Security Concept

Data security at AEB

Technical and organizational measures / Controls

October 12, 2024; V4.2

Contents

1 About this document

This document outlines all the security control systems for the services of AEB SE.

The measures can be both technical and organizational in nature. They reflect the state of the art and also incorporate the human factor.

AEB has the right to adjust the necessary measures as long as this does not lower the security level already in place. The measures outlined here are, unless otherwise stipulated, general in nature in that they are the same for all customers.

The date serves as the document version.

The Security Concept includes the purposes data protection and data security and describes them independently from each other. This may result in duplicates with additional information regarding some aspects.

1.1 Data protection

Article 32 of the EU General Data Protection Regulation (GDPR) and other applicable laws mandate the selection of appropriate technical and organizational measures to satisfy the legally defined level of protection of (personal) data (hereinafter PII). Measures are required only insofar as the resources involved are reasonable in relation to the intended purpose of the protection.

1.2 Data security

This document outlines the current security measures and principles at AEB, which form the minimum requirements of any AEB contract (based on the General Terms and Conditions or Service Level Agreement).

2 General

2.1 Certifications

AEB makes its security certificates available in the Trust Center at: https://www.aeb.com/en/trust-center/certificates.php.

2.2 Application process control

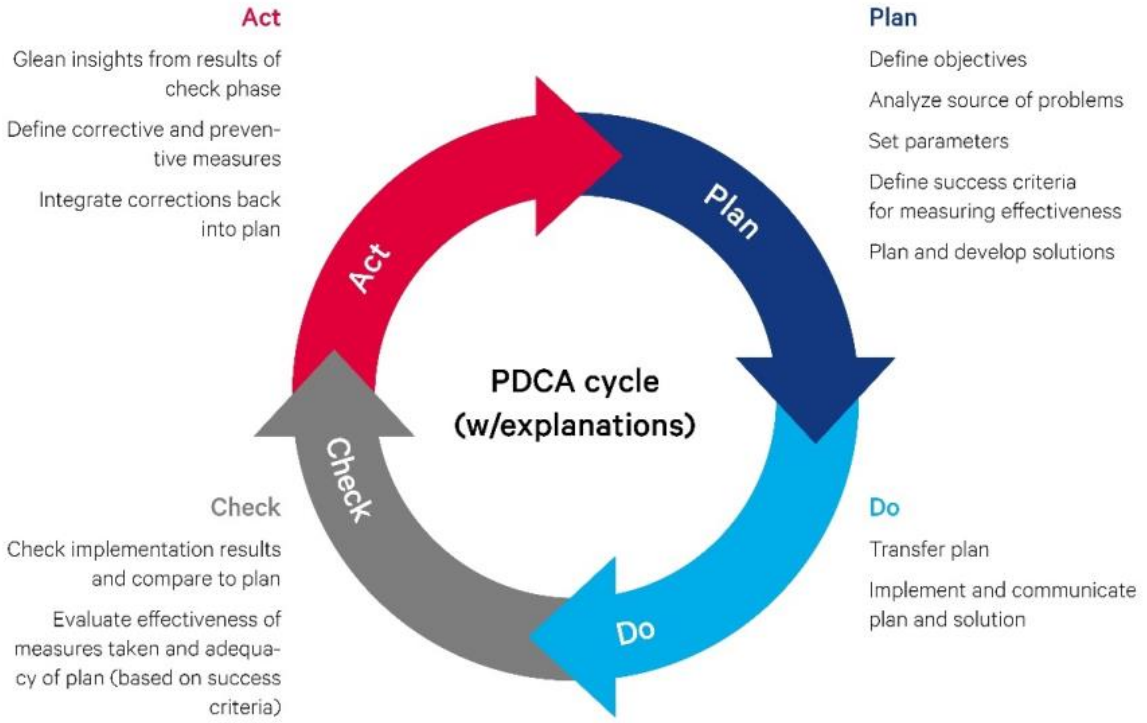
>> To ensure that applications are correctly implemented and process data correctly

- Both the services and the associated technologies and processes are tested by the ATLAS coordinating office at the Karlsruhe Regional Finance Office and certified only if all requirements are met.

- The ATLAS coordinating office also has access to the testing and certification logs.

2.2.1 Quality assurance

Quality is a top priority throughout AEB and is assigned a special status. Task and process managers define, optimize, and check the application development processes as well as the maintenance and service processes on the basis of the PDCA cycle.



The application testing includes both functional and usability tests. Each update is subject to multiple testing and approval phases. Constant monitoring and implementation ensures that the latest technical requirements are met. Maintenance and service is evaluated and optimized in close cooperation with customers. The work method is service- and process-oriented.

2.2.2 Quality assurance through defined processes

All new development steps and application maintenance proceed according to defined and communicated processes (principle of transparency). All application development and maintenance tasks are executed as projects with a defined project workflow (manifested in sample projects) and a defined process. A comprehensive role concept with various levels of two-person approvals is integrated into the process. Provisions for security checks are also in place to ensure compliance.

2.2.3 Quality assurance through external auditors

Where necessary, applications are tested and certified by external auditors.

This testing and certification is based in part on IDW auditing standards and opinions such as IDW AuS 330 (“Auditing for the Use of Information Technology”) or IDS RS FAIT 1 (“Principles of Proper Accounting for the Use of Information Technology”).

AEB is audited annually in accordance with both the German (IDW PS 951 Type 2) and international standard (ISAE 3402). These correspond to the American SOC 2.

Audits are currently carried out for the following services:

- Export Filing: ATLAS
- Compliance Screening
- Export Filing Platform
- Origin and Preferences

from the AEB Cloud.

2.3 General organizational control (management systems)

2.3.1 Data protection

The company’s data protection officer checks and monitors compliance with the applicable legal requirements. The data protection officer is part of the data protection management system and has a Data Protection Guideline available. Some of the controls set forth below are mandatory under Article 32 GDPR (“technical and organizational measures for ensuring the security of the processing”), also taking into account the data protection impact assessment.

2.3.2 Security control, risk management

The information security management system (ISMS) with ISO 27001 certification ensures that IT security is managed as a continuous process-orientated PDCA cycle. This process, which is based on assets (information and values), includes a determination of necessary protections and detailed risk observations (risk assessment and treatment).

The most important and relevant protection objectives are:

- Availability
- Confidentiality
- Integrity

The ISMS contains controls during the check phase – internal and external audits, etc. – as well as regular management evaluations. Various measures to train and educate employees add another level by ensuring a high level of security awareness.

For a comprehensive description, refer to our information security guideline (part of the Guideline Integrated Management System) in our Trust Center at https://www.aeb.com/en/trust-center/security.php.

3 Data protection – Technical and organizational measures

The following classification of measures is, for the time being, still based on Germany's (old) Federal Data Protection Act (BDSG) in the version valid until May 25, 2018.

Classifications can also be derived from the EU's General Data Protection Regulation (GDPR) that came into effect on May 25, 2018 – using, for example, the protection objectives of availability, confidentiality, integrity (and resilience). For more information on AEB's data protection as a cloud provider, please refer to the chapter on ISO 27018.

3.1 Input control

>> To ensure that it is possible to subsequently check and determine whether and by whom data, especially personal data, was entered into data processing systems, modified, or deleted

- All systems that process personal data keep a log of all data entry, modifications and deletions. This logging ensures that it can be subsequently determined whether and by whom personal master data has been entered, modified, or removed.
- Personalized user accounts also in the specialist applications.
- Separate system logs and application logs, ruling out manipulation of the application logs at the system level
- GDPR assignment: Integrity

3.2 Order control

>> To ensure that personal data from orders can only be processed according to the client's instructions

- Regulation of instructions in principal service and data processing agreement
- Administration of users and rights by client at application level
- Transfer/entry of data by the client. The client decides when and what data is transferred.
- Access to this data limited to roles with corresponding access rights
- Automated processing of the data by certified software (ATLAS procedure, Compliance, etc.). This ensures that the data is processed in accordance with the contracted procedure.
- Use of standardized contracts as stipulated by law for relations with customers and service providers
- Employees are regularly reminded of the need-to-know principle and their obligation of confidentiality
- Inclusion of subcontractors with corresponding confidentiality, data processing, system access agreements
- GDPR assignment: Availability, confidentiality

3.3 Separation control

>> To ensure that data collected for different purposes can be processed separately

- Separation of:
  – Employee data
  – Customer contact data
  – Customer test data (project work, customer developments)
  – Remote maintenance access data
  – Customer data in AEB data center
- System level:
  Customer data in data center administered in strict separation and in separate systems (databases, etc.) from AEB data (including the CRM system)
- Different applications:
  Customer data and employee data processed using separate applications
- Rights within the application:
  Customer contact data strictly separated from remote maintenance access data
- GDPR assignment: Confidentiality, availability

3.4 Physical access control

>> To block unauthorized parties from physical access to data processing systems that process and use data, especially personal data

At the Stuttgart headquarters (data center):

- There are three areas: public area, private area, and specially protected area. All access points are secured by locks with transponders
- The issuing and return of transponders is documented
- The Security Guide includes instructions for employees on how to deal with guests
- All public access points as well as delivery and loading areas are outside of the security zones. Inbound deliveries in security zones are always supervised.

Other sites have special provisions in place for on-site security measures that satisfy the minimum AEB standard. These provisions are also in the Security Guide.

