Network infrastructure (routers, switches, cables, etc.)
- Virtualisation infrastructure
- Operating systems and software in the case of SaaS services

The following assets are the responsibility of Personio when used in the context of IaaS:

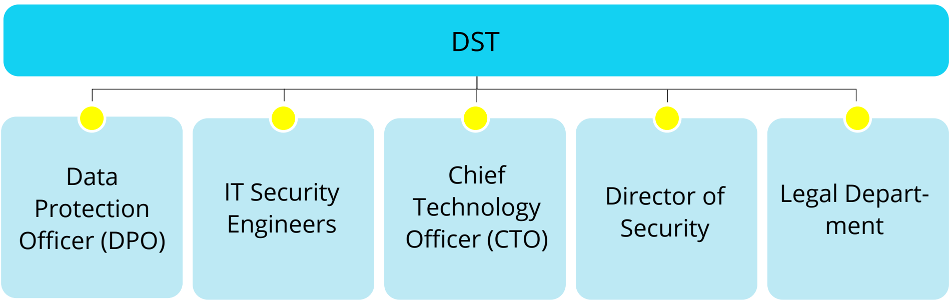
- Amazon Machine Images (AMI)
- Operating Systems
- Applications and program libraries
- Data in Transit
- Data in Rest
- Credentials
- Policies and configurations


Managed by AWS Customers: Customer IAM
Customer Data
Platform & Application Manager
Operating System, Network & Firewall Configuration
Client-side Data Encryption & Data Integrity Authenticator
Server-side Encryption (File System and/or Data)
Network Traffic Protection (Encryption/Integrity/Id)
Optional- Opaque Data: 0s and 1s (In transit / at rest)
Managed by Amazon Web Services: AWS IAM
Foundation Services
AWS Global Infrastructure
Compute
Storage
Databases
Networking
Regions
Availability Zones
Edge Locations
AWS End Points

Source: AWS

Personio has formed a Data Protection and Information Security Team (DST) for issues related to data protection as well as data security. Depending on the specific issue, different persons of this team may become active.

The following persons are part of the DST:



DST

Data Protection Officer (DPO)

IT Security Engineers

Chief Technology Officer (CTO)

Director of Security

Legal Department

Access Control

Personio uses different levels of access control for its systems and services on AWS. These are managed through AWS' Identity and Access Management (IAM), which enables a fine granulation of access to different services within the AWS cloud and records access to services. IAM permissions are automatically provisioned via SSO.

The overriding principle for Personio when assigning rights is "need-to-know". In practice, this means that employees are only given access to those functions they need to perform their jobs. The security engineering team carries out regular audits to check whether the assigned access rights comply with the need-to-know principle. Access to back-end systems is only possible via secure and authenticated connections. Public release of back-end systems is prohibited.

In accordance with the need-to-know principle, only a strictly limited number of Personio employees have access to the system that stores customer data. This direct access is exclusively for error analysis and is monitored.

Firewalling and security Groups

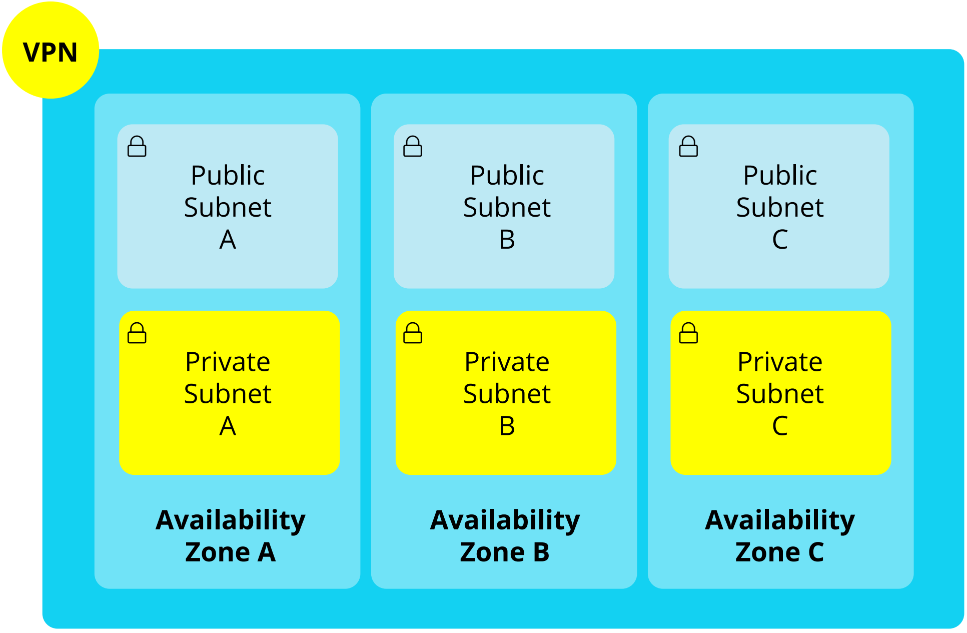
A web firewall is used to protect against common web exploits and bots that can affect availability or compromise security. Personio uses security groups to ensure that AWS services can only be accessed on the expected ports and from the expected network.

