

AEB



Data Protection Guideline

Version 2.1

July 2018

The following **Data Protection Guideline** provides an overview of key information relating to data protection at AEB.

The primary aim of this guideline is to ensure proper application of relevant data protection laws such as the EU's General Data Protection Regulation (GDPR) and applicable national laws, for AEB especially Germany's Federal Data Protection Act. The guideline's key points and principles are as follows:

- **Data protection is a top priority:** The AEB Executive Board is the controller as defined by Art. 4 GDPR and responsible for the content of this guideline. In this capacity, the AEB Executive Board is committed to the **principles set forth in Art. 5 GDPR**.
- 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 reduction and data economy
 - **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
 - **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
- 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 offers a standardized processing contract pursuant to 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 performs regular **self-monitoring and audits** to check compliance with 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 advanced 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.
- **Data protection is part of AEB's security culture.** The underlying rules are binding and can be found in the AEB internal **Security Guide**. This culture is practiced through security campaigns and supported and monitored through the use of a **ISO 27001**-certified information security management system. This certificate can be viewed at <https://service.aeb.de/en/open/guidelines-and-certificates/>.

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

- Our statement on data protection and security: <https://www.aeb.com/intl-en/data-protection.php>
- Our portal for guidelines and **certificates** relating to data privacy and information security: <https://service.aeb.de/en/open/guidelines-and-certificates/>
- Our data protection portal: <https://service.aeb.de/en/open/data-protection/>

Stuttgart, July 2018

AEB Executive Board