- Multi-level technical locking systems, in some cases with alarm equipment
- Building security and identity control of all persons present outside of business hours by security staff
- Regulation concerning physical access rights for non-employees
- Central storage for issuing electronic code keys (tokens), recording of issue and return

- Server and infrastructures (remote maintenance routers, etc.) protected by controlled access (coded locks, code keys) to the server room
- Video monitoring of central areas and system-critical components
- Remote maintenance systems secured as follows:
  - Access to remote maintenance for authorized persons only
  - Systems for remote maintenance access to customers located in an isolated network environment
- GDPR assignment: Confidentiality, availability

3.5 User access control

>> To prevent unauthorized parties from using data processing systems

- Workstation computers secured as follows:
  - User login only through centrally controlled identity management system
  - Requirement for employees to lock workstation computers
  - Workstation computers automatically locked after a maximum of 15 minutes of idle time
  - Personal access code required or biometric recognition to unlock computers
- Centralized password guidelines:
  - For administrative access (requirement to regularly change passwords, minimum requirements for password length and complexity, two-factor authentication)
  - For employee access (minimum requirements for password length and complexity, two-factor authentication)
  - For customer access (requirement to regularly change passwords, minimum requirements for password length and complexity)
- GDPR assignment: Confidentiality, availability, integrity

3.6 Electronic access control

>> To ensure that those authorized to use a data processing system can only access the data for which they are authorized and that data, especially personal data, is not subject to unauthorized viewing, copying, modification, or deletion when it is processed or used or after it is stored

- Central rights management, separated for system access and application access
- Controls to prevent users from changing their own rights
- Controls to prevent users from requesting a change without the approval of the person in charge (superior, role manager,...) in accordance with the established approval process
- External access restricted to VPN- or SSH-secured connections
- Data encrypted for storage (in databases, etc.)

- Security checks / penetration tests of external access carried out by appropriately specialized companies
- Regulations for changes of jobs or roles within companies
- Access authorization reviewed whenever processing operations are initiated or modified
- GDPR assignment: Confidentiality, availability, integrity

3.7 Transmission control

>> To ensure that data, especially personal data, cannot be viewed, copied, modified, or deleted without authorization while it is transmitted electronically, transported, or saved to storage media and that it is possible to check and determine the intended destinations of data, especially personal data, transferred using data transmission equipment

- All transmission of unencrypted data prohibited by enterprise-wide security guide
- All download/upload internet connections secured through either SSL/TLS, SSH, or VPN
- All branch offices and mobile systems using only VPN- or SSH-secured connections controlled by AEB
- No local storage of personal data; all data stored centrally in the systems of AEB
- External connections possible only through approved applications
- External connections possible only through approved services
- All remote data transfer connections logged wherever technically possible
- Regulations for the disposal of waste with confidential content in compliance with relevant DIN regulations (concerning the protection class and security levels)
- Legal admissibility, suitable guarantees, etc. are contractually ensured.
- The need-to-know principle applies
- GDPR assignment: Confidentiality, availability, integrity

3.8 Availability control

>> To ensure that data, especially personal data, is protected against random destruction or loss

- Redundant systems
  – Database: Cluster (where required)
  – File server: Cluster
  – SAN/storage: redundant components
- Uninterrupted power supply (UPS), including emergency power system
- Fire alarm and extinguishing systems

- Tape backup
  - Regular tape backups
  - Data storage in separate fire containment section / separate building
  - Additional regular backup of user data during the day using database tools
- Early detection of system-critical states through monitoring and alerting
- Maintenance of emergency concept (business continuity management) to prevent and deal with emergencies
- Regular testing of data security / backup systems, etc.
- GDPR assignment: Availability, durability

3.9 Pseudonymization and encryption

>> To ensure that traceability of data to individuals is at least restricted

- Privacy-by-design and privacy-by-default measures, including the appropriate training for product teams and based on the principles of avoiding and limiting data
- All download/upload internet connections secured through either SSL/TLS, SSH, or VPN
- Standard process for hard-drive encryption of employees' clients
- Remote wiping option for mobile devices, use of mobile device management (MDM)
- Currently no plans to pseudonymize the data, as personal data is of a business (not personal) nature and business interests, including ability to ensure tamper-proof data management, outweigh personal interests

3.10 Restoration and reliability

>> To ensure that deployed systems can be restored in the event of a problem and that all functions of the system are available and any malfunctions reported

- Established incident management with corresponding roles for processing incidents
- Early detection of system-critical states through monitoring, automatic repair of abnormalities, and notifications through alerting
- Automated failover mechanisms, especially virtualization, reduce the impact of hardware failures
- Availability of an emergency management process and measures, including regular exercises
- Availability of a business continuity management process and measures to prevent and deal with emergencies.
- Availability of backup systems

Information, software, and system images are backed up every 24 hours at the latest using a multi-stage concept. In addition to a local backup on disk, encrypted data carriers are available at a secure remote location.

The backups are tested regularly, randomly at least once a month. A full restore test/DR test is carried out at least once a year.

Details about the backup concept can be found in the document "Excerpt from the AEB security concept: details about backups," available in the AEB Trust Center.

For cloud operation, the following also applies: More details can be found in the Service Description (AEB Cloud or AEB Private Cloud) and in further documents in the AEB Trust Center.

3.11 Ensuring resilience

>> To ensure that sufficient resilience or robustness is always present

- Process-oriented operation of ISMS, including regular inspection for vulnerabilities and threats to reinforce sustainability
- Maintenance of an overview of processing activities with integrated assessment of consequences for data protection and assessment of the appropriateness of technical and organizational measures
- Integration of privacy by design in product management: triggering of advance control by procedural manager together with the data protection officer, also for assessment of consequences for data protection (administration of processes including checks, coordination, analysis, and evaluation)
- Specific checks using penetration tests
- Use of next-generation firewall
- However also monitoring Monitoring to ensure early detection and at least limit or even prevent damage due to malware
- Availability of buffers (resources) to absorb unusual load spikes
- Regular reminders on the background and procedures in the event of data breaches
- Regular emergency drills (BCM) to provide insight into possible improvement measures for prevention

3.12 Regular effectiveness checks

>> To ensure the security of the processing; with a process for a regular efficacy review and evaluation

- Internal and external ISO 27001 audits, data processing
- Regular checks of technical and organizational measures with responsible roles, including whether they reflect the state of the art
- Inclusion of possible references (for standard data protection model, etc.)

- Targeted, regular penetration testing, including analysis and follow-up on results
- Management evaluations as a regular routine with Executive Board and data protection officer
- Operation of data protection as a DSMS (Data Protection Management System)

3.13 Addressing (potential) risks

>> To ensure that a risk assessment is included in processing or selection of appropriate technical and organizational measures

- ISMS with associated processes, roles, and tools
- Separate consideration of risks from the perspective of those affected
- Assessment of consequences for data protection with integration into procedures and processing activities, with possible inclusion of relevant supervisory authority
- Consideration of applicable technical guidelines and recommendations of Federal Office for Information Security (BSI) where relevant for processors
- Process-driven recalibration to reflect current conditions and any changes (likelihood of risk scenarios, etc.)

3.14 Preventing concatenation

>> To ensure that data is used only for the purpose for which it was collected (purpose limitation principle)

- Use of role concept to limit processing, use, and transmission rights
- Programmed omission or closure of interfaces in procedures and procedure components
- Rules prohibiting backdoors, quality assurance audits to check compliance in software development
- Functional separations based on role concept
- Separations through role concepts with phased access rights based on identity management and a secure authentication process
- Structured processes for modifying purpose (taking into account legal basis, necessity, compatibility)
- Regular awareness training

3.15 Transparency

>> To ensure that obligations to provide information are met

- Records of processing activities pursuant to Art. 30 GDPR (both as controller and as processor)
- Data protection statement on AEB website (see AEB Trust Center)
- Support for obligations to provide information under Art. 30 GDPR, outlined in data privacy portal of AEB
- Integration of data protection checks in the process for approving products and applications
- Notification of workforce of rights of data subjects to receive information
- Documentation of contracts with internal employees, contracts with external service providers and third parties from whom data is collected or to whom data is transmitted
- Process for operating procedures with procedural managers with regular exchange
- Process for conduct in case of procedures under Chapter 3 GDPR (Rights of the data subject)

3.16 Possibility of intervention

>> To ensure that data subjects can exercise their rights to intervene

- Documented processing of disruptions, troubleshooting, and changes to the process and to the protective measures for IT security and data protection
- Option for individual functionalities to be disabled wherever possible without impacting overall system
- Option for activities of controller to be tracked to ensure rights of data subjects
- Process for interaction between controller and processor to deal with transactions of data subjects
- Active option for compilation, consistent correction, blocking, and deletion of all data stored for a particular person
- Regular reminders regarding the duty to cooperate (for internal and external parties)

4 Information Security Controls from ISO 27001 / Annex A / SoA

The following controls are derived from ISO 27001:2023, Annex A.
Their nomenclature is based on the following levels:

- Security category (A.5)
- Control (A.5.1)

This document provides information from AEB on the requirements for all controls.
Each control is assigned to a control owner. Controls are maintained through a managed process, including a regular review that considers the current state of the art and other factors.

The following list can thus be used as a Statement of Applicability (SoA).
The following applies to all controls:

- There are no exclusions
- All requirements have been implemented and are active

AEB has extended ISO 27001 to include ISO 27018. Statements regarding this standard can be recognized by the respective addition **"For cloud operation, the following also applies: …**". Additional controls from Annex A of ISO 27018 that are assigned to the data protection principles can be found in the separate chapter **"Information Security Controls from ISO 27018 / Annex A"**.

4.1 A.5 – Organizational controls

4.1.1 A.5.1 – Policies for information security

>> Information security policy and topic-specific policies should be defined, approved by management,

published, communicated to and acknowledged by relevant personnel and relevant interested parties,

and reviewed at planned intervals and if significant changes occur.

The "Integrated Management System" (IMS) Guideline defines how information security is managed.

The internal Security Guide establishes the security policies.

Both documents are policies subject to our document management protocols. The policies established therein are binding for all employees and partners. They have been approved by management, published, and communicated to employees and relevant external parties.

