Sicherheitskonzept

# Datensicherheit bei der AEB

Technische und organisatorische Maßnahmen / Controls

12.10.2024; V4.2

www.aeb.com

# Inhalt

# 1 Grundsätzliches zum Dokument

Dieses Dokument führt alle Sicherheits-Maßnahmensysteme (Controls) der Services der AEB SE auf.

Die Maßnahmen können sowohl technischer als auch organisatorischer Natur sein. Sie sind auf dem Stand der Technik und schließen auch den Faktor Mensch mit ein.

AEB ist berechtigt, die erforderlichen Maßnahmen anzupassen, sofern das bisher erreichte Sicherheitsniveau nicht unterschritten wird. Die hier dargestellten Maßnahmen sind - wenn nicht anders vereinbart - übergreifend im Sinne für alle Kunden gleich ausgelegt.

Dieses Dokument ist mit Angabe des Datums (Stand) versioniert.

Das Sicherheitskonzept ist für die jeweiligen Verwendungszwecke einzeln lesbar. Dadurch können sich in einzelnen Aspekten Doppelungen mit Ergänzungen ergeben.

## 1.1 Verwendungszweck Datenschutz

Nach geltenden Gesetzen (z.B. die EU-Datenschutz-Grundverordnung mit Art. 32 DS-GVO) sind geeignete technische und organisatorische Maßnahmen zu wählen, die dem erforderlichen Schutzbedarf der (personenbezogenen) Daten (im folgenden pbD.) entsprechend den gesetzlichen Anforderungen genügen. Erforderlich sind Maßnahmen nur, soweit ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

## 1.2 Verwendungszweck Security / Informationssicherheit

Dieses Dokument stellt den Stand der AEB-Sicherheitsmaßnahmen und -prinzipien dar. Diese werden als Minimal-Anforderungen Bestandteil eines Vertrags (Aufgrund AGB oder SLA) der AEB.

# 2 Allgemeines

## 2.1 Zertifizierungen

AEB stellt für den Themenbereich Sicherheit ihre Zertifikate im Trust Center zur Verfügung unter: https://www.aeb.com/de-de/trust-center/zertifikate.php

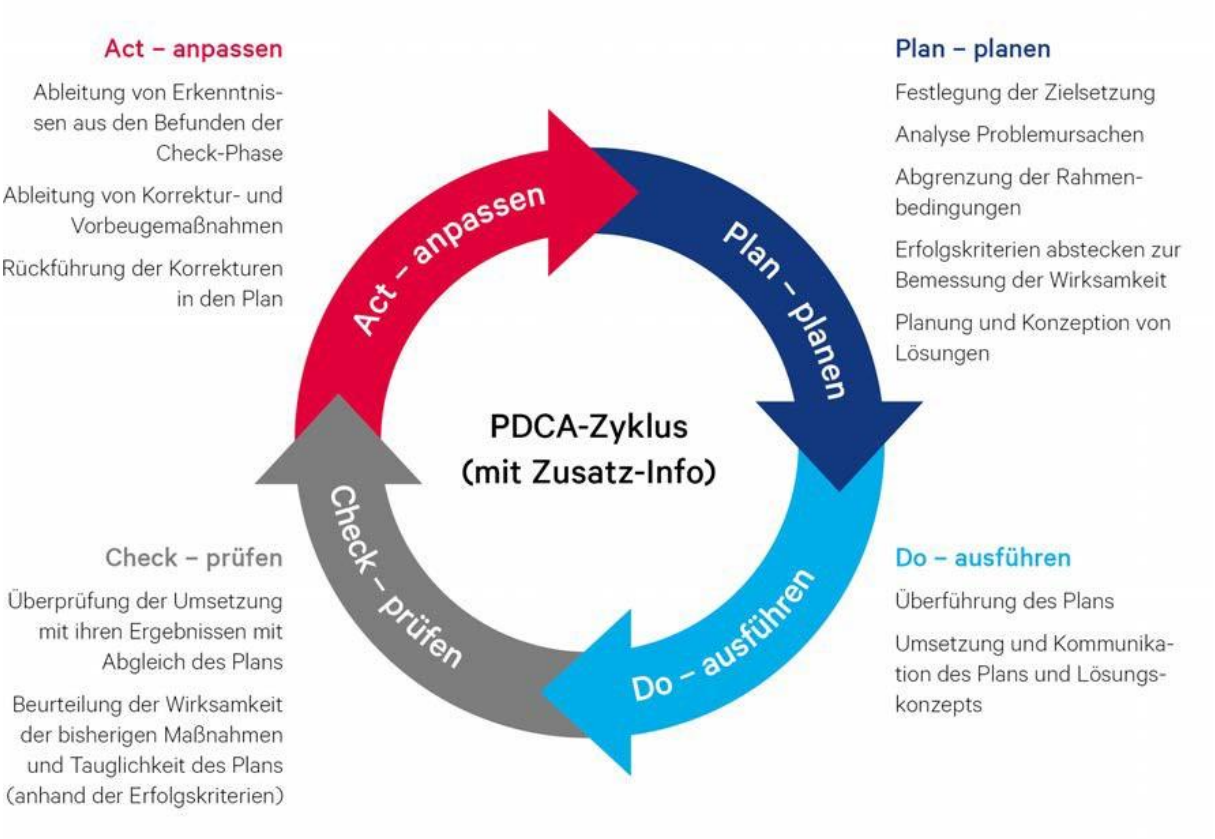
## 2.2 Applikationsablaufkontrolle

>> Sorge zu tragen, dass Applikationen richtig implementiert sind und die richtige Datenverarbeitung durch die Applikationen erfolgt.

