Security Concept

Data Security at AEB SE

Technical and Organizational
Measures and Controls

April 30, 2019

AEB

www.aeb.com

Contents

1 About this document

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

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.

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. 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).

1.3 SOX compliance

The requirements for service providers, especially those outlined in Section 404 of the Sarbanes-Oxley Act (SOX), oblige companies that are subject to SOX to include outsourced compliance-relevant tasks in their internal controls.

These controls can be simplified by requesting a report on the outsourced services. In this report, the service provider describes its own internal control system (data privacy, data security, access controls, data integrity, etc.). This control system must be sophisticated enough to achieve the stated objectives. And it must be fully implemented. The relevance can be certified by an external auditor.

For further information, refer to:

- **SSAE16** (Statement on Standards for Attestation Engagements No. 16) with reference to **ISAE 3402** (International Standard on Assurance Engagements No. 3402)
- Additionally, for Germany: **PS 951** auditing standard of the IDW (Institute of Public Auditors in Germany), which references ISAE 3402.
- Earlier basis: SAS 70 (report type 2)

2 General controls

2.1 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 General organizational control (management systems)

2.2.1 Data protection

The company's data protection officer checks and monitors compliance with the applicable legal requirements. The data protection officer keeps a data protection concept 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").

A limited circle from the IT teams grants access rights with mandatory oversight by a second person. The rights are subject to regular event- and time-controlled checks, especially as regards data center operations. The limited circle from the IT teams referred to above can raise an objection and exercise a veto.

2.2.2 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 security criteria 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) at https://service.aeb.de/en/open/guidelines-and-certificates/.

2.3 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 security criteria of availability, confidentiality, integrity (and resilience). References in the sections below make it easier to choose the right classifications, at least for a certain transition period.

2.3.1 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

- Comprehensive logging by all systems that process personal master data, making it possible to subsequently determine whether and by whom personal master data was entered, modified, or removed
- Personalized user accounts extending to the specialized applications
- Separate system logs and application logs, ruling out manipulation of the application logs at the system level
- GDPR classification: integrity

2.3.2 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 client, who decides which data is transferred and when
- Access to this data limited to roles with corresponding access rights
- Automated processing of data by certified software (ATLAS procedure, compliance, etc.), ensuring that data is processed in accordance with contracted procedure
- Use of standardized contracts as stipulated by law for relations with customers and service providers
- Inclusion of subcontractors with corresponding confidentiality, data processing, system access agreements
- GDPR classification: availability, confidentiality

2.3.3 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 the 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 classification: confidentiality, availability

2.3.4 Physical access control

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

- 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 classification: confidentiality, availability

2.3.5 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 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 classification: confidentiality, availability, integrity

2.3.6 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 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
- GDPR classification: confidentiality, availability, integrity

2.3.7 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)
- GDPR classification: confidentiality, availability, integrity

2.3.8 Availability control

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

- Data encrypted for storage (in databases, etc.)
- 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 classification: availability, resilience

2.3.9 Measures for 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 private) nature and business interests, including ability to ensure tamper-proof data management, outweigh personal interests

2.3.10 Measures to ensure 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
- Availability of an emergency management process, including regular exercises
- Availability of backup systems

2.3.11 Measures to ensure 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
- 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

2.3.12 Measures for regular effectiveness checks

» To ensure security during processing

- 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

2.3.13 Measures to address (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
- 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

2.3.14 Measures to prevent 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

2.3.15 Measures for 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 privacy statement on AEB website
- 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

2.3.16 Measures to ensure possibility of intervention

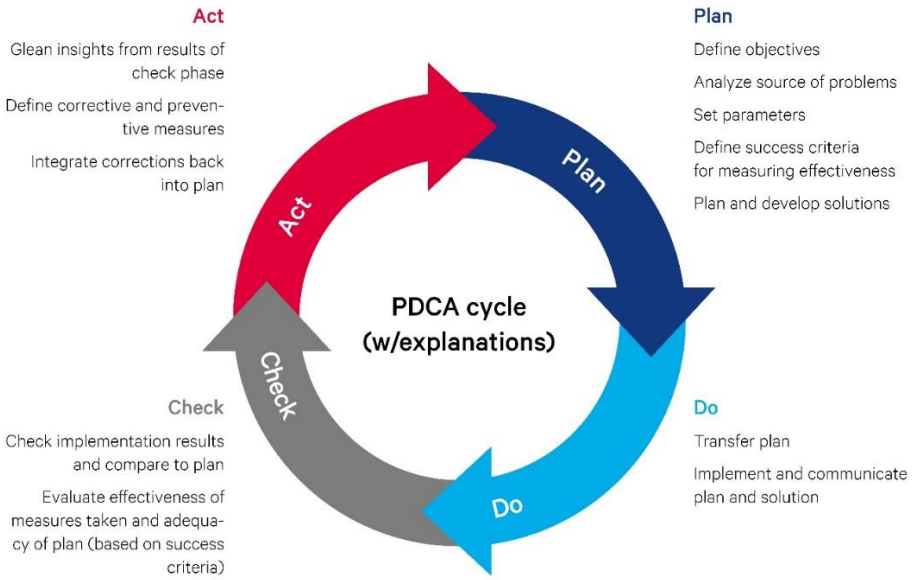
» To ensure that data subjects can exercise their rights to intervene

- 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

3 Application controls

3.1 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.

3.2 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.

3.3 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 SE . Headquarters . Sigmaringer Strasse 109 . 70567 Stuttgart . Germany . +49 711 72842 0 . www.aeb.com . info@aeb.com . Registry court: District Court of Stuttgart . HRB 767 414 . Managing Directors: Matthias Kiess, Markus Meissner . Chairman of the board of directors: Maria Meissner

Locations

Düsseldorf . Hamburg . Lübeck . Mainz . Malmö . Munich . New York . Paris . Prague . Rotterdam . Salzburg . Singapore . Soest . Stuttgart . Warwick . Zürich