- The IMS Guideline can be accessed at any time from the AEB Trust Center: https://www.aeb.com/en/trust-center/security.
- The Security Guide can be reviewed in AEB's offices (during an audit, for example).

The documents are subject to a PDCA cycle. They can be modified at any time following approval by the ISMS leadership. Situations that might typically trigger the need for changes include findings in management reviews, especially at the start of a new year. Management reviews are tasked with questioning the policies. The reasons for changes are documented in the ISMS document on corrective and preventive measures, and they can also affect the rules in the policies.

For cloud operation, the following also applies: The IMS Guideline and AEB's Data Protection Guideline make it clear that AEB, as an IT provider, complies with (data protection) legislation and supports its customers as a processor. Accordingly, AEB offers a customized and up-to-date template for Agreements on Processing (in its Trust Center). It clarifies the responsibilities.

4.1.2 A.5.2 – Information security roles and responsibilities

>> Information security roles and responsibilities should be defined and allocated according to the organization needs

The information security responsibilities have been defined and allocated. Persons with defined responsibilities include:

- IT Security Manager responsible for information security, reachable at Security@aeb.com
- Person responsible for ISMS management
- Person responsible for security operations
- Person responsible for software security assurance
- Person responsible for security in the departments
- Data Protection Officer
- Emergency Officer

For more information, please refer to our IMS Guideline in the AEB Trust Center: https://www.aeb.com/en/trust-center.

4.1.3 A.5.3 – Segregation of duties

>> Conflicting duties and conflicting areas of responsibility should be segregated.

The segregation of duties and roles is part of our Internal Control System (ICS). We also work with and manage roles very closely. These roles incorporate responsibilities, tasks, and skills and are linked to the authorization concept. We keep a list of role conflicts and consult it when allocating roles.

For more information, please refer to our IMS Guideline in the AEB Trust Center: https://www.aeb.com/en/trust-center/security.php.

4.1.4 A.5.4 – Management responsibilities

>> Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

All new employees complete a mandatory training program, and their participation is documented. This training program has a defined curriculum that includes information security. Management subsequently ensures regular security briefings for all employees. The responsibility for knowing the content of these briefings lies with the employees themselves and their supervisors.

4.1.5 A.5.5 – Contact with authorities

>> The organization should establish and maintain contact with relevant authorities.

Authorities we deem relevant:

- Baden-Württemberg Ministry of the Interior (State Data Protection Officer)
- Chamber of Commerce and Industry
- Federal Office for Information Security (BSI)
- Other authorities in Germany, the EU, non-EU Europe, …

Internal committees and responsible roles maintain these relevant contacts.

Maintenance of contacts also includes visits to congresses or continuing education opportunities (e.g. offered by the State Commissioner for Data Protection or the Chamber of Commerce and Industry).

4.1.6 A.5.6 – Contact with special interest groups

>> The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.

The same statements made above under "A.5.5 – Contact with authorities" apply here as well.

Contacts to security-related professional associations or interest groups are maintained by the appropriate persons (such as the Data Protection Officer) and used as needed. A variety of network and media are used, including newsletters, magazines, forums, and webinars.

4.1.7 A.5.7 – Threat intelligence

>> Information relating to information security threats should be collected and analyzed to produce threat intelligence.

AEB differentiates between attack paths, motives, and threat intelligence.

AEB uses BSI modules to ensure appropriate protection of attack paths.

Potential motives and threat intelligence are dynamic and are regularly reviewed to reassess the presumed probabilities of occurrence if warranted by the risk management assessment.

This is achieved through specially convened ISMS roundtables augmented by the findings obtained from technical sources, security incident reports, and penetration tests.

Training sessions raise awareness of the methods, tools, and technologies of potential attackers.

4.1.8 A.5.8 – Information security in project management

>> Information security should be integrated into project management.

Security checks are integrated into projects (characteristic B).

These checks are carried out by the project managers with the support of a security employee and include an assessment of the necessary protections:

- Availability (systems in the AEB Cloud, etc.)
- Confidentiality and data protection
- Integrity

A documented change request and release management process is also used to track changes in the project. Both in standard development projects and customer projects, (security) standards for program code and interfaces are applied.

4.1.9 A.5.9 – Inventory of information and other associated assets

>> An inventory of information and other associated assets, including owners, should be developed and maintained.

- Clients and client components are inventoried and managed with the help of a tool.
- The inventory of assets is an early phase of the recurring process in the operation of our ISMS.
- The inventory is managed in our internal risk management tool.
- The inventory process includes checking and documenting that each asset has an owner.
- The owner can also be linked to a role.
- The role includes the responsibility for effective implementation of the protective measures. Those responsible can consult the internal ISMS Guide for more detailed instructions.

4.1.10 A.5.10 – Acceptable use of information and other associated assets

>> Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented, and implemented.

Rules and their implementation are based on specifications for the protection objectives defined in policy documents like the Security Guide and ISMS Guide, which define criteria used to classify acceptable use. Specific requirements for protection are defined and managed in the internal risk management tool within the larger context of the ISMS.

The complete procedure for handling assets can be found in AEB's internal ISMS Guide.

We provide guidance on how to implement labeling requirements.

Monitoring and regular maintenance of our data protection–related processing activities is achieved by applying the rules of our internal data protection management system to the log of processing activities.

4.1.11 A.5.11 – Return of assets

>> Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract, or agreement

Our personnel management software automatically generates a task in the form of a checklist for the return of assets when an employee leaves the company and checks to ensure this task has been completed. The persons responsible ensure the appropriate implementation and documentation. The personnel management software also generates a task to track the return of the transponder.

4.1.12 A.5.12 – Classification of information

>> Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.

- AEB classifies information and documents
- The benchmark reference here is our IMS Guideline (available in the AEB Trust Center: https://www.aeb.com/en/trust-center/security.php).
- Protection objectives and a software tool are used to classify the need for protection at the level of individual assets.
- The need for protection is then the basis for subsequent risk assessments, such as a data protection impact assessment.

4.1.13 A.5.13 – Labeling of information

>> An appropriate set of procedures for information labeling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

This set of procedures derives from:

- The selection of the internal risk management tool
- Its user documentation
- The help in the risk management tool, which serves as a bridge between the user documentation and our ISMS Guide

The business impact is represented at the process or asset level, where information on availability, confidentiality, and integrity is provided. Select from predefined values (from "insignificant" to "threatening"). The internal specification provides assistance in making the right selection.

Documents are subject to managed document control.

4.1.14 A.5.14 – Information transfer

>> Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.

General:

AEB has agreements within the organization and with external parties on how to handle the transfer of data (data on the move). Corresponding procedures and controls have been implemented and are being applied.

Specifically, these rules are established and communicated in the Security Guide and Partner Management Guide policy documents.

The partner agreements can also be found in the corresponding contracts, including the non-disclosure agreements (NDAs), partner agreements for system access, the various service descriptions (which are part of the contract), and the service level agreements (SLAs) with the individual customers.

Details

AEB differentiates networks in “zones” as follows:

- Each external network, such as a customer’s or carrier’s network, is one zone.
- Internally, the network is highly segmented by design, specifically through VLANs that separate the various areas from one another: one zone for employees, one for guests, one for specific services, etc.

The transition / data transfer between two zones is called a “zone change.”

All data that is transferred is encrypted at the latest when it undergoes a zone change.

The encryption is typically at least TLS 1.2 (with AES 256-bit).

4.1.15 A.5.15 – Access control

>> Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.

Access to networks and network services is established using role-based groups and corresponding group assignments. The necessary rights are assigned through the corresponding roles. Networks are highly segmented, and each segment is protected by next-gen firewalls.

General approach:

- Need-to-know principle
- As much access as necessary, as little as possible

Both the access control policy, compliance with access control, the relevant systems and networks, and the roles with their rights are regularly reviewed at least once a year.

4.1.16 A.5.16 – Identity management

>> The full lifecycle of identities should be managed.

AEB creates and manages four types of user accounts:

- User accounts for internal purposes (employees, partners)
- User accounts for accessing AEB Cloud solutions (customers, partners)
- Privileged user accounts for internal purposes (employees)
- Privileged user accounts for administering own Cloud solutions (customers)

For all user account types, processes have been defined and implemented that ensure the correct registration and de-registration of users. Employee accounts are automatically created when a new employee joins the company, for example, then automatically deactivated when the employee leaves the company and automatically deleted after a defined period. Accounts are administered via centralized identity and access management (IAM), for example.

AEB performs checks for unused access data at regular intervals. If any compromise is identified, an organizational process is used to reset the affected accounts.

For cloud operation, the following also applies: The configuration guide in the AEB Service Portal also includes information about setting up users for the administrator of the own client (I_CLIENTADMIN).

4.1.17 A.5.17 – Authentication information

>> Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.

AEB uses a formal process to control the allocation, management, and handling of secret authentication, which AEB always stores in encrypted form. AEB employees use a password tool for this. The rules for this are documented in the internal Security Guide.

AEB manages passwords using a state-of-the-art central password tool that, among other things, ensures:

- Use of strong passwords
- Role-based rights concept for physical and electronic access by password or password group
- Log of all changes
- Log of all accesses

Various policies establish the requirement to use the password tool in all situations.

4.1.18 A.5.18 – Access rights

>> Access rights to information and other associated assets should be provisioned, reviewed, modified, and removed in accordance with the organization’s topic-specific policy on and rules for access control.

See also A.5.16 – Identity management.

Tasks are automatically created in the personnel management software and/or internal ticketing system whenever an employee joins or leaves the company or changes responsibilities (moves to a different role or team, etc.), and the roles and rights are also reviewed here.

Accounts and rights in all objects relevant for access to information (directories, accounts, roles, applications, etc.) are checked by the responsible persons at regular intervals (at least annually).

Checks on unused access data are also carried out at regular intervals (at least annually). If any compromise is identified, an organizational process is used to reset the affected accounts.