- Sowohl die Services als auch die zugehörigen Techniken und Prozesse werden von der Koordinierenden Stelle (KoSt) ATLAS bei der Oberfinanzdirektion Karlsruhe geprüft und nur bei vollständiger Abbildung der Anforderungen zertifiziert.
- Prüf- und Zertifizierungsprotokolle liegen auch der KoSt ATLAS vor.

### 2.2.1 Qualitätssicherung

Qualität steht in allen Bereichen der AEB im Vordergrund. Ihr wird eine besondere Stellung eingeräumt. Aufgaben- und Prozessverantwortliche definieren, optimieren und prüfen die Prozesse der Applikationsentwicklung, aber auch der Wartung und des Services anhand des PDCA-Kreislaufs.




Im Bereich der Applikationen werden dabei nicht nur Funktions- sondern auch Usability-Tests durchgeführt. Jede Neuerung wird dabei mehrfach geprüft und abgenommen. Die Aktualität fachlicher Anforderungen wird ständig verfolgt und umgesetzt. Im engen Kundenkontakt wird Wartung und Service bewertet und optimiert. Die Arbeitsweise ist Service- und Prozessorientiert.

### 2.2.2 Qualitätssicherung durch definierte Prozesse

Alle Schritte der Neuentwicklung sowie die Wartung der Applikationen durchlaufen definierte und kommunizierte Prozesse (Prinzip der Transparenz). Alle Applikationsentwicklungs- und Wartungsaufgaben werden als Projekte mit definiertem Projektablauf (manifestiert in Muster-Projekten) und einem beschriebenen Prozess realisiert. Darin integriert ist ein umfassendes Rollenkonzept mit diversen Stufen der Freigaben unter Nutzung des 4-Augen-Prinzips. Zur Sicherstellung der Compliance sind außerdem Sicherheits-Checks vorgesehen.

### 2.2.3 Qualitätssicherung durch externe Prüfer

Applikationen werden - wo erforderlich - auch durch externe Prüfer geprüft und zertifiziert.

Dies geschieht u.a. in Anlehnung an IDW-Prüfungsstandards und Stellungnahmen wie IDW PS 330 („Abschlussprüfung bei Einsatz von Informationstechnologie“) oder IDW RS FAIT 1 („Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie“).

AEB wird jährlich nach dem deutschen (IDW PS 951 Typ 2), sowie dem internationalen Standard (ISAE 3402) geprüft. Diese entsprechen dem amerikanischen SOC 2.

Geprüft werden derzeit die Services:

- Export Filing: ATLAS,
- Compliance Screening,
- Export Filing Platform
- Warenursprung und Präferenzen / Origin and Preferences

aus der AEB Cloud.

## 2.3 Allgemeine organisatorische Kontrolle (Managementsysteme)

### 2.3.1 Datenschutz

Der betriebliche Datenschutzbeauftragte prüft und kontrolliert die Einhaltung der relevanten gesetzlichen Vorschriften. Der Datenschutzbeauftragte ist Teil des Datenschutzmanagementsystems und hält eine Datenschutzleitlinie verfügbar. Einige der nachfolgend geschilderten Kontrollen sind verpflichtend gemäß Art. 32 DS-GVO (technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung), auch unter Berücksichtigung der Datenschutz-Folgenabschätzung.

### 2.3.2 Sicherheitskontrolle, Risikomanagement

Der Betrieb des ISMS (Information Security Management System in Verbindung mit dem Zertifikat zur ISO 27001) stellt das IT-Security Management als kontinuierlichen Prozess-orientierten PDCA-Kreislauf sicher. Dieser Prozess, basierend auf Assets (Informationen, Werten), schließt Schutzbedarfsermittlung und detaillierte Risiko-Betrachtungen (Risikobewertung und -behandlung) ein.

Die wichtigsten und relevanten Schutzziele sind

- Verfügbarkeit
- Vertraulichkeit
- Integrität

Das ISMS enthält Kontrollen der Check-Phase u.a. in Form von internen und externen Audits, sowie regelmäßige Managementbewertungen. Eine weitere Ebene ist die Sicherstellung eines hohen Sicherheitsbewusstseins (security awareness) mit Hilfe diverser Maßnahmen zur Aus- und Weiterbildung der Beschäftigten.

Für eine umfassende Darstellung verweisen wir auf unsere Informationssicherheitsleitlinie (als Teil der Leitlinie Integriertes Managementsystem) in unserem Trust Center unter: https://www.aeb.com/de-de/trust-center/sicherheit.php

# 3 Datenschutz - Technische und organisatorische Maßnahmen

Die nachfolgende Zuordnung der Maßnahmen orientiert sich bis auf weiteres noch an der bis 25.05.2018 gültigen Fassung des (alten) BDSG.

Aus der seit 25.05.2018 anwendbaren EU-Datenschutz-Grundverordnung (kurz: DS-GVO) lassen sich auch Zuordnungen ableiten etwa nach den Schutzzielen Verfügbarkeit, Vertraulichkeit, Integrität (und Belastbarkeit). Zum Datenschutz der AEB als Cloud-Anbieter finden sich weitere Maßnahmen im Kapitel zur ISO 27018.