Network separation / Availability zones / **Geolocation**

Personio ensures separation of networks used for different purposes in the AWS environment by using different AWS accounts as well as different VPCs (Virtual Private Clouds). Direct network access between VPCs in different AWS accounts is not possible.

Personio stores data exclusively in AWS data centres in the European Union. All front-end and back-end systems operated by Personio are redundant and distributed across multiple availability zones. This ensures that even if one availability zone fails, the Personio application can continue to operate without restriction.

Each availability zone is connected to several internet service providers and is supplied by several power circuits. They are interconnected via high-speed links so that applications distributed across multiple zones can use LAN connections to communicate between zones. This enables optimal performance of all systems used by the Personio application.
The diagram below shows a typical network architecture in AWS. It shows a VPC within an AWS region that is distributed across three availability zones. In each availability zone, different subnets can be created that are either public or private.



We have built a similar network and applied best practices to ensure that customer data is only accessible within the private subnets. This means that all of our infrastructure is within a private network (with no public IPs) and therefore not directly accessible from the internet. Only the publicly accessible parts of the infrastructure, such as load balancers, are on the public network, as they are used for routing customer traffic.

Intrusion detection / Malware detection / **Logging of security-related events**

Personio uses an intrusion detection system (IDS). It consists of agents and a central master that monitors the availability of the agents and is informed by the agents in case of anomalies.
The IDS monitors:

- Log files for unusual or unknown entries
- Changes to system files (file integrity monitoring) as well as AWS' own configurations
- All login attempts as well as changes in rights within the systems
- Changes in the device file system and the loaded kernel modules to detect the connection of unauthorised hardware
- Network traffic
    - Known exploits and rootkits
    - Spoofing
- All changes to the IDS itself including restarts or agent failures
- API events triggered by IAM users within AWS account environments.
- Unused services or users on the respective systems
- Changes in used (network) ports

If security-related anomalies are detected on a system, they are automatically reported to the relevant Personio staff, who then perform a manual check of the anomaly. Particularly critical anomalies, such as the detection of a rootkit, are automatically prevented. Furthermore, the IDS supports a security policy enforcement that meets the requirements of PCI DSS 3.0.

This is used to enforce secure configurations of running services and to detect possible security risks (for example, unused system access).

Logging / Audit Trail

Personio uses logging in its AWS environments for several areas. These include:

- System events
- Error logging
- User activity
- Logins and requests to database systems
- Other security-related events / audit logging

By using AWS Cloudtrail, Personio has the ability to record all events within the cloud environments used, thereby not only creating transparent user and resource activity, but also providing a high level of transparency for forensic analysis of potential security incidents. The information collected by Cloudtrail is analysed by the IDS to detect anomalies in a timely manner.

Change Management

Personio manages configurations of systems and software using “infrastructure as code”. The associated code is stored in repositories of a version management system to make changes traceable in terms of time and content.

Before changes are imported into the operating environment, they are tested in a staging environment that is identical to the operating environment. This applies to configuration changes as well as to system and software updates.

Backups

Personio creates at least daily backups of all data required to operate the infrastructure, as well as all data entered or uploaded by customers in the Personio application.

Performance and Auto Scaling

Personio uses both horizontal and vertical auto scaling features provided by AWS to enable the best possible performance. This makes it possible to add resources to the networks in a fully automated way when the existing resources are no longer sufficient.

Monitoring

Personio uses various monitoring tools to ensure maximum availability and performance of the application. These monitor at least the following parameters:

Availability

- Accessibility of the application
- Accessibility of backend systems and services

Resources

- CPU utilisation
- Utilisation of network interfaces
- Utilisation of persistent and volatile memories

Performance

- Application Performance Index (Apdex)
- Application response times
- Response times of back-end systems
- Query times for database contents

Security

- See section “Intrusion Detection / Malware Detection / Logging of security-relevant events”.
- Update status of systems

Monitoring

- Error logs
- Access logs

In addition to this automated monitoring, DST employees monitor relevant online media and blogs for the disclosure of security vulnerabilities in order to be able to react to them promptly.

Security Audits and penetration tests

Personio conducts both internal and external security tests at regular intervals. In addition, the security of the Personio application is regularly checked for possible vulnerabilities by an external, independent provider (results of the last penetration test as well as the data protection audit report are available on request, a summary of the last data protection audit can be found on our data protection website under downloads). Furthermore, internal audits are also carried out, in which not only the technical, but also the organisational measures within the company are examined for their effectiveness.

Finally, we would like to refer you to our data protection website personio.com/data-security, where you can view or request further information and documents on the subject. Should any questions remain unanswered, please do not hesitate to contact privacy@personio.de.

Personio

The People Operating System

https://www.personio.com / privacy@personio.de