4.1.19 A.5.19 – Information security in supplier relationships

>> Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

AEB has established partner management and application management frameworks to ensure this.

- The Integrated Management System (IMS) Guideline also takes supplier relationships into account in the areas of quality and security.
- The security criteria by level of access are reflected in the agreements for system access by partners. These are regularly checked and partners are audited accordingly.
- Standard confidentiality agreements are available, and NDAs are also used, such as when guests sign in.
- Agreements covering third-party data processing are also in place.

4.1.20 A.5.20 – Addressing information security within supplier agreements

>> Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.

Suppliers and partners are classified and, depending on this classification and any identified need for protection, information security requirements for suppliers and partners are defined. The Integrated Management System (IMS) Guideline also takes supplier relationships into account in the areas of quality and security.

The security criteria by level of access are also reflected in the agreements for system access by partners.

Partners are regularly checked and audited based on their classification.

Standard NDAs cover confidentiality. Guests are also prompted to accept them when signing in.

4.1.21 A.5.21 – Managing information security in the ICT supply chain

>> Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. (ICT = information and communications technology)

AEB has established a partner management and application management system to ensure that requirements are included in agreements with suppliers. These agreements address and define the interaction with information security risks associated with information and communications technology services and product supply chain.

See also A.5.20 – Addressing information security within supplier agreements.

4.1.22 A.5.22 – Monitoring, review, and change management of supplier services

>> The organization should regularly monitor, review, evaluate, and manage change in supplier information security practices and service delivery.

The provision of services by suppliers and any changes to them are monitored, regularly reviewed, and audited. This is controlled and ensured through partner management and the processes established there.

4.1.23 A.5.23 – Information security for use of cloud services

>> Processes for acquisition, use, management, and exit from cloud services should be established in accordance with the organization's information security requirements

Cloud services, like all other applications, are subject to extensive application management that places a particular focus on security and data protection, and on the analysis and regular review of providers.

In addition, AEB has defined special terms and conditions for the cloud services it uses.

4.1.24 A.5.24 – Information security incident management planning and preparation

>> The organization should plan and prepare for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles, and responsibilities.

The process for reporting security incidents is organized and regularly communicated. The reporting allows several options for triggering and is processed with the help of tools. Possible recipients (for IT security incidents, data breaches, emergencies) have been established through roles and trained.

For cloud operation, the following also applies: AEB has established an internal process for reporting and handling data breaches. Among other things, the criticality is analyzed according to the safety criteria and

taken into account in the further procedure. If necessary, the process provides for cooperation with the affected customers as agreed.

4.1.25 A.5.25 – Assessment and decision on information security events

>> The organization should assess information security events and decide if they are to be categorized as information security incidents.

AEB has implemented security incident processes to ensure that they are reported and handled as quickly as possible through appropriate management channels.

This includes processes for both normal operations (the Security Event Management process) and exceptional circumstances (Security Incident Management process and processes in the Emergency Guide and in Business Continuity Management (BCM) and for data protection in the event of data breaches).

Regular meetings are also held at which the criticality of reports is assessed.

4.1.26 A.5.26 – Response to information security incidents

>> Information security incidents should be responded to in accordance with the documented procedures.

AEB has implemented security incident processes to ensure that information security events are reported and handled as quickly as possible through appropriate management channels.

This includes processes for both normal operations (the Security Event Management process) and exceptional circumstances (Security Incident Management process and processes in the Emergency Guide and in Business Continuity Management (BCM) and for data protection in the event of data breaches).

4.1.27 A.5.27 – Learning from information security incidents

>> Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.

AEB has established a security incident process. This includes following up on the knowledge gained from security events and taking long-term action. The same applies to the emergency process and the response to data breaches.

Regular meetings also ensure that knowledge is evaluated and used.

4.1.28 A.5.28 – Collection of evidence

>> The organization should establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.

AEB has defined and applies procedures for the identification, collection, acquisition, and preservation of information that can serve as evidence.

4.1.29 A.5.29 – Information security during disruption

>> The organization should plan how to maintain information security at an appropriate level during disruption

AEB has process management in place that includes various security phases. The statuses and associated actions of each phase are documented and communicated through training. The Security Incident Management process takes effect as soon as a disruption occurs. Particular emphasis is placed on the transitions toward further escalation and emergency management, and on the tools to be applied at each phase, including the involvement of additional roles and the application of additional guides such as emergency plans.

AEB has defined its requirements for information security and the continuity of information security management in adverse situations, such as during a crisis or disaster, and has positioned itself accordingly.

A management system for BCM is in place and includes the perspectives of emergency prevention and emergency response.

This is documented here, among other places:

- https://www.aeb.com/en/trust-center/security.php#Emergency-preparedness

An emergency officer has been appointed to ensure that the BCM requirements are met. This officer takes appropriate precautions in consultation with the Executive Board and the affected resources, such as in infrastructure and IT. Regularly scheduled and conducted drills help to respond to emergencies with maximum preparedness and close any gaps. As part of this, contingency plans are developed and maintained.

Verification of effectiveness is part of the Emergency Concept. The emergency preparedness concept and associated BCM project provide for emergency drills, for example. These drills are jointly designed, implemented, and evaluated for sustainability with an eye on criticality. The status of continuity is documented through regular availability reports. The dates for planned maintenance work also regularly include failsafe testing.

Regular reporting on BCM is in place (emergency officer together with IT security and management).

Regular exchanges are conducted to assess the need for new emergency drills.

4.1.30 A.5.30 – ICT readiness for business continuity

>> ICT readiness should be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.

- AEB breaks down the task into emergency prevention, ongoing preparedness, and response.
- The objectives are high availability, awareness, and resilience in the areas of prevention (avoidance wherever possible) and response (minimization of duration and extent of damage) with a view to AEB and its customers.
- Our BCM Guideline takes precedence.
- Results include security KPIs in connection with emergencies.
- Requirements include maintaining up-to-date supporting emergency plans, conducting emergency drills and evaluating the findings to improve resilience and awareness, and training affected organizational units up to the crisis management team.
- A roadmap to a BIA (Business Impact Analysis), drawing on data from the ISMS risk tool, is used to focus on critical processes. The roadmap integrates RTO and RPO assessments.

4.1.31 A.5.31 – Legal, statutory, regulatory, and contractual requirements

>> Legal, statutory, regulatory, and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented, and kept up to date

AEB has defined procedures and measures to ensure that all legal, statutory, regulatory, and contractual requirements relevant to information security are always met.

This includes both regularly reviewing these requirements and ensuring that they are identified and documented, as well as continuously reviewing and adapting the relevant documentation and processes to meet current standards and regulations.

A compliance officer has been installed and entrusted with the task of identifying the relevant rules and obligations and ensuring that their observance in the organization is managed.

Customers, partners, and employees already have access to comprehensive information in the AEB Trust Center: https://www.aeb.com/TrustCenter/. In the case of further questions or extended requirements, we negotiate individual contracts with the customers through our Legal team or provide further information through our Compliance team (including tender management, where applicable).

Some of the components are listed below:

- ISMS
- Code of Conduct (EN)
- Anti-Corruption (EN)
- AGB 3.0

We have set up a whistleblower system to report violations of the law, our Code of Conduct, or our compliance guidelines. Our legal ombudsman accepts tips confidentially.

AEB's data storage is located in Germany. During data transfer (including use), the applicable data protection requirements are observed. Further information is available at https://www.aeb.com/en/trust-center/data-centers.php.

A policy on the use of cryptographic controls for protection of information has also been developed and implemented. It is referenced in the internal Security Guide.

4.1.32 A.5.32 – Intellectual property rights

>> The organization should implement appropriate procedures to protect intellectual property rights.

Compliance with the requirements relating to intellectual property rights and the use of proprietary software can be ensured by appropriate license agreements or corresponding passages in AEB SE's General Terms and Conditions and by the appropriate processes. The use and conditions of third-party open-source and proprietary software is outlined here transparently by AEB for its contractual partners: https://documents.aeb.com/licenses/xnsg_nsg/en/index.html. Contractual partners can also find a list of third-party components here.

4.1.33 A.5.33 – Protection of records

>> Records should be protected from loss, destruction, falsification, unauthorized access, and unauthorized release.

Unless otherwise required, we keep everything for 10 years. Electronic storage is subject to the rules for data backup as documented in the Security Guide under "communication, documents, and data."

Related customer inquiries are forwarded internally to the responsible roles without delay.

4.1.34 A.5.34 – Privacy and protection of personally identifiable information (PII)

>> The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

A company data protection officer has been appointed to ensure compliance with the relevant data protection laws. This person can turn to our in-house counsel or an outside attorney for IT law. Employee training and continuing education measures on these topics and on ensuring awareness are in place. External partners can contact AEB through our Trust Center (https://www.aeb.com/en/trust-center/data-protection.php).

Questions about the legal basis, legitimacy, and appropriateness are integrated into auditing processes (for example, for applications or in the procedure directory).

A regularly revised security concept includes technical and organizational measures to protect PII using state-of-the-art technology.

4.1.35 A.5.35 – Independent review of information security

>> The organization's approach to managing information security and its implementation including people, processes, and technologies should be reviewed independently at planned intervals, or when significant changes occur.

We subject our ISMS to regular external ISO 27001 certification audits for this purpose.

Additional third-party audits are performed for purposes such as verifying data security for our data protection management system. In some cases, the audits of the technical and organizational measures (TOMs) in accordance with Article 28 of the GDPR by our business partners can also be evaluated as part of the third-party data processing audits.

For cloud operation, the following also applies: AEB offers its customers a wide range of information to assure themselves of proper operation. AEB has itself be audited by independent, accredited bodies and provides appropriate evidence such as certificates.

