Guideline

Data protection

Version 3.0

January 2022

www.aeb.com

AEB Data Protection Guideline

The following **Data Protection Guideline** provides an overview of key information on how personally identifiable information (PII) is handled at AEB.

Core themes of this guideline:

- Proper application of relevant data protection laws – especially the EU's General Data Protection Regulation (GDPR) and national legislation such as Germany's Federal Data Protection Act.
- Commitment to data protection principles (such as those defined in ISO 29100)
- Fulfillment of our responsibilities as a data processor to data controllers

The guideline's key points and **principles** are as follows:

Data protection is a top priority: The AEB Board of Directors is the controller as defined by Art. 4 GDPR and responsible for the content of this guideline. In this capacity, the AEB Board of Directors is committed to the principles set forth in Art. 5 GDPR and to the **data protection principles** defined in ISO 29100 and elsewhere:

Data protection principle	Core message of AEB, instructions for implementation
Consent and choice	It is important to AEB that users of the AEB applications (as data subjects) are asked to provide only the PII actually required in the specific context. That's why we see this principle as linked to the imperatives of data minimization, predetermination of purpose, and transparency.
Legitimacy and orientation of purpose	AEB provides data in its applications to the extent technically required. The use of PII is therefore typically based on overriding legitimate interests or legal obligations of the controller. Here we are also driven by the desire to make applications lean, user-friendly, and easy to master. Product design always takes technical necessity into account. AEB maintains a list of processing activities in accordance with Art. 30 GDPR that is used to identify PII and to examine, regularly check, and document the processing of PII in keeping with the relevant regulation. Key steps here include the legitimacy check based on applicable laws and the integrated two-stage risk assessment.
Limitation of collection, data minimization	The record of PII is limited to what is really necessary. The approach is to collect as little PII as possible. AEB's applications do not call for any private or sensitive user data. Our product development processes incorporate checks for the aforementioned imperatives, and AEB employees are trained accordingly.
Use, retention, disclosure limitation	AEB provides for the deletion of PII when the purpose of processing the PII ends and there are no legal or contractual requirements for their retention. The requirements for retention stem from the types of data in the applications in connection with the controller's business interests. The deletion routines are based on the specifications of the AEB Deletion Concept.

Data protection principle	Core message of AEB, instructions for implementation
Accuracy and quality	AEB provides the data subjects themselves with the possibility of entering, checking, and, if necessary, correcting their data. The nature and scope of the data (contact details in the exchange of messages) provide a good check of the accuracy of the information.
Openness, transparency, and notice	AEB addresses its information obligations as a controller in its detailed Data Protection Statement, which is also applied to cases where PII may be collected. AEB provides information on data processing in various places (system descriptions, Agreement on Processing, and in the AEB Trust Center).
Individual participation and access	AEB provides the data subjects themselves with the possibility of entering, checking, and, if necessary, correcting their data. The limited nature and scope of the data (contact details) provide a good check of the accuracy of the information.
Accountability	AEB provides information externally and internally on how it uses a data protection management system to comply with its data protection obligations. Internally, the AEB intranet offers direct access to information on the data protection management system. Externally, AEB offers information through its Data Protection Statement and the information on data protection in the Trust Center.

Information security	AEB operates an information security management system (ISMS) based on ISO 27001. Confidentiality, availability, and integrity are considered essential security criteria. Particular importance is attached to the integrated regular controls and risk assessment.
	Risk assessment in the environment of the data protection management system also depends on the following ISMS criteria:
	• Context for understanding the organization, including the technical environment and criteria such as
	  • Legal and regulatory factors (international environment, court decisions, etc.)
	  • Contractual factors
	  • Business factors (specific characteristics or context of use of a proposed application, relevant standards, etc.)
	• Risk assessment methodology
	• Risk treatment methodology
	Monitor and review by tracking risks and control measures and improving the process.

Privacy compliance	AEB operates an ISMS based on ISO 27001 and ISO 27018. Particular importance is attached to the integrated regular controls and risk assessment in close consultation among the company management, security roles, and Data Protection Officer.

The primary data protection objectives are:

- Protecting data subjects – including the in-depth study of privacy by design and privacy by default and the principles of data minimization, with initial considerations always devoted to the questions of necessity and lawfulness of data processing and a regular and process-oriented risk assessment taking the perspective of the data subject.
- Protecting the data in line with the security objectives of confidentiality, integrity, availability, and resilience to achieve a good and appropriate level of data protection – both for customers and internally for AEB employees.
- Ensuring transparency and awareness of the information obligations both internally and externally.
- Documenting processing activities with integrated risk assessment and monitoring such factors as legal foundations and compliance with the predetermined purpose.
- Training and developing AEB employees on data protection and security awareness.
- Supporting AEB customers wherever AEB acts as the processor (as defined by Art. 28 GDPR).
- Cooperating with the relevant supervisory authorities.
- Keeping adequate resources available.

Other key points:

- The Data Protection Officer (contact: mailto:dataprotectionofficer@aeb.com) is integral to this Data Protection Guideline. The Data Protection Officer is an AEB employee duly appointed for support, consultation, and monitoring purposes.
- AEB complies with its obligations as a processor
    - in accordance with its legal obligations (from Art. 28 GDPR et al.)
    - in accordance with its contractual obligations to customers (to assist with data protection impact assessment, etc.) as a data controller
    - under its standardized Agreement on Processing per Art. 28 GDPR, customized to the primary hosting and support services it provides as the processor
- AEB maintains an up-to-date summary of the state-of-the-art technical and organizational data protection measures that it undertakes (pursuant to Art. 32 GDPR) as an integral part of its processing contracts under Art. 28 GDPR. AEB's security concept also provides information on security measures based on the controls of ISO 27001 (Statement of Applicability) and ISO 27018.
- AEB performs regular self-monitoring and audits to check the compliance and effectiveness of these measures, including documentation and assessment of findings to remedy any shortcomings.
- All AEB employees sign a confidentiality agreement when they are hired and are notified of the binding legal nature of this agreement.
- AEB's Data Protection Officer conducts regular training and refresher seminars to educate the workforce in matters pertaining to data protection. This includes notifying them of their rights and responsibilities and providing easily accessible information for further study.
- AEB complies with its information obligations to both internal and external parties.

- AEB uses a process-driven **data protection management system** to implement data protection. This ensures regular dialog within the data protection organization and the application of **accountability, monitoring, risk assessment, and continuous improvement** in practice.
- **Data protection is part of AEB's security culture.** The underlying rules are binding and can be found in our internal **Security Guide**. This culture is practiced through security campaigns and supported and monitored through the use of a ISO 27001–certified ISMS. This certificate can be viewed at https://www.aeb.com/en/trust-center/certificates.php.

AEB takes transparency very seriously. For more information, **please visit our website**:

- Our Data Protection Statement
- Our Trust Center with guidelines and certificates relating to data protection and information security
- Our data protection page in the Trust Center

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

Locations

Düsseldorf . Hamburg . Lübeck . Mainz . Malmö . Manila . Munich . New York . Prague . Amsterdam . Salzburg . Singapore . Soest . Stuttgart . Warwick . Zurich