Datenschutz

Stand: 15.11.2024
Version: 1.2.1

TOM

Technische und organisatorische Maßnahmen

BEX /einfach/grenzenlos

Verfasser:	BEX Components AG
Verwendung:	~~Intern~~ | ~~Partner~~ | Öffentlich
Status:	~~Entwurf~~ | Final

Inhaltsverzeichnis

1 Einleitung 3

Technische und organisatorische Maßnahmen des Auftragnehmers 3

1.1 Präambel 3

1.2 Getroffene Maßnahmen 3

1.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DSGVO, Art. 25 Abs. 1 DSGVO) 5

2 Anhänge und Verweise 6

3 Änderungshistorie 6

1 Einleitung
Technische und organisatorische Maßnahmen des Auftragnehmers

1.1 Präambel

Die BEX Components AG, als nicht-öffentliche Stelle, die selbst oder im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der DSGVO sowie des Bundesdatenschutzgesetzes, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Nachfolgend werden die von der BEX dazu getroffenen, erforderlichen Maßnahmen beschrieben. Diese beziehen sich auf die Besonderheiten des Standorts Aalen.

Unsere Server sind bei unserem Mutterkonzern AEB SE gehostet. Die Technischen und organisatorischen Maßnahmen können Sie im Trust Center der AEB SE einsehen: https://www.aeb.com/sicherheitskonzept.

1.2 Getroffene Maßnahmen

Die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

1. **Zutrittskontrolle**
   Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

   Der Zutritt in die Geschäftsräume der BEX Components AG ist nur über ein Zutrittskontrollsystem möglich. Dritte dürfen die Räume nur in Begleitung einer autorisierten Person betreten. Alle Besucher werden in einem Besucherprotokoll dokumentiert. Mitarbeiter werden hierzu unterwiesen.

   Dritte, wie z. B. auch externe Mitarbeiter, welche über einen längeren Zeitraum in den Räumen der BEX tätig sind, müssen einem Vertrag zur Auftragsverarbeitung und einer Vereinbarung für Datenschutz- und Vertraulichkeit zustimmen.

   Ausgabe und Rücknahme von Schlüsseln oder Transponder wird dokumentiert.

2. **Zugangskontrolle**
   Zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

   Verpflichtung der Mitarbeiter zur Sperrung des Arbeitsplatzrechners (Automatische Sperrung).

   Die Einrichtung und der Entzug von Rollen und Berechtigungen erfolgen nur auf Anweisung hierzu besonders autorisierter Personen. Dies wird dokumentiert und in regelmäßigen Abständen überprüft.

   Die Systeme besitzen hohe Komplexitätsvoraussetzungen für Passwörter. Dafür wird kein regelmäßiger Passwortwechsel verlangt. Dabei wird systemseitig auf die Eignung (Mindestanforderung: 15 Zeichen, a-z, A-Z, 0-9, Sonderzeichen) geachtet und verhindert, dass das gleiche Passwort wiederverwendet werden kann. Zusätzlich wird in Systemen, wo möglich, eine Zwei-Faktor Authentifizierung eingesetzt, um den Schutz weiter zu erhöhen.

   Die Festplatten von mobilen Systemen sind mindestens mit XTS AES 128 verschlüsselt.

   Um die Systeme der BEX Components AG vor Viren- und Malwarebefall zu schützen, werden auf zentralen und dezentralen Systemen marktübliche Schutzprogramme eingesetzt.

Während des mobilen Arbeitens (z. B. Hotels, Veranstaltungen, Messen) ist sichergestellt, dass der Mitarbeiter nur mittels persönlicher Zugangskennung via VPN auf die Systeme zugreifen kann.

3. **Zugriffskontrolle**
   Zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

   Das Grundprinzip der Zugriffskontrollleitlinie ist, dass der Zugang zu allen Systemen, Diensten und Informationen verboten und technisch unterbunden wird, solange er nicht einzelnen Benutzern oder Benutzergruppen ausdrücklich erlaubt wird.

   Beschäftigte werden bei Einstellung zu Vertraulichkeit verpflichtet.

   Sofern systembedingt generische Benutzer für spezielle Tätigkeiten genutzt werden müssen, ist deren mögliche Verwendung auf gezielte Rechte eingeschränkt, welche keinen Zugriff auf auftragsbezogene Daten erhalten.

   Sensible Daten auf Papier werden mit einem Aktenschredder der Sicherheitsstufe P-4 (Kreuzschnitt 4x40mm) oder durch einen beauftragten Dienstleister vernichtet. Wiederbeschreibbare Festplatten oder SSDs werden vor der Entsorgung oder dem Übergang durch ein mehrfaches, vollständiges Überschreiben gelöscht und mechanisch zerstört.