4.1.36 A.5.36 – Compliance with policies, rules, and standards for information security

>> Compliance with the organization's information security policy, topic-specific policies, rules, and standards should be regularly reviewed.

AEB has a multi-stage concept for this:

- Security and compliance roles tasked with ongoing responsibility and review
- Regular exchanges with the IS Board, Compliance team, and others to address topics including changes in security requirements.
- Maintenance of a documented overview of relevant requirements, including any potential requirements
- Regular internal audits with cross-checking of relevant security policies and sample testing, building rounds
- Regular reminder and refresher training
- Project- and ticket-driven checks to ensure that the necessary activities are taking place
- Strategic meetings of the Security Working Group
- Review at least annually of the status of requirements by the person responsible on the Board of Directors
- Prompt action whenever any unfulfilled requirement is uncovered

Our compliance with technical and other requirements is also checked through other means:

- Regular testing by IT Operations as part of change management
- An approval process for new applications

- Ongoing responsibility and review by those responsible for the guidelines and the role of the Domain Security Officer
- Regular data protection review by the Data Protection Officer
- Regular ISO 27001 internal audits with cross-checking of the relevant security policies
- Regular external audits
- Regular penetration tests performed by external service providers
- Regular meetings in the Security Network of the Security Working Group
- Regular checks and maintenance of the controls

4.1.37 A.5.37 – Documented operating procedures

>> Operating procedures for information processing facilities should be documented and made available to personnel who need them.

All changes are subject to and controlled by change processes. They are documented in internal guides (such as the Change Management Process, Admin Guide, and Security Guide).

4.2 A.6 – People controls

4.2.1 A.6.1 – Screening

>> Background verification checks on all candidates to become personnel should be carried out before they join the organization and thereafter on an ongoing basis, taking into consideration applicable laws, regulations, and ethics, and be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations, and ethics and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

4.2.2 A.6.2 – Terms and conditions of employment

>> The employment contractual agreements should state the personnel's and the organization's responsibilities for information security

At the start of any contractual relationship, employees and partners sign standardized contracts with an appropriate confidentiality clause that includes data processing. The assignment of responsibilities internally follows a strict role concept and is checked and documented through the allocation of roles.

4.2.3 A.6.3 – Information security awareness, education, and training

>> Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education, and training as well as regular updates of the organization's information security policy, topic-specific policies, and procedures, as relevant for their job function.

New employees must internalize defined security-related content. Regular security campaigns, publications, and training sessions are also actively communicated to all employees, including reminders about existing rules for ensuring compliance with security obligations and notifications of any amendments or updates to these rules.

For cloud operation, the following also applies: AEB monitors IT security incidents and data breaches. Employees are regularly informed about security incident procedures and the significance and possible consequences of violations.

4.2.4 A.6.4 – Disciplinary process

>> A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

The disciplinary process has been implemented and documented.

4.2.5 A.6.5 – Responsibilities after termination or change of employment

>> Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced, and communicated to relevant personnel and other interested parties.

Our personnel management software automatically generates and monitors completion of the information security tasks to be performed when there is a change or termination of employment.

4.2.6 A.6.6 – Confidentiality or non-disclosure agreements

>> Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed, and signed by personnel and other relevant interested parties.

Confidentiality agreements are in place for both internal and external use.

The content is the responsibility of owners (from Legal, Data Protection, and Human Resources) and is regularly maintained.

Changes can stem from audits, legislation, requirements identified in exchanges with business partners (suppliers, customers), changes to the inventory of vulnerable assets, and other sources.

An ongoing dialog in the area of legal, ISMS, and data protection ensures that the agreements are reviewed.

For cloud operation, the following also applies: See also ISO27018 A.10.1 – Confidentiality or non-disclosure agreements (AEB employees are obligated to maintain confidentiality as part of their employment contract and receive regular training on this.)

4.2.7 A.6.7 – Remote working

>> Security measures should be implemented when personnel are working remotely to protect information accessed, processed, or stored outside the organization's premises.

AEB generally allows teleworking (working remotely or from home). Security measures are implemented at both the technical and organizational level. Approvals follow processes. A corresponding policy has been established.

4.2.8 A.6.8 – Information security event reporting

>> The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

AEB has implemented security incident processes to ensure that information security events are reported and handled as quickly as possible through appropriate, known management channels.

This includes processes for both normal operations (Security Event Management process, etc.) and exceptional circumstances (Security Incident Management process, but also processes in the Emergency Guide and in Business Continuity Management (BCM) or for data protection in the event of data breaches).

Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services. This happens in a ticketing system.

Employees are notified of their duty to cooperate in the internal Security Guide and in corresponding training courses.

Customers can contact the AEB Support with all security concerns and reports via the channels available to them. From there, initial reactions but also escalations are controlled.

AEB immediately reports any security incidents it detects to the affected customers.

4.3 A.7 – Physical controls

4.3.1 A.7.1 – Physical security perimeters

>> Security perimeters should be defined and used to protect areas that contain information and other associated assets.

The AEB buildings are divided into various areas:

- Public areas
- Private areas
- Specially protected areas

Depending on the area, there are different authorized groups of people and corresponding security measures, such as logged access, video surveillance, and alarms.

Further documentation can be found in the document on physical and electronic access in the Trust Center.

4.3.2 A.7.2 – Physical entry

>> Secure areas should be protected by appropriate entry controls and access points.

At the Stuttgart headquarters (data center):

- There are three areas: public area, private area, and specially protected area. All access points are secured by locks with transponders
- The issuing and return of transponders is documented
- The Security Guide includes instructions for employees on how to deal with guests
- All public access points as well as delivery and loading areas are outside of the security zones. Inbound deliveries in security zones are always supervised.

Other sites have special provisions in place for on-site security measures that satisfy the minimum AEB standard. These provisions are also in the Security Guide.

4.3.3 A.7.3 – Securing offices, rooms, and facilities

>> Physical security for offices, rooms and facilities should be designed and implemented.

Offices are protected by security mechanisms at the building complex, which include:

At the Stuttgart headquarters (data center):

- Lockable access points (personalized transponders)
- Video monitoring
- Security personnel

Other sites have special provisions in place for on-site security measures that satisfy the minimum AEB standard as set forth in the Security Guide.

Data centers

Data centers, IT facilities (provider rooms, sub-distributors, etc.) are protected by security measures at the building complex.

The following measures are in place in Stuttgart:

- Lockable access points (personalized transponders)
- Video monitoring
- Security personnel
- Personalized PINs (access to data centers)

4.3.4 A.7.4 – Physical security monitoring

>> Premises should be continuously monitored for unauthorized physical access.

The premises are continuously monitored for unauthorized physical access.

At the Stuttgart headquarters (data center):

- Video recording
- Security personnel

Other sites have special provisions in place for on-site security measures that satisfy the minimum AEB standard as set forth in the Security Guide.

4.3.5 A.7.5 – Protecting against physical and environmental threats

>> Protection against physical and environmental threats such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.

For the Stuttgart offices:

- Fire alarm system, sprinkler system, emergency power supply, locking system, security service
- E-check and other checks based on employer liability insurance association specifications
- Other internal documentation on security service and video monitoring

Other work locations meet the standard for on-site security measures.

For the data centers:

- Fire alarm system and early fire detection
- Automatic extinguishing system
- Burglar alarm system and 24x7 security service
- Water alarm system
- Video monitoring

4.3.6 A.7.6 – Working in secure areas

>> Security measures for working in secure areas should be designed and implemented.

- Our own personnel have been instructed on the policies and code of conduct for working in security zones in both normal operations and exceptional circumstances.
- Outside personnel are only authorized to perform work in security zones if registered and approved and under supervision.
- The requirements of the Security Guide for secure areas and the regulations for physical access control apply.

4.3.7 A.7.7 – Clear desk and clear screen

>> Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

(See also A.8.1 – User endpoint devices.) The clean and clear desk policy is in practice and already taught and communicated in the onboarding process.

4.3.8 A.7.8 – Equipment siting and protection

>> Equipment should be sited securely and protected.

This is ensured by the structural measures of the infrastructure and building design. Regular rounds through the building offer further protections.

4.3.9 A.7.9 – Security of assets off-premises

>> Off-site assets should be protected.

Equipment is always protected by passwords, PINs, or the like. Hard disks in desktops and laptops are always encrypted.

4.3.10 A.7.10 – Storage media

>> Storage media should be managed through their lifecycle of acquisition, use, transportation, and disposal in accordance with the organization’s classification scheme and handling requirements.

The procedure for handling removable media is set forth in the internal Security Guide:

- Data is kept in its context whenever possible and not copied to removable media.
- When it becomes necessary for data (especially data containing internal, confidential, or highly confidential information) to be copied to and stored on removable media, it must be encrypted and backed up using appropriate technologies (such as BitLocker).
- This applies in particular to data carriers intended for transport (such as tape backups).
- Such carriers are subject to an additional process that ensures this.

Data storage media are securely destroyed:
A contracting partner collects them, destroys them securely, and certifies this destruction and the entire process to AEB.

The destruction is described in DIN 66399:

- Security class: 2 (= high demand for confidential data) (DIN 66399-1)
- Security level: for hard disks, etc.: H-4 (DIN 66399-2)

A certificate is issued to confirm the destruction of each data carrier.

4.3.11 A.7.11 – Supporting utilities

>> Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.

At the Stuttgart headquarters (data center):

- Modern, certified, approved electrical system
- Electrical system with surge protection and power distribution by area
- Mirrored UPS system 230/400V (A-B configuration)
- Grid backup system (diesel generator) for autonomous operation
- The energy concept implemented during construction allows the building to operate in part autonomously without external energy or power supply (photovoltaic system, DC heat recovery via heat pump, free cooling, sprinkler tank)
- All systems are inspected by VdS on a regular basis

At the AEB offices in Germany:

- UPS-secured grid infrastructure
- Provider connections via two fiber optic connections each and separate transmission technology

4.3.12 A.7.12 – Cabling security

>> Cables carrying power, data or supporting information services should be protected from interception, interference, or damage.