## 3.1 Eingabekontrolle

>> Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem Daten, insbesondere personenbezogene Daten, in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

- Alle Produkte, die personenbezogene Stammdaten verarbeiten, protokollieren sämtliche Eingaben, Änderungen, Löschungen. Diese Protokollierung stellt sicher, dass nachträglich festgestellt werden kann, ob und wenn von wem personenbezogene Stammdaten eingegeben, verändert oder entfernt worden sind.
- Personalisierte Benutzerkonten auch in den Fachanwendungen.
- Trennung von System- und Anwendungsprotokollen, dadurch ist eine Manipulation der Anwendungsprotokolle auf Systemebene ausgeschlossen.
- Zuordnung DS-GVO: Integrität

## 3.2 Auftragskontrolle

>> Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

- Regelung der Weisungen im Hauptleistungs- und Auftragsverarbeitungsvertrag
- Benutzer- und Rechteverwaltung auf Anwendungsebene durch den Auftraggeber
- Übermittlung/Erfassung der Daten durch den Auftraggeber. Er entscheidet, wann welche Daten übermittelt werden.
- Zugriff auf diese Daten haben nur Rollen mit entsprechender Zugriffsbefugnis

- Automatisierte Verarbeitung der Daten durch zertifizierte Software (z.B. Verfahren ATLAS, Compliance etc.). Dadurch wird sichergestellt, dass die Daten gem. beauftragten Verfahren verarbeitet werden.
- Einsatz von Standardverträgen gemäß gesetzlichen Vorgaben für Verhältnisse mit Kunden und Dienstleistern.
- Mitarbeitende werden regelmäßig an das Need-To-Know-Prinzip und ihre Verpflichtung zur Geheimhaltung erinnert
- Einbindung von Subunternehmen mit entsprechenden Verträgen zu Vertraulichkeit, Auftragsverarbeitung, Systemzugang.
- Zuordnung DS-GVO: Verfügbarkeit, Vertraulichkeit

## 3.3 Trennungskontrolle

>>Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

- Trennung von:
  – Mitarbeitendendaten
  – Kundenkontaktdaten
  – Kundentestdaten (Projektarbeit, Kundenentwicklungen)
  – Fernwartungszugangsdaten
  – Kundendaten im AEB-Rechenzentrum
- Systemebene:
  Kundendaten im Rechenzentrum werden von Daten der AEB (u.a. auch zu CRM-System) streng getrennt und in verschiedenen Systemen (Datenbanken…) verwaltet.
- Unterschiedliche Anwendungen:
  Für Kundendaten und Mitarbeitendendaten werden unterschiedliche Anwendungen eingesetzt.
- Berechtigungen innerhalb der Anwendung:
  Kundenkontaktdaten sind streng von Fernwartungszugangsdaten getrennt.
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit

## 3.4 Zutrittskontrolle

>>Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die Daten, insbesondere personenbezogene Daten, verarbeitet und genutzt werden, verwehren

Für den Hauptsitz Stuttgart (Rechenzentrum) gilt:

- Es gibt drei Bereiche: öffentlicher Bereich, private Bereich und besonders geschützte Bereich. Alle Zugänge sind gesichert durch Schlösser mit Transponder

- Die Ausgabe und Rücknahme von Transpondern wird dokumentiert
- Mitarbeitende werden im Zuge des Security Guide auf den Umgang mit Gästen unterwiesen
- Alle öffentlichen Zugänge, Liefer- und Ladebereiche befinden sich außerhalb der Sicherheitszonen. Die Anlieferungen in Sicherheitszonen erfolgen ausschließlich unter Aufsicht.

Für andere Standorte gelten gesonderte Regelungen zu Sicherheitsmaßnahmen am Standort, die den AEB Standard nicht unterschreiten. Regelungen stehen auch im Security Guide.

- Mehrstufige technische Schließsysteme, teilweise mit Ausrüstung zur Alarmierung.
- Sicherung des Gebäudes und Identitätskontrolle aller Anwesenden außerhalb der Geschäftszeiten durch einen Wachdienst.
- Regelung zur Zutrittsberechtigung für Nicht-Angestellte
- Zentrale Aufbewahrung zur Vergabe von elektronischen Codeschlüsseln (Tokens), Protokollierung der Aus- und Rückgabe.
- Server und Infrastrukturen (z.B. Fernwartungsrouter) sind durch Zutrittskontrolle (Codeschlösser, Codeschlüssel) zum Serverraum geschützt.
- Video-Überwachung zentraler Bereiche und systemkritischer Komponenten
- Fernwartungssysteme sind gesichert durch:
  - Zugriff auf Fernwartungsdaten nur für Berechtigte.
  - Systeme für Fernwartungszugänge zu Kunden stehen in einer abgeschotteten Netzwerkumgebung.
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit

## 3.5 Zugangskontrolle

>>Zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

- Arbeitsplatzrechner sind gesichert durch:
  – Anmeldung nur durch zentral gesteuertes Identity Management.
  – Verpflichtung der Mitarbeitenden zur Sperrung des Arbeitsplatzrechners.
  – Automatische Sperrung der Arbeitsplatzrechner nach höchstens 15 Minuten.
  – Eine Entsperrung ist nur mit dem persönlichen Zugangscode oder ggf. biometrischer Erkennung möglich
- Zentrale Kennwortrichtline:
  – für Administrationszugänge (regelmäßiger Zwang zur Änderung der Kennwörter, Mindestanforderung an Kennwortlänge und Komplexität, 2-Faktor-Authentifizierung).
  – für Mitarbeitendenzugänge (Mindestanforderung an Kennwortlänge und Komplexität, 2-FaktorAuthentifizierung).
  – für Kundenzugänge (regelmäßiger Zwang zur Änderung der Kennwörter, Mindestanforderung an Kennwortlänge und Komplexität).
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit, Integrität

## 3.6 Zugriffskontrolle

>> Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Daten, insbesondere personenbezogene Daten, bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

- Zentrale Berechtigungsverwaltung, getrennt für System- und Anwendungszugang.
- Anwender können Berechtigungen nicht selbständig ändern.
- Anwender können nicht ohne Freigabe durch Verantwortlichen (Vorgesetzte, Rollenverantwortliche, ...) eine Änderung beantragen; hierzu ist ein Freigabeprozess etabliert.
- Grundsätzlich keine externen Zugänge außer VPN- bzw. SSH gesicherte Verbindungen.
- Daten werden verschlüsselt gespeichert (z.B. in Datenbanken)
- Sicherheitsprüfungen / Penetrationstests der externen Zugänge durch darauf spezialisierte Firmen.
- Regelung bei Aufgaben- oder Rollenwechsel innerhalb Unternehmen.
- Zugriffsberechtigung ist Gegenstand im Zuge der Eröffnung und Pflege von Verarbeitungstätigkeiten
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit, Integrität