4. **Trennungskontrolle**
   Zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

   In Systemumgebungen, in denen Entwicklungen und Tests stattfinden, werden diese Tätigkeiten auf separaten Entwicklungs- und Testsystemen mit Testdaten durchgeführt.

   Die Trennung der Kundendaten ist innerhalb der BEX-Anwendungen softwaretechnisch implementiert. Jeder Kunde besitzt eine eindeutige technische Identifikationsnummer, die bei jedem dem Kunden zugehörigen Datensatz hinterlegt ist und über die die Verknüpfung des Kunden zu seinen Daten hergestellt wird (Mandantisierung).
   Jedem Benutzer des Kunden hat ebenfalls diese Identifikationsnummer zugeordnet, so dass er bei der Anmeldung nur Zugriff auf die dem Kunden über die ID zugeordneten Daten hat – und ein Zugriff auf die Daten anderer Kunden ausgeschlossen wird.

5. **Pseudonymisierung**
   Zu gewährleisten, dass die Verarbeitung personenbezogener Daten in einer Weise stattfindet, dass die Daten ohne Hinzuziehen zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technische und organisatorische Maßnahmen unterliegen.

   Aktuell setzen wir keine Pseudonymisierung ein.

6. **Weitergabekontrolle**
   Zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

   Die Weitergabe personenbezogener Daten auf elektronischem Wege erfolgt verschlüsselt.

   Bei Systemübernahmen („Transition") aus dem Rechenzentrum der BEX Components AG werden die Datenträger mit den Daten verschlüsselt. Der Übermittlungsweg des Passwortes wird im Einzelfall abgestimmt.

   Personenbezogene Daten werden nach vollständiger Abwicklung einer Dienstleistung oder eines Projektes in regelmäßigen Löschläufen entfernt. Eine längere Speicherung erfolgt nur, wenn Aufbewahrungspflichten bestehen oder aber eine andere Rechtsgrundlage zu finden ist.

7. **Eingabekontrolle**
   Zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

   Die Produkte der BEX protokollieren Eingaben. Diese Protokollierung stellt sicher, dass Änderungen nachvollzogen und einem Anwender zugeordnet werden können.

   Ebenso werden im von BEX genutzten ERP-System gemachte Änderungen mit Zeitstempel und Nutzer festgehalten.

8. **Verfügbarkeitskontrolle**
   Zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

   Personenbezogene Daten werden grundsätzlich auf zentralen Serversystemen gespeichert. Alle zentralen Server- und Managementsysteme werden im Rechenzentrum der AEB und BEX Components AG betrieben (siehe https://www.aeb.com/sicherheitskonzept).

9. **Auftragskontrolle**
   Zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können.

   Die BEX setzt Subunternehmer ein (siehe https://bex.ag/static_downloads/BEX_Subunternehmer.pdf). Diese wurden im Vorfeld sorgfältig geprüft und mit Verträgen zur Vertraulichkeit verpflichtet. Subunternehmen werden in regelmäßigen Abständen durch Audits geprüft.

1.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DSGVO, Art. 25 Abs. 1 DSGVO)

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird durch den Datenschutzbeauftragten und durch die Informationssicherheitsbeauftragte regelmäßig und kontinuierlich überprüft und verbessert.

Die BEX Components AG ist nach ISO 27001 zertifiziert. In jährlichen Audits wird das Informationssicherheitsmanagementsystem von unabhängigen externen Prüfern auditiert.

2 Anhänge und Verweise

Titel des Anhangs / Verweis	Beschreibung

3 Änderungshistorie

Datum	Bearbeiter	Beschreibung der Änderung
30.04.2018	KLV, RIA	Anlage des Dokuments
18.08.2020	KLS, KLV	Überarbeitung
23.04.2021	KLV	Überprüfung der Aktualität
26.04.2022	KLV	Technische und organisatorische Maßnahmen überarbeitet
22.02.2023	KLV	Technische und organisatorische Maßnahmen überarbeitet
10.09.2024	KLV	Technische und organisatorische Maßnahmen überarbeitet
15.11.2024	KLS	Inhalt in aktuelles Dokumenten-Design überführt. Link für die Subunternehmer eingefügt.

Noch Fragen? Kein Problem!
Wir sind für Sie da:

Per E-Mail:

datenschutz@bex.ag

Telefonisch:

+49 7361 999 39 10

(Mo-Fr: 8-16 Uhr)

Oder jederzeit unter:

www.bex.ag

BEX Components AG

Gartenstraße 97

73430 Aalen