At the Stuttgart headquarters (data center):

- Separate cable routing for power and data lines
- Structured CAT7 cabling and fiber optics
- Data line types marked by distinct colors for cables and labeling
- Documentation of switch ports and cable runs
- Redundant connections for all key components
- Structured CAT7 cabling and fiber optics
- Wi-Fi 6
- Building code requirements for new construction as of 2015–2017
- Electrical inspection in compliance with VdS (annual inspection) and DGUV V3 of the installer
- Computer-controlled connection monitoring system
- Electrical inspection in compliance with VdS (annual inspection) and DGUV V3 of the installer

At AEB's offices in Germany:

- Structured CAT7 cabling and fiber optics
- Separate "network cabinet" for connection and network in a dedicated AEB space
- Documentation of switch ports
- Computer-controlled connection monitoring system

4.3.13 A.7.13 – Equipment maintenance

>> Equipment should be maintained correctly to ensure availability, integrity, and confidentiality of information.

- E-check of all mobile and fixed equipment
- Regular servicing and functional check
- Service contracts
- Regular check (at least annually) of equipment (UPS, climate control, etc.)
- Regular servicing and functional check
- Service contracts
- Periodic replacement of infrastructure

4.3.14 A.7.14 – Secure disposal or re-use of equipment

>> Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Paper, discs, and other devices with data on them are securely destroyed. The disposal of data media is designed in such a way that it is assumed that they contain personal data:

A partner collects them, destroys them securely (on site), and certifies this to AEB, as for the entire process.

The destruction is described in DIN 66399:

- Security class: 2 (= high demand for confidential data) (DIN 66399-1)
- Security level
  - for hard disks, etc.: H-4 (DIN 66399-2)
  - for paper: P-4 (DIN 66399-2)

This also applies to cloud operation.

4.4 A.8 – Technological controls

4.4.1 A.8.1 – User endpoint devices

>> Information stored on, processed by, or accessible via user endpoint devices should be protected.

AEB allows access to AEB data, applications, and networks via employee devices only for

- Company notebooks that are appropriately secured
- Other mobile devices that are centrally administered and secured by AEB using an Enterprise Mobility Management (EMM) solution.

This includes techniques such as conditional access, MDM, or MAM. AEB thus ensures that the relevant security features are in place and that AEB data is sequestered from the user's personal data and applications.

A corresponding policy for BYOD has been implemented and is technically enforced.

4.4.2 A.8.2 – Privileged access rights

>> The allocation and use of privileged access rights should be restricted and managed.

Users with special administrative rights or privileges are consolidated in appropriate role groups, where they are subject to the groups' processes and approvals.

The person responsible for these roles is usually the Head of IT, the IT Security Manager, or a member of the Executive Board.

For particularly privileged rights (firewall access, admin portals, etc.), the user must use a special, personalized administrator account. The "normal" user account will not be granted these rights / cannot be assigned to the respective roles.

4.4.3 A.8.3 – Information access restriction

>> Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.

Access control is established and restricted using role-based groups and corresponding group assignments. The necessary rights are assigned through the corresponding roles. General approach:

- Need-to-know principle
- As much access as necessary, as little as possible

Both the access control policy and the roles with their rights are regularly reviewed at least once a year.

For cloud operation, the following also applies: AEB ensures that when storage space is (re)allocated, it does not contain legacy data. Users do not access memory directly in AEB applications, but only information provided via database.

4.4.4 A.8.4 – Access to source code

>> Read and write access to source code, development tools, and software libraries should be appropriately managed.

Access is possible only for employees involved in development, and this is ensured by role-based access control integrated in the identity management.

4.4.5 A.8.5 – Secure authentication

>> Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.

Access to systems and applications is always controlled by a secure log-on procedure. Wherever possible, a second factor is enforced.

These regulations apply uniformly to the following account types: Employees, customers, and services.

Passwords at AEB must meet the following criteria:

- At least 11 characters overall

Additionally, three of the following four conditions must be fulfilled:

- At least one upper-case letter
- At least one lower-case letter
- At least one numeral
- At least one special character (non-alphanumeric character)

Rotation:

- AEB adheres to the results of current security research for internal accounts and does not provide for password rotation for employees.
- The AEB platform does not provide for password rotation.
- In all other applications, customers decide for themselves whether to use password rotation, and while both variants are possible, AEB recommends not using password rotation.

Different rules apply for privileged accounts (SSH Keys passphrase is included):

- Passwords must have at least 14 (fourteen) characters

Passwords must meet at least three of the following four criteria:

- At least one upper-case letter
- At least one lower-case letter
- At least one numeral
- At least one special character (non-alphanumeric character)

It is especially important to note that the last 24 passwords may not be reused.

This also applies to cloud operation.

4.4.6 A.8.6 – Capacity management

>> The use of resources should be monitored and adjusted in line with current and expected capacity requirements.

All resources (IT infrastructure and networks) are proactively monitored 24/7. Special tools and graphics are used to view and analyze predictions for system capacities and capacity trends.

New systems, system extensions, and line upgrades are planned in projects and a controlled change management process, which in turn triggers the appropriate measures to expand capacity.

Planning always includes a forward-looking buffer reflecting the momentum of recent years and adjusted to the forecasts for future development.

4.4.7 A.8.7 – Protection against malware

>> Protection against malware should be implemented and supported by appropriate user awareness.

AEB relies on a multi-level anti-malware concept:

In addition to standard operating system security policies and cloud provider protections, all internal AEB clients have the latest next-generation anti-malware software installed, which monitors the behavior of processes, prevents potentially harmful activities, and reports them for further investigation. Current anti-malware software is also active on the servers operated by AEB. Networks are also segmented, with next-generation firewalls between segments, providing additional security with various threat prevention features.

This is supported by an internal policy for employees and administrators on dealing with malware.

4.4.8 A.8.8 – Management of technical vulnerabilities

>> Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.

A vulnerability management process has been established to provide information about technical vulnerabilities and their management. This ensures that this information is obtained in a timely fashion, the organization's exposure to such vulnerabilities is evaluated, and appropriate measures are taken to address the associated risk.

Measures include:

- Continuous vulnerability monitoring is implemented for all devices and applications running on them.
- Regular application security checks are also carried out in the form of vulnerability scans (at least once a month) and penetration tests (at least three times a year).
- Vulnerabilities are classified by their criticality using the Common Vulnerability Scoring System (CVSS), among others.
- Critical vulnerabilities are remedied immediately, those classified as "high" within 4 weeks, where "remedy" means a complete removal of the vulnerability or a mitigation down one level.
- All other vulnerabilities are addressed during planned maintenance work.
- Customers are notified immediately of vulnerabilities classified as "high" and "critical" if they cannot be remedied in the specified time.

4.4.9 A.8.9 – Configuration management

>> Configurations, including security configurations, of hardware, software, services, and networks should be established, documented, implemented, monitored, and reviewed.

AEB has guidelines and instructions for the secure configuration of all relevant systems and hardware. They are reviewed and, if necessary, adjusted both regularly and whenever new information comes to light or major changes occur.

Proper configuration and compliance with the guidelines is monitored automatically.

4.4.10 A.8.10 – Information deletion

>> Information stored in information systems, devices, or any other storage media should be deleted when no longer required.

Data/information is permanently deleted in accordance with the security standard (ISO/IEC 27002) and legal requirements as soon as it is no longer needed.

4.4.11 A.8.11 – Data masking

>> Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

AEB has implemented an information classification scheme based on the legal, regulatory, and contractual requirements and the risk assessment. This ensures that data and information is handled in accordance with its need for protection.

Internal audits regularly check compliance with the relevant regulations and the correct handling of data and information.

4.4.12 A.8.12 – Data leakage prevention

>> Data leakage prevention measures should be applied to systems, networks, and any other devices that process, store, or transmit sensitive information.

Measures implemented to prevent data leaks include the following:

- Classification of information (see also control A.5.12)
- Electronic access control (see also control A.5.18)
- Regulations and technical measures to manage information transfer (see also control A.5.14)

- Manual and automatic blocking of accounts, user activities, or transfers in general in the event of unusual behavior
- Encryption of data at rest

4.4.13 A.8.13 – Information backup

>> Backup copies of information, software, and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

Information, software, and system images are backed up every 24 hours at the latest using a multi-stage concept. In addition to a local backup on disk, encrypted data carriers are available at a secure remote location.

The backups are tested regularly, randomly at least once a month. A full restore test/DR test is carried out at least once a year.

Details about the backup concept can be found in the document “Excerpt from the AEB security concept: details about backups,” available in the AEB Trust Center.

For cloud operation, the following also applies: More details can be found in the Service Description (AEB Cloud or AEB Private Cloud) and in further documents in the AEB Trust Center.

4.4.14 A.8.14 – Redundancy of information processing facilities

>> Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Information processing facilities are always implemented to comply with availability requirements. Availability is an essential safety criterion.

- AEB provides (multiple) redundancy for all relevant systems.
- AEB has established processes that ensure regular checks as well as availability in special situations.

4.4.15 A.8.15 – Logging

>> Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected, and analyzed.

Monitoring, alerting, logging, and the setup and operation of the logging of system administrator and system user activities follow controlled processes and are defined in the application management. The corresponding policies are also defined by AEB in the internal Admin Guide and in the Logging and Monitoring Concept.

The access rights to the log information are restricted and protected against unauthorized access and manipulation.

Log information is used only for authorized purposes and by authorized employees. The data is regularly deleted after the expiry of reasonable and documented periods.

Corresponding log information is available for 30 days.