## 3.7 Weitergabekontrolle

>> Sorge zu tragen, dass Daten, insbesondere 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 Daten, insbesondere personenbezogene Daten, durch Einrichtungen zur Datenübertragung vorgesehen ist

- Der unternehmensweite Security Guide verbietet grundsätzlich den Versand von unverschlüsselten Daten.
- Alle Download-/Upload-Verbindungen via Internet sind gesichert durch entweder SSL/TLS, SSH oder VPN.
- Alle Niederlassungen bzw. mobilen Systeme verwenden ausschließlich VPN oder SSH gesicherte Verbindungen, die der Hoheit der AEB unterliegen.
- Es findet keine lokale Speicherung personenbezogener Daten statt, alle Daten werden zentral in den Systemen der AEB gehalten.
- Externe Verbindungen sind nur über freigegebene Anwendungen möglich.
- Externe Verbindungen sind nur über freigegebene Services möglich.

- Alle DFÜ-Verbindungen werden protokolliert so weit technisch machbar.
- Regelung zur Entsorgung von Abfällen mit vertraulichen Inhalten im Einklang mit relevanten DIN-Vorschriften (zu Schutzklasse und Sicherheitsstufen).
- Rechtliche Zulässigkeit, geeignete Garantien, etc. werden vertraglich sichergestellt.
- Es gilt das Need-To-Know-Prinzip
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit, Integrität

## 3.8 Verfügbarkeitskontrolle

>> Sorge zu tragen, dass Daten, insbesondere personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind

- Redundante Systeme
  – Datenbank: Cluster (bei Bedarf)
  – Fileserver: Cluster
  – SAN/Storage: redundante Komponenten
- Unterbrechungsfreie Stromversorgung (USV) incl. Netzersatzanlage (NEA)
- Brandmelde- und Brandlöschanlagen
- Bandsicherung
  – Regelmäßige Bandsicherung
  – Auslagerung der Daten in gesonderten Brandabschnitt/gesondertes Gebäude
  – Zuzüglich untertags regelmäßiger Sicherung der Nutzdaten auf Basis Datenbank-Tools
- Früherkennung von systemkritischen Zuständen durch Monitoring und Alerting
- Führen eines Notfallkonzepts (Business Continuity Management) zur Notfall-Prävention und -Bewältigung
- Regelmäßige Tests u.a. der Datensicherung/Back-up-Systeme
- Zuordnung DS-GVO: Verfügbarkeit, Belastbarkeit

## 3.9 Pseudonymisierung und Verschlüsselung

>> Sorge zu tragen, dass eine Rückbeziehbarkeit von Daten auf (natürliche) Personen zumindest eingeschränkt ist

- Maßnahmen zu Privacy-by-design und Privacy-by-default; incl. entsprechenden Schulungsmaßnahmen im Produktebereich; mit Geboten zur Datenvermeidung und Datensparsamkeit
- Alle Download-/Upload-Verbindungen via Internet sind gesichert durch entweder SSL/TLS, SSH oder VPN
- Standard-Prozess zur Festplattenverschlüsselung der Clients der Mitarbeitenden

- Möglichkeit zum remote wiping für mobile Geräte; Betrieb eines Mobile Device Managements (MDM)
- Eine Pseudonymisierung der Daten ist derzeit nicht vorgesehen. Begründung: Die personenbezogenen Daten sind geschäftlicher, nicht privater Natur. In der Interessensabwägung überwiegen die geschäftlichen Interessen. Diese bestehen u.a. auch in der Sicherstellung einer Revisionssicherheit.

## 3.10 Wiederherstellbarkeit und Zuverlässigkeit

>> Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können sowie Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

- Betrieb eines etablierten Incident Managements, mit entsprechenden Rollen zur Abarbeitung
- Früherkennung von systemkritischen Zuständen durch Monitoring, automatischer Behebung von Fehlzuständen und Benachrichtigung durch Alerting
- Durch automatisierte Failover-Mechanismen, insbesondere durch Virtualisierung, werden die Auswirkungen von Hardwareausfälle reduziert.
- Vorhalten eines Prozesses und Maßnahmen zum Emergency Management samt regelmäßiger Übungen dazu
- Vorhalten eines Prozesses und Maßnahmen zu Business Continuity Management (Notfall-Vorsorge und -Bewältigung)
- Vorhalten von Backup-Systemen

Sicherungen von Information, Software und Systemabbildern erfolgen über ein mehrstufiges Konzept spätestens alle 24h. Neben einer lokalen Sicherung auf Disk stehen entsprechende verschlüsselte Datenträger an einer sicheren, entfernten Location bereit.

Die Sicherungen werden regelmäßig, stichprobenartig mindestens einmal pro Monat, getestet. Ein Full Restore Test/DR Test findet mindestens jährlich statt.

Mehr Details zum Backupkonzept finden sich im Dokument "Auszug aus dem AEB Security Konzept: Details zum Backup", das im Trustcenter der AEB bereit steht.

Für den Cloud-Betrieb gilt zusätzlich: Mehr Details finden sich in der Servicebeschreibung (AEB Cloud oder AEB Private Cloud) und in weiteren Dokumenten im AEB Trust Center.

