Data protection

Date: November 15, 2024
Version: 1.2.1

TOM

Technical and organizational measures

BEX /exceeding/boundless

Author: BEX Components AG
Application: ~~Internal~~ | ~~Partner~~ | Public
Status: ~~Draft~~ | Final

Contents

1 Introduction
Technical and organizational measures of the Supplier

1.1 Introduction

BEX Components AG, as a private body that collects, processes, or uses personal data itself or on behalf of Clients, must take the technical and organizational measures necessary to ensure compliance with the provisions of the GDPR and the Federal Data Protection Act. Measures are required only insofar as the resources involved are reasonable in relation to the intended purpose of the protection.

The necessary measures taken by BEX are described below. They relate to the special features of the Aalen location.

Our servers are hosted by our parent company AEB SE. You can view the technical and organizational measures in the AEB SE Trust Center: https://www.aeb.com/security-concept.

1.2 Measures taken

Appropriate measures depending on the type of personal data or categories of data to be protected.

1. **Physical access control**
   Blocks unauthorized parties from physical access to data processing systems that process or use personal data.

   Access to the business premises of BEX Components AG is only possible via an access control system. Third parties are only allowed to enter the premises with an authorized person. All visitors are documented in a visitor log. Employees are instructed on this.

   Third parties, such as external employees who work on BEX premises for a longer period of time, must agree to a data processing agreement and a data protection and confidentiality agreement.

   The issuing and return of keys and transponders is documented.

2. **User access control**
   Prevents unauthorized parties from using data processing systems.

   Requirement for employees to lock workstation computers (automatic locking).

   Roles and authorizations may only be set up and revoked upon the instruction of specially authorized persons. This is documented and reviewed at regular intervals.

   The systems have high complexity requirements for passwords. No regular password change is required. The system checks for suitability (minimum requirement: 15 characters, a-z, A-Z, 0-9, special characters) and prevents the same password from being reused.
   In addition, two-factor authentication is used in systems where possible to further increase protection.

   The hard disks of mobile systems are encrypted with at least XTS AES 128.

   To protect the systems of BEX Components AG from viruses and malware, standard protection programs are used on central and decentralized systems.

   While working remotely (e.g. from hotels, events, trade fairs), it is ensured that the employee can only access the systems using a personal access ID via VPN.

3. **Electronic access control**
   Ensures that those authorized to use a data processing system can only access the data for which they are authorized and that personal data is not subject to unauthorized viewing, copying, modification or deletion when it is processed or used or after it is stored.

   The basic principle of the electronic access control policy is that access to all systems, services, and information is restricted and technically blocked, unless it is explicitly allowed for individual users or user groups.

   Employees are obliged to maintain confidentiality when they are hired.

   If the system requires generic users to be used for special activities, their possible use is restricted to specific rights that do not have access to order-related data.

   Sensitive data on paper is destroyed using a file shredder with security level P-4 (cross-cut 4x40mm) or by a contracted service provider. Rewritable hard disks or SSDs are erased and mechanically destroyed by being completely overwritten several times before disposal or transfer.

4. **Separation control**
   Ensures that personal data collected for different purposes can be processed separately.

   In system environments in which development and testing take place, these activities are carried out on separate development and test systems with test data.

   The separation of customer data is technically implemented in the software within the BEX applications. Each customer has a unique technical identification number that is stored with each data record associated with the customer and is used to link the customer to their data (clientization).
   Customer users are also assigned this identification number so when they log in, they only have access to the data assigned to the customer via the ID – and access to the data of other customers is excluded.

5. **Pseudonymization**
   Ensures that the processing of personal data takes place in a manner that the data can no longer be linked to a specific data subject without additional information, as long as such additional information is stored separately and is subject to appropriate technical and organizational measures.

   We do not currently use pseudonymization.

6. **Transmission control**
   Ensures that personal data cannot be viewed, copied, modified or deleted without authorization while it is electronically transmitted, transported or saved on storage media and that it is possible to monitor and determine the intended destinations of personal data transferred using data transmission equipment.

   The transfer of personal data by electronic means is encrypted.

   When systems are transferred ("transition") from the BEX Components AG data center, the data carriers with the data are encrypted. The method of transmission of the password is agreed on a case-by-case basis.

   Personal data is deleted at regular intervals after a service or project has been completed. Data will only be stored for longer if there are retention obligations or to comply with another legal requirement.

7. **Input control**
   Ensures that it is possible to subsequently check and determine whether and by whom personal data was entered into data processing systems, modified, or deleted

The BEX products log entries. This logging ensures that changes can be traced and assigned to a user.

Changes made in the ERP system used by BEX are also recorded with a time stamp and user.

8. **Availability control**
   Ensures that personal data is protected against random destruction or loss

   Personal data is always stored on central server systems. All central server and management systems are operated in the data center of AEB and BEX Components AG (see https://www.aeb.com/security-concept).

9. **Order control**
   Ensures that personal data from orders can only be processed according to the Client's instructions.

   BEX uses subcontractors (see https://bex.ag/static_downloads/BEX_Sub_contractors-en.pdf). These were carefully checked in advance and are bound by confidentiality agreements. Subcontractors are audited at regular intervals.

1.3 Process for regular testing, assessment, and evaluation (Art. 32(1) d) GDPR, Art. 25(1) GDPR)

The effectiveness of the technical and organizational measures is regularly and continuously reviewed and improved by the data protection officer and the information security officer.

BEX Components AG is certified according to ISO 27001. The information security management system is audited annually by independent external auditors.

2 Appendices and references

Name of appendix/reference	Description
Annex 1	Specification of order or contract (details)
Annex 3	Annex 3 to the data processing agreement – Subcontractors

3 Change history

Date	Changed by	Description of change
April 30, 2018	KLV, RIA	Document created
August 18, 2020	KLS, KLV	Revision
April 23, 2021	KLV	Checked whether up to date
April 26, 2022	KLV	Technical and organizational measures revised
February 22, 2023	KLV	Technical and organizational measures revised
September 10, 2024	KLV	Technical and organizational measures revised
November 15, 2024	KLS	Content transferred to current document design. Link for subcontractors added.

Still have questions? No problem!

We are here for you:

Email:

datenschutz@bex.ag

Phone:

+49 7361 999 39 10

(Mon–Fri 8 am to 4 pm)

Or at any time under:

www.bex.ag

BEX Components AG

Gartenstrasse 97

73430 Aalen