For cloud operation, the following also applies: AEB offers its customers administrative options to read out their relevant log data themselves. The regularity and depth of testing are the responsibility of the customer.

4.4.16 A.8.16 – Monitoring activities

>> Networks, systems, and applications should be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.

Suspicious events are processed automatically and reported to the responsible employees in order to maintain network and operational integrity in a way that ensures business continuity. (See control A.5.25 for handling instructions.) This also helps improve other processes: auditing, security and risk assessment, vulnerability management, network performance, capacity management, and more.

This happens through central logging and monitoring, supported by intrusion prevention and detection systems and other dedicated threat intelligence systems.

Monitoring is carried out in accordance with all regulatory requirements and applicable legislation, and all records are stored in accordance with the AEB retention guidelines (see the internal Admin Guide for more information).

4.4.17 A.8.17 – Clock synchronization

>> The clocks of information processing systems used by the organization should be synchronized to approved time sources.

The clocks off all relevant information processing systems are synchronized via NTP to a single reference time source.

4.4.18 A.8.18 – Use of privileged utility programs

>> The use of utility programs with the capability of overriding system and application controls should be restricted and tightly controlled.

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

Means of technical support include:

- Review and analysis of installed or used software.
- Next-generation firewalls with IDS/IPS that can also monitor access across internal network zones and intervene as appropriate
- (Next-generation) malware protection mechanisms that can block such tools from running locally

An organizational application management process is also in place that determines which tools are approved by AEB. Security and data protection are integral parts of this process.

4.4.19 A.8.19 – Installation of software on operational systems

>> Procedures and measures should be implemented to securely manage software installation on operational systems.

Structured application management is in place for all business-relevant software, hardware, and cloud solutions in use.

The corresponding processes and policies have been implemented and communicated and are regularly taught and reviewed.

It is referenced in the internal Security Guide and in the Admin Guide. Here there are also notes on the use of permitted software along with notes on prohibited software and guidelines for the secure installation and configuration of applications.

These responsibilities are also taught to new employees during their information and data security onboarding and to existing employees as part of regular refresher courses.

4.4.20 A.8.20 – Network security

>> Networks and network devices should be secured, managed, and controlled to protect information in systems and applications

AEB has established a multi-level DMZ concept for networks as well as consistent, small-scale “zoning.” Transitions between zones are also secured by appropriate next-generation firewalls with IDS and IPS. AEB’s networks are administered exclusively by AEB employees.

4.4.21 A.8.21 – Security of network services

>> Security mechanisms, service levels, and service requirements of network services should be identified, implemented, and monitored.

All internal AEB networks are administered exclusively by AEB employees. Appropriate security mechanisms and conditions have been defined, are monitored automatically, and are regularly reviewed and adjusted if necessary.

Where external networks are necessary for the provision of services (internet and carrier networks, etc.), the agreements with the external parties incorporate corresponding terms and conditions. Like the entire partnership, these are monitored and regularly audited.

4.4.22 A.8.22 – Segregation of networks

>> Groups of information services, users, and information systems should be segregated in the organization's networks.

AEB has established a multi-level DMZ concept for networks as well as consistent, small-scale "zoning." Transitions between zones are also secured by appropriate next-generation firewalls with IDS and IPS.

4.4.23 A.8.23 – Web filtering

>> Access to external websites should be managed to reduce exposure to malicious content.

AEB applies guidelines and above all technical measures to ensure that access to external websites is restricted to prevent security threats and risks to AEB data.

These guidelines are regularly reviewed.

4.4.24 A.8.24 – Use of cryptography

>> Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.

Guidelines for the use of cryptographic measures to protect information – and for the use, protection, and lifespan of cryptographic keys – have been established. They are documented in the internal Security Guide and are regularly taught and referenced.

AEB informs its customers about the encryption methods used and possible options.

4.4.25 A.8.25 – Secure development lifecycle

>> Rules for the secure development of software and systems should be established and applied.

Security interests in the development and maintenance of software and systems are defined and regulated through quality management in the form of processes and how-tos and in the Security Guide. They have been implemented in development guides and criteria for secure coding. Topic owners have been assigned responsibility for certain software development processes.

4.4.26 A.8.26 – Application security requirements

>> Information security requirements should be identified, specified, and approved when developing or acquiring applications.

Security considerations are taken into account in the development and maintenance of software and systems as part of quality management. This is regulated by processes, guidelines, and instructions as defined in the internal Security Guide, the Product Development Guide, and elsewhere. One of the key points is the application of secure coding practices. Developers must use secure libraries and frameworks and follow guidelines that aim to avoid common vulnerabilities to ensure the integrity and security of applications.

An application management process is in place for the procurement of applications, in which the review of security and data protection requirements and the release are integral parts of the process.

Examples of the tests/securities, in addition to a general assessment of the need for protection, include the following:

- Authentication and electronic access control: The applications must have mechanisms for authenticating and authorizing users and for controlling access to sensitive data and functions.
- Data encryption: Applications must encrypt sensitive data both during transmission and at rest to protect it from unauthorized access or disclosure.
- Validation of input data: Applications must validate all incoming input from external sources to ensure that it is safe and free of malicious code.

4.4.27 A.8.27 – Secure system architecture and engineering principles

>> Principles for engineering secure systems should be established, documented, maintained, and applied to any information system development activities.

Secure system architecture and technology in development is integrated into appropriate processes. This is part of the requirements and associated instructions and is ensured across the board by the specifications of the Security Guide and the provision of the framework.

4.4.28 A.8.28 – Secure coding

>> Secure coding principles should be applied to software development.

We define criteria for the development of secure software that are based on established sets of criteria. These criteria are defined in more detail by development documentation and QM measures for the various tech stacks.

4.4.29 A.8.29 – Security testing in development and acceptance

>> Security testing processes should be defined and implemented in the development lifecycle.

The development of new products and continued development of existing products is planned and implemented within the quality and change management processes. Before new or modified information systems are released, they are subjected to manual or automated testing against the defined requirements and against the requirements for data protection and security. Test managers are responsible for the testing process and serve as contacts for test management. Continuous automated testing also protects against unintended side effects of the development.

4.4.30 A.8.30 – Outsourced development

>> The organization should direct, monitor, and review the activities related to outsourced system development.

The partner management processes regulate and define how activities associated with outsourced system developments are integrated and monitored or run. The partner manager of each development partner is primarily responsible for this.

4.4.31 A.8.31 – Separation of development, test, and production environments

>> Development, testing and production environments should be separated and secured.

Dedicated managers ensure the provision, operation, and maintenance of a secure development environment. Regular checks are run as part of the application management process to ensure that the development environment and the entire application environment are secure and up to date.

Development/QA/consolidation/test systems are strictly separated from production systems. This is ensured by specific processes and policies.

Where AEB is not responsible for development (third-party systems), it's possible that there are no development systems. Nevertheless, a strict separation is maintained here as well between QA/consolidation/test systems and production systems.

In special cases, a single environment may include two other systems separated from each other (separate production systems for first customer operations and normal operations, for example, or separate test systems for smoke tests and implementation tests).

For cloud operation, the following also applies: AEB also takes into account the data protection measures including risk assessment for situations in which test data should be used.

4.4.32 A.8.32 – Change management

>> Changes to information processing facilities and information systems should be subject to change management procedures.

All changes to technical systems are subject to change processes, which control the change. They are documented in internal guides (such as the Change Management Process, Admin Guide, and Security Guide).

This applies specifically to changes in the operating platform, ensuring that changes here do not negatively impact business-critical applications.

When changes are made to customized systems, processes are defined individually with the customers.

All changes to software artifacts are subject to release management. In addition to release planning, QA, and security, communication with the customer is also coordinated and software changes with noticeable effects for customers are evaluated.

4.4.33 A.8.33 – Test information

>> Test information should be appropriately selected, protected, and managed.

The selection, protection, and control of test data is integrated within quality management processes and how-tos. Tests take place in a protected environment to ensure that no security breaches occur and that no production data is inadvertently modified. Test data is not transferred to productive systems.

Customer-owned hardware devices are stored in secure rooms and administered only there with access controls for authorized employees only.

Data on customer hardware is deleted immediately after receipt and test data before go-live.

4.4.34 A.8.34 – Protection of information systems during audit testing

>> Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.

Management systems (such as those for information security and data protection) are managed by the owner. The owner's responsibilities also include organizing audits and other security checks, both internal and external, while maintaining the operability and protecting confidentiality.

All upcoming audits are clearly organized with an audit plan.

No audits/reviews of information systems take place without a person responsible for the respective information system present. The person responsible ensures that no changes are made to the systems as a result of the audit and that smooth operation is guaranteed despite the audit.

5 Information Security Controls from ISO 27018 / Annex A

ISO 27018 introduces requirements for controls in two places:

- From chapters preceding Annex A: In some cases, these directly expand on the controls of ISO 27001. They are defined directly in the chapter "Information Security Controls from ISO 27001 / Annex A / SoA" with the addition "For cloud operation, the following also applies: …."
- From Annex A of ISO 27018: We have defined these below as separate controls associated with the data protection principles.

Their nomenclature is based on the following levels:

- Regulatory scope (A.1 through A.11)
- Control (e.g.: A.05.1)

This document provides information from AEB on the requirements for all controls.
Each control is assigned to a control owner. Controls are maintained through a managed process, including a regular review that considers the current state of the art and other factors.

The following applies to all controls:

- There are no exclusions
- All requirements have been implemented and are active

5.1 A.1 – Consent and choice

5.1.1 A.01.1 – Obligation to cooperate regarding PII principals' rights

>> The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfill their obligation to facilitate the exercise of PII principals' rights to access, correct, and/or erase PII pertaining to them.

AEB supports its customers as data controllers when the rights of data subjects are exercised (per Chapter 3 GDPR). The terms of this support are part of AEB's standard Agreement on Processing per Art. 28 GDPR.