## 3.11 Sicherstellung der Belastbarkeit

>> Sorge zu tragen, dass eine ausreichende Widerstandsfähigkeit oder Robustheit auf Dauer vorliegt

- Betrieb ISMS -> prozessorientiert wird regelmäßig auf Schwachstellen und Bedrohungen geschaut; damit untermauern wir eine Nachhaltigkeit
- Führung einer Übersicht von Verarbeitungstätigkeiten mit integrierter Datenschutz-Folgenabschätzung und Einschätzung der Angemessenheit der technischen und organisatorischen Maßnahmen
- Integration Privacy-by-design im Produktmanagement -> Triggerung zur Vorabkontrolle durch Verfahrensverantwortlichen im Verbund mit dem DSB, auch zur Datenschutz-Folgenabschätzung (Pflege Verfahren samt Checks, Abstimmung, Analyse und Bewertung)
- Konkrete Prüfungen durch Penetrationstests.
- Einsatz von Next Generation Firewalls
- Aber auch Monitoring. Gutes Monitoring sorgt auch zu Früherkennung und somit zumindest Schadensbegrenzung, wenn nicht sogar noch Abwehr von Schädigungen durch Malware.
- Vorhalten von Puffern (Ressourcen) zum Abfangen außergewöhnlicher Last-Spitzen
- regelmäßige Erinnerung zu Hintergründen und Vorgehen bei Datenpannen
- regelmäßige Notfallübungen (BCM) sollen Einblick geben in etwaige Verbesserungsmaßnahmen zu Prävention und Vorsorge

## 3.12 Regelmäßigen Überprüfung der Wirksamkeit

>> Zur Gewährleistung der Sicherheit der Verarbeitung; mit Verfahren zu regelmäßiger Überprüfung und Bewertung der Wirksamkeit

- Durchführung von internen und externen Audits zu ISO 27001, Auftragsverarbeitung
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen mit den verantwortlichen Rollen, auch hinsichtlich des Stands der Technik
- Einbeziehung möglicher Referenzen (z.B. zu SDM-Standard-Datenschutzmodell)
- Konkrete regelmäßige Prüfungen durch Penetrationstests; mit Auswertung und Weiterverfolgung anhand der Befunde
- Managementbewertungen als regelmäßige Routine mit Geschäftsleitung und Datenschutzbeauftragtem
- Betrieb von Datenschutz als DSMS (Datenschutz-Managementsystem)

## 3.13 Berücksichtigung von (möglichen) Risiken

>> Sorge zu tragen, dass eine Risikoabwägung in die Verarbeitung oder Auswahl geeigneter technischer und organisatorischer Maßnahmen einfließt

- Betrieb eines ISMS mit zugehörigen Prozessen, Rollen und Werkzeugen

- dabei auch gesonderte Betrachtung von Risiken aus Sicht Betroffener
- Durchführung eines Verfahrens zur Datenschutz-Folgenabschätzung mit Integration in die Verfahren/Verarbeitungstätigkeiten und möglicher Einbeziehung der zuständigen Aufsichtsbehörde
- Berücksichtigung der einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), soweit als Auftragsverarbeiter von Bedeutung
- prozessgesteuerte Neubetrachtung unter Berücksichtigung aktueller Rahmenbedingungen und etwaigen Veränderungen (z.B. Eintrittswahrscheinlichkeiten zu Risiko-Szenarien)

## 3.14 Nichtverkettung

>> Sorge zu tragen, dass Daten nur für den Zweck verarbeitet werden, zu dem sie erhoben wurden (Zweckbindungsgrundsatz)

- Einsatz eines Rollenkonzepts zur Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
- Funktionstrennung gemäß Rollenkonzept
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements und eines sicheren Authentisierungsverfahrens
- geregelte Zweckänderungsverfahren (unter Berücksichtigung von Rechtsgrundlage, Erforderlichkeit, Vereinbarkeit)
- Durchführung regelmäßiger Schulungen zur Awareness

## 3.15 Transparenz

>> Sorge zu tragen, dass Informations- und Auskunftspflichten Rechnung getragen werden

- Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO (sowohl als Verantwortlicher als auch als Auftragsverarbeiter)
- Datenschutzerklärung als Teil des Web-Auftritts der AEB (s. AEB Trust Center)
- Unterstützung zu Informationspflichten zu Art. 30 DS-GVO, dargestellt im Datenschutz-Portal der AEB
- Integration datenschutzrechtlicher Prüfungen in den Freigabeprozess von Produkten oder Applications
- Vermittlung der Auskunftsrechte von Betroffenen an die Belegschaft

- Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden.
- Prozess zum Betrieb der Verfahren mit Verfahrensverantwortlichen mit regelmäßigem Austausch
- Prozess zu Verhalten bei Vorgängen zu Kap. 3 DS-GVO (Betroffenen-Rechte)

## 3.16 Intervenierbarkeit

>> Sorge zu tragen, dass Betroffene ihre Rechte zur Intervention ausüben können

- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes
- wo möglich Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Nachverfolgbarkeit der Aktivitäten des Verantwortlichen zur Gewährung der Betroffenenrechte
- Einrichtung eines Verfahrens für das Zusammenspiel zwischen Verantwortlichem und Auftragsverarbeiter für den Umgang mit Vorgängen Betroffener
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten
- regelmäßige Erinnerung zur Mitwirkungspflicht (für intern und auch für extern)

# 4 Informationssicherheits-Maßnahmen (Controls) der ISO 27001 / Annex A / SoA

Die nachfolgenden Controls sind die Controls des Annex A der ISO 27001:2023.
Sie sind in ihrer Nomenklatur aufgebaut nach den Ebenen:

- Sicherheitskategorien/Abschnitte (z.B. A.5)
- Control (z.B. A.5.1)

AEB nimmt hier zu den Anforderungen für alle Controls Stellung.
Jedes Control ist einem Control-Verantwortlichen zugewiesen. Die Pflege der Controls ist prozess-gesteuert und gemanagt. Dabei wird ein regelmäßiger Review, u.a. auch mit Blick auf Stand der Technik durchgeführt.

Damit kann die nachfolgende Liste als Erklärung zur Anwendbarkeit (Statement of Applicability, kurz: SoA) genutzt werden.
Umfassend gilt:

- Es gibt keine Ausschlüsse
- Alle Maßnahmen (Controls) sind umgesetzt und aktiv

Die AEB hat die ISO 27001 um die ISO 27018 erweitert. Aussagen zu dieser Norm sind erkennbar an dem jeweiligen Zusatz „Für Cloud-Betrieb gilt zusätzlich: …“. Weitere Controls aus dem Anhang A der ISO 27018, die den Datenschutz-Prinzipien zugeordnet sind, finden sich im separaten Kapitel "Informationssicherheits-Controls der ISO 27018 / Anhang A".

## 4.1 A.5 - Organisatorische Maßnahmen

### 4.1.1 A.5.1 - Informationssicherheitsrichtlinien

>> Informationssicherheitspolitik und themenspezifische Richtlinien sollten definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.

In der Leitlinie "Integriertes Management System" (IMS) ist das Management der Informationssicherheit definiert.

Im internen "Security Guide" sind die Sicherheitsrichtlinien festgeschrieben.

Beide Dokumente sind Richtliniendokumente und unterliegen der Dokumentensteuerung. Die darin festgelegten Richtlinien sind für alle Mitarbeitenden und Partner verbindlich. Sie sind von der Geschäftsleitung genehmigt, herausgegeben und den Beschäftigten, sowie relevanten externen Parteien bekanntgemacht.

- Die Leitlinie "Integriertes Management System" (IMS) ist im Trust Center jederzeit verfügbar unter: https://www.aeb.com/de/trust-center/sicherheit.php
- Eine Einsichtnahme in den Security Guide ist bei AEB (z.B. im Rahmen eines Audits) möglich.

Die Dokumente sind einem PDCA-Zyklus unterworfen. Sie können jederzeit bei Freigabe durch die ISMS-Leitung modifiziert werden. Typische Situationen für Änderungsbedarfe sind z.B. Erkenntnisse in Managementbewertungen, insbesondere zum Jahreswechsel. Die Managementbewertungen sehen vor, die Policy zu hinterfragen. Änderungsbedarfe werden im ISMS-Dokument zu Korrektur- und Vorbeugemaßnahmen begleitend gepflegt; sie können auch die Regeln der Leitlinie betreffen.

Für Cloud-Betrieb gilt zusätzlich: Die Leitlinie IMS und die Datenschutzleitlinie der AEB stellen klar, dass die AEB als IT-Provider die (datenschutzrechtliche) Gesetzgebung beachtet und als Auftragsverarbeiter ihre Kunden unterstützt. Entsprechend bietet die AEB eine maßgeschneiderte und aktuelle Vorlage zu Vereinbarungen zur Auftragsverarbeitung (in ihrem Trust Center). Darin werden die Verantwortlichkeiten klargestellt.

### 4.1.2 A.5.2 - Informationssicherheitsrollen und -verantwortlichkeiten

>> Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit sollten entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.

Die Sicherheitsverantwortlichkeiten für Informationssicherheit sind festgelegt und zugeordnet. Unter anderem sind folgende Verantwortliche etabliert:

- IT-Security Manager als Verantwortlicher für die Informationssicherheit. Er ist zu erreichen unter Security@aeb.com
- Verantwortlicher für das ISMS Management
- Verantwortlicher für Security Operations
- Verantwortlicher für Software Security Assurance
- Sicherheitsverantwortliche für die Fachbereiche
- Datenschutzbeauftragter
- Notfallbeauftragter

Siehe dazu auch unsere Leitlinie "Integriertes Managementsystem (IMS)" in unserem Trust Center unter: https://www.aeb.com/de/trust-center/sicherheit.php

### 4.1.3 A.5.3 - Aufgabentrennung

>> Sich widersprechende Aufgaben und Verantwortungsbereiche sollten voneinander getrennt werden.

Aufgaben- bzw. Funktionstrennung ist Teil unseres Internes Kontrollsystem (IKS). Dazu betreiben wir ein intensives Management und Arbeiten mit Rollen. In diesen sind Verantwortungen, Aufgaben und Kompetenzen abgebildet und mit dem Berechtigungskonzept verknüpft. Eine Liste von Rollenunverträglichkeiten wird geführt und bei der Rollenvergabe beachtet.

Siehe dazu auch unsere Leitlinie "Integriertes Managementsystem (IMS)" in unserem Trust Center unter: https://www.aeb.com/de-de/trust-center/sicherheit.php

### 4.1.4 A.5.4 - Verantwortlichkeiten der Leitung

>> Die Leitung sollte von dem gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.

Alle neuen Mitarbeitenden durchlaufen ein verpflichtendes Ausbildungsprogramm, dessen Teilnahme dokumentiert wird. Inhalte dieses Ausbildungsprogramms sind festgelegt und beinhalten auch die Informationssicherheit. Anschließend vermittelt die Leitung zusätzlich und regelmäßig Security-Inhalte für alle Mitarbeitenden. Die Verantwortung für die Wahrnehmung der Inhalte liegt beim Mitarbeitenden selbst und bei den betreuenden Kollegen.

### 4.1.5 A.5.5 - Kontakt mit Behörden

>> Die Organisation sollte mit den zuständigen Behörden Kontakt aufnehmen und halten.

Als relevante Behörden sehen wir u.a.:

- Innenministerium Baden-Württemberg (Landes-Datenschutzbeauftragter)
- IHK
- BSI
- Weitere Behörden z.B. in Deutschland, der EU, dem europäischen Ausland, ...

Interne Gremien und verantwortliche Rollen pflegen diese relevanten Kontakte.

Unter Kontakt-Pflege verstehen wir auch Besuche von Kongressen oder Weiterbildungsangeboten (z.B. des LfDI oder an IHK).

### 4.1.6 A.5.6 - Kontakt mit speziellen Interessensgruppen

>> Die Organisation sollte Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden herstellen und pflegen.

Hier gelten die gleichen Aussagen, wie zu A.5.5 - Kontakt mit Behörden.

Kontakte zu Security-Fachverbänden oder Interessengruppen werden von Zuständigen (z.B. Datenschutzbeauftragter) gepflegt und bedarfsorientiert wahrgenommen. Zahlreiche Netzwerke und Medien (wie Newsletter, Zeitschriften, Foren, Webinare) werden genutzt.

### 4.1.7 A.5.7 - Bedrohungsintelligenz

>> Informationen über Bedrohungen der Informationssicherheit sollten erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.

AEB unterscheidet Angriffspfade, Motive und Bedrohungsintelligenz.

AEB schützt sich geeignet mit Blick auf Angriffspfade unter Nutzung von Bausteinen des BSI.

Mögliche Motive und Bedrohungsintelligenz sind dynamisch und werden entsprechend regelmäßig betrachtet, um bei entsprechender Einschätzung im Risikomanagement vermutete Eintrittswahrscheinlichkeiten neu zu justieren.

Dazu dienen entsprechend eingerichtete Austausch-Runden im ISMS-Umfeld, aber auch Befunde aus technischen Quellen, Auswertungen von Sicherheitsvorfällen und Pentests.

Weiterbildungsmaßnahmen sensibilisieren zu Methoden, Werkzeugen und Technologien möglicher Angreifer.

### 4.1.8 A.5.8 - Informationssicherheit im Projektmanagement

>> Die Informationssicherheit sollte in das Projektmanagement integriert werden.

Bei Projekten (Charakteristik B) sind Sicherheits-Checks integriert

Diese Checks werden vom Project Management durchgeführt, unterstützt von einem Security Mitarbeitenden. Dabei richtet sich der Blick u.a. auf die Schutzbedarfsermittlung zu:

- Verfügbarkeit (z.B. von Systemen in der AEB Cloud)
- Vertraulichkeit und Datenschutz
- Integrität

Des Weiteren werden im Projekt Änderungen durch dokumentiertes Change-Request & Release-Management nachvollziehbar gemacht.
Die Verwendung von (Security-)Standards für Programm-Code und Schnittstellen findet sowohl in den Projekten der Standardentwicklung als auch in Kundenprojekten statt.

### 4.1.9 A.5.9 - Inventar der Informationen und anderen damit verbundenen Werten

>> Ein Inventar der Informationen und anderen damit verbundenen Werten, einschließlich der Eigentümer, sollte erstellt und gepflegt werden.

- Clients und Clientkomponenten werden inventarisiert und toolgestützt verwaltet.
- Die Inventarisierung von Werten ist eine frühe Phase des wiederkehrenden Prozesses beim Betrieb unseres ISMS.
- Die Inventarisierung wird im internen Risikomanagement-Tool verwaltet.
- Im Zuge der Inventarisierung wird auch erfasst und geprüft, dass es zu jedem Wert einen Eigentümer gibt.
- Der Eigentümer kann auch an eine Rolle geknüpft sein.
- In der Verantwortung der Rolle liegt es, die Schutzmaßnahmen wirksam zu betreiben. Nähere Instruktionen können Zuständige dem internen ISMS Guide entnehmen.

### 4.1.10 A.5.10 - Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

>> Regeln für den zulässigen Gebrauch und Verfahren für den Umgang mit Informationen und anderen zugehörigen Vermögenswerten sollten aufgestellt, dokumentiert und angewendet werden.

Regelung und Verwaltung geschehen über Vorgaben zu Schutzzielen, die aus Richtlinien-Dokumenten wie Security Guide und ISMS Guide angesprochen werden. Dabei werden Kriterien vorgegeben, die zur Einstufung für den zulässigen Gebrauch anleiten. Konkrete Schutzbedarfe werden im Zuge des ISMS im internen Risikomanagement-Tool hinterlegt und gepflegt.

Der gesamte Ablauf zum Umgang mit Werten ist in der AEB-internen Richtlinie "ISMS Guide" enthalten.

Wir führen eine Anleitung zum Umgang mit Kennzeichnungspflichten.

Im Falle von datenschutzrechtlichen Verarbeitungstätigkeiten findet eine Kontrolle und regelmäßige Pflege durch Regeln des internen DSMS im Umgang mit dem Verzeichnis von Verarbeitungstätigkeiten statt.

### 4.1.11 A.5.11 - Rückgabe von Werten

>> Das Personal und gegebenenfalls andere interessierte Parteien sollten alle Werte der Organisation, die sich in ihrem Besitz befinden, bei Änderung oder Beendigung ihres Beschäftigungsverhältnisses, Vertrags oder ihrer Vereinbarung zurückgeben.

In der Personalverwaltungssoftware wird bei Austritt automatisch eine Aufgabe, in Form einer Checkliste, zur Rückgabe von Werten angelegt und geprüft. Die jeweiligen Verantwortlichen kümmern sich um die Umsetzung und Dokumentation. Die Rückgabe des Transponders wird zusätzlich über einen Task in der Personalverwaltungssoftware abgewickelt.

### 4.1.12 A.5.12 - Klassifizierung von Information

>> Informationen sollten entsprechend den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.

- AEB klassifiziert Informationen und Dokumente
- Führende Grundlage ist die Leitlinie "Integriertes Managementsystem (IMS) (siehe auch in unserem Trust Center unter: https://www.aeb.com/de/trust-center/sicherheit.php ).
- Schutzziele dienen zur toolgestützten Einstufung von Schutzbedarfen auf der Ebene einzelner Werte.
- Schutzbedarfe sind wiederum Grundlage für nachfolgende Risikobetrachtungen, wie auch z.B. einer Datenschutz-Folgenabschätzung.

### 4.1.13 A.5.13 - Kennzeichnung von Information

>> Ein angemessener Satz von Verfahren zur Kennzeichnung von Information sollte entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden

Dieser Satz Verfahren ergibt sich aus

- der Auswahl des internen Risikomanagement-Tools
- seiner Benutzerdokumentation
- und einem Brückenschlag dieser Benutzerdokumentation und unserem ISMS Guide durch die Hilfen in Risikomanagement-Tool

Eine Darstellung des Business Impact findet auf Werte-Ebene (Prozesse und/oder Assets) statt, bei der Angaben zu Verfügbarkeit, Vertraulichkeit und Integrität getroffen werden. Dazu sind fest vorgegebene Werte auszuwählen (von "unbedeutend" bis "bedrohlich"). Die interne Vorgabe enthält geeignete Hilfestellung, um die jeweilige Festlegung zu treffen.

Dokumente unterliegen einer gemanagten Dokumentenlenkung.

### 4.1.14 A.5.14 - Informationsübertragung

>> Für alle Arten von Übertragungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien sollten Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.

#### Generell

Der Umgang mit der Übertragung von Daten (Data on the move) ist für innerhalb der Organisation und mit externen Partnern vereinbart. Entsprechende Verfahren und Maßnahmen dazu sind implementiert und werden angewendet.

Diese sind insbesondere in den Richtliniendokumenten Security Guide und Partnermanagement Guide festgelegt und kommuniziert.

Die Vereinbarungen mit Partnern finden sich auch in den entsprechenden Verträgen, unter anderem in Non Disclosure Agreements (NDA), Partner-Verträgen für den Systemzugang, den entsprechenden Servicebeschreibungen (die Vertragsbestandteil sind) oder individuellen Service Level Agreements (SLA) mit den Kunden.

#### Details

AEB differenziert Netzwerke in "Zonen". Dabei ist

- jedes externe Netzwerk eine Zone. Also ist z.B. das Netzwerk eines Kunden eine Zone. Oder das Netzwerk eines Carriers
- intern ist das Netzwerk bewusst stark segmentiert. Insbesondere durch VLANs sind die verschiedenen Bereiche voneinander getrennt. So gibt es z.B. eigene Zonen für Mitarbeitende, für Gäste oder für spezielle Services

Den Übergang/die Datenübertragung zwischen zwei Zonen wird als "Zonenwechsel" bezeichnet.

Alle Daten, die übertragen werden, werden spätestens, wenn sie einen Zonenwechsel machen, verschlüsselt.

Die Verschlüsselung ist üblicherweise mindestens TLS 1.2 (mit AES 256 Bit).

### 4.1.15 A.5.15 - Zugangssteuerung

>> Regeln zur Kontrolle des physischen und logischen Zugriffs auf Informationen und andere zugehörige Werte sollten auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.

Der Zugang zu Netzwerken und Netzwerkdiensten wird über rollenbasierte Gruppen und entsprechende Gruppenzugehörigkeiten festgelegt. Die benötigten Rechte werden über die jeweiligen Rollen zugeteilt. Netzwerke sind stark segmentiert und jedes Segment durch nextGen Firewalls geschützt.

Grundlegend gilt:

- Need-to-Know-Prinzip
- So viel Zugriff wie nötig, so wenig wie möglich

Sowohl die Richtlinie, das Einhalten der Zugangssteuerung, die beteiligten Systeme und Netze, als auch die Rollen und deren Rechte werden regelmäßig mindestens einmal pro Jahr überprüft.

### 4.1.16 A.5.16 - Identitätsmanagement

>> Der gesamte Lebenszyklus von Identitäten sollte verwaltet werden.

AEB erstellt und verwaltet vier Arten von Benutzerkonten:

- Benutzerkonten für Intern (Mitarbeitende, Partner)
- Benutzerkonten für die Verwendung der AEB Cloud Lösungen (Kunden, Partner)
- Privilegiert Benutzerkonten für Intern (Mitarbeitende)
- Privilegiert Benutzerkonten für die Administration der eigenen Cloud Lösungen (Kunden)

Für alle Benutzerkontenarten sind Prozesse definiert und umgesetzt, die das korrekte Registrieren und Deregistrieren von Benutzern sicherstellen. Z.B. werden Mitarbeitendenkonten durch Eintritt ins Unternehmen automatisch angelegt und durch Ausscheiden automatisch deaktiviert und nach Ablauf einer Frist automatisch gelöscht. Die Verwaltung erfolgt z.B. über ein zentrales Identity and Access Management (IAM)

AEB führt in regelmäßigen Abständen Überprüfungen auf ungenutzte Zugangsdaten durch. Nach Bekanntwerden einer Kompromittierung wird das Zurücksetzen betroffener Accounts über einen organisatorischen Prozess geregelt.

Für den Cloud-Betrieb gilt zusätzlich: Der Konfigurationsleitfaden im Serviceportal der AEB widmet sich auch dem Administrator des eigenen Mandanten (I_CLIENTADMIN) zum Thema Einrichtung von Usern.

### 4.1.17 A.5.17 - Information zur Authentifizierung

>> Die Zuweisung und Verwaltung von Authentifizierungsinformationen sollte durch einen Managementprozess gesteuert werden, der auch die Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen umfasst.

Die Zuweisung und Verwaltung geheimer Authentisierungsinformationen ebenso wie der Umgang damit wird in AEB über einen formalen Prozess gesteuert. Diese werden in AEB nur verschlüsselt gespeichert. AEB Mitarbeitende verwenden ein entsprechendes Passwort-Tool. Die Regelungen dazu sind im internen Security Guide dokumentiert.

AEB setzt für die Verwaltung von Kennwörtern ein zentrales Passwort Tool nach Stand