This agreement stipulates how direct requests from data subjects to AEB as the processor are handled.

AEB also supports customers with information in our Trust Center (https://www.aeb.com/en/trust-center/data-protection.php), including on how to fulfill their information obligations as controllers.

AEB trains its employees to provide support for processes involving data subject rights.

5.2 A.2 – Purpose legitimacy and specification

5.2.1 A.02.1 – Public cloud PII processor's purpose

>> PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.

Predetermined purpose is an essential principle in data protection.

AEB's standard Agreement on Processing per Art. 28 GDPR sets forth the purposes, the predetermination of purpose, and the obligation to follow instructions. This extends as well to the service agreement(s) on which the processing is based.

Information in the AEB Trust Center (e.g. recording of processing activities) also serves to ensure transparency.

AEB ensures that any subcontractors are bound to the same predetermined purpose and obligation to follow instructions. AEB's standard Agreement on Processing includes a section dedicated to the possible use of subcontractors, including provisions on approval by the controller.

AEB naturally grants controllers the right to check for compliance with legal and contractual obligations.

5.2.2 A.02.2 – Public cloud PII processor's commercial use

>> PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.
NOTE: This control supplements the more general controls defined in A.3.1 and in no way replaces them.

AEB will not use the PII processed under a contract for marketing or advertising purposes without express consent. Training sessions are held accordingly.

5.3 A.3 – Collection limitation

No additional controls apply to this privacy principle.

5.4 A.4 – Data minimization

5.4.1 A.04.1 – Secure erasure of temporary files

>> Temporary files and documents should be erased or destroyed within a specified, documented period.

Processes for erasing temporary data are in place that track the regular deletion of files.

The maximum retention period for such files – unless otherwise agreed at the service/process/customer level – is set at three months.

5.5 A.5 – Use, retention, and disclosure limitation

5.5.1 A.05.1 – PII disclosure notification

>> The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.

The AEB standard Agreement on Processing per Art. 28 GDPR stipulates:
"The Supplier may process the Data of data subjects only within the scope of the order and the Client's instructions unless an exception as set forth in Art. 28(3) a) GDPR is present.

(…)

The Supplier shall notify the Client without delay of any controls and measures undertaken by the regulatory authority if they relate to this order. This applies even if a responsible authority in administrative or criminal proceedings relating to the processing of personal data investigates the Supplier's processing activities."

5.5.2 A.05.2 – Recording of PII disclosures

>> Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom, and at what time.

AEB has established a process for handling official searches that provides for logging.

AEB has established a process for handling unauthorized disclosures of PII (data breaches). AEB complies with its obligation to support the controller with its notifications (per Art. 33 and 34 GDPR). This is part of AEB's standard Agreement on Processing per Art. 28 GDPR.

5.6 A.6 – Accuracy and quality

No additional controls apply to this privacy principle.

5.7 A.7 – Openness, transparency, and notice

5.7.1 A.07.1 – Disclosure of subcontracted PII processing

>> The use of subcontractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use.

AEB's standard Agreement on Processing per Art. 28 GDPR includes a section governing the use of subcontractors. This includes providing appropriate information to the controller at an early stage.

In the interests of transparency, AEB provides a current overview of its subcontractors in the Trust Center at https://www.aeb.com/en/trust-center/data-protection.php.

5.8 A.8 – Individual participation and access

No additional controls apply to this privacy principle.

5.9 A.9 – Accountability

5.9.1 A.09.1 – Notification of a data breach involving PII

>> The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure, or alteration of PII.

The processor supports the customer to the extent possible in complying with the obligations set forth in Art. 32–36 GDPR. This is part of AEB's standard Agreement on Processing per Art. 28 GDPR.

AEB has prepared the framework for reporting a data breach to the customer based on the requirements of Art. 33 GDPR.

AEB uses the appropriate contacts provided by the customer in issuing such notifications.

AEB has established a process that, in addition to notification, appropriately documents, logs, and retains to the extent necessary the subsequent steps of the investigation and follow-up.

5.9.2 A.09.2 – Retention period for administrative security policies and guidelines

>> Copies of security policies and operating procedures should be retained for a specified, documented period on replacement (including updating).

AEB archives its security policies for at least five years.

5.9.3 A.09.3 – PII return, transfer, and disposal

>> The public cloud PII processor should have a policy in respect of the return, transfer, and/or disposal of PII and should make this policy available to the cloud service customer.

The subject of the disposal and return of PII is addressed in AEB's standard Agreement on Processing per Art. 28 GDPR.

AEB supports customers in their disposal obligations, including with instructions (Deletion Concept) available in the AEB Trust Center: https://www.aeb.com/en/trust-center/data-protection.php.

AEB also advises on how to handle disposal requests from data subjects.

AEB also supports customers with requests for the return of PII.

5.10 A.10 – Information security

5.10.1 A.10.1 – Confidentiality or non-disclosure agreements

>> Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.

At the start of any contractual relationship, employees and partners sign standardized contracts with an appropriate confidentiality clause that includes data processing.
These contracts stipulate a predetermined purpose with an obligation to follow instructions within the scope of the processing.
The obligation of confidentiality extends beyond the contract term.
The above issues are also the subject of AEB's professional development program.

5.10.2 A.10.2 – Restriction of the creation of hardcopy materials

>> The creation of hardcopy material displaying PII should be restricted.

AEB follows a paperless operating model.
No processes involving customer data include steps for printing hardcopies.
Exceptions may occur in certain circumstances (for testing purposes, for example) if requested by the customer.

Regular inspections of the building check for appropriate behavior, including clean desk.

5.10.3 A.10.3 – Control and logging of data restoration

>> There should be a procedure for, and a log of, data restoration efforts.

- On the subject of data backup, see: A.8.13 – Information backup
- A.5.29 – Information security during disruption
- A.8.15 – Logging
- Documented process description in data restoration processes

5.10.4 A.10.4 – Protecting data on storage media leaving the premises

>> PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g., by encrypting the data concerned).

See A.5.14 – Information transfer

This applies to the transfer of data storage media as well.

Physical access to AEB's data center is granted to selected, authorized roles from IT and Facility.

Security controls (such as encryption) are part of the AEB Security Guide.

When in doubt, AEB acts as if the data storage media included PII, and the controls are based on this.

5.10.5 A.10.5 – Use of unencrypted portable storage media and devices

>> Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use off such portable media and devices should be documented.

Regulations from A.8.24 – "Use of cryptography" and A.7.10 – "Storage media"

Employees follow internal guidelines on "data outside the company" in the Security Guide.

If a storage medium is received unencrypted, the sender is notified of this, and either the encryption is performed subsequently or the situation and its background are documented.

5.10.6 A.10.6 – Encryption of PII sent over public data-transmission networks

>> PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.

See A.5.14 – "Information transfer" with statements on "data on the move."

5.10.7 A.10.7 – Secure disposal of hardcopy materials

>> Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.

Refer to A.7.10 – Storage media

The AEB standard refers to the reference DIN 66399. The selection of the protection class or security level takes into account the possibility that the media contain PII.

5.10.8 A.10.8 – Unique use of user IDs

>> If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication, and authorization purposes.

- A.5.16 – Identity management
- A.8.2 – Privileged access rights
- Every employee has (at least) one unique user ID.
  This also helps us comply with the input control.

5.10.9 A.10.9 – Records of authorized users

>> An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.

Please refer to the section on electronic access control and specifically to the detailed information “Excerpt from the AEB Security Concept: details on physical and electronic access,” available in the AEB Trust Center under Security at AEB.

The AEB rights concept includes the following stages:

- One employee has 1-n roles.
- One role has authorization(s), including access rights.

5.10.10 A.10.10 – User ID management

>> De-activated or expired user IDs should not be granted to other individuals.

All users are assigned a unique, non-reusable ID at the database level.

5.10.11 A.10.11 – Contract measures

>> Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.

See also section Order control

For AEB, the legally binding basis is the GDPR. Processing is carried out on the basis of the provisions of Art. 28 GDPR. AEB has corresponding agreements in place with its customers.

The technical and organizational measures of AEB as the processor are applicable to this agreement. The list contains controls for Art. 32 GDPR, ISO 27001, and ISO 27018.

The agreement contains a provision not to reduce the level of security it establishes.

In the interests of transparency, the latest information is always made available on the AEB website (AEB Trust Center).

AEB's General Terms and Conditions refer to the requirement to have a processing agreement in place. This includes a reference to access to the necessary documents.

5.10.12 A.10.12 – Subcontracted PII processing

>> Contracts between the public cloud PII processor and any subcontractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the subcontractor.

AEB addresses the subject of subcontractors in its Data Processing Agreement. Current subcontractors are named and listed in our Trust Center.

Agreements with subcontractors include the verification of appropriate security measures. The level of security promised to cloud customers must not be undercut when subcontractors are added.

Controls include inquiries about changes to security measures.

5.10.13 A.10.13 – Access to data on pre-used data storage space

>> The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.

See the Separation control.

AEB's applications ensure the separation of clients.

5.11 A.11 – Privacy compliance

5.11.1 A.11.1 – Geographical location of PII

>> The public cloud PII processor should specify and document the countries in which PII can possibly be stored.

- See https://www.aeb.com/en/trust-center/data-centers.php.
- The places of processing are documented in the procedures of the AEB procedure directory
- Customers can get support with their procedure directory at https://www.aeb.com/en/trust-center/data-protection.php#Other-materials
- Customers can find information on any data transfers by means of the data processing agreement documentation and an overview of subcontractors; also available at Data protection: data processing agreements (aeb.com).

5.11.2 A.11.2 – Intended destination of PII

>> PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.

The end-to-end encryption in place ensures that data can be encrypted and processed only in the AEB data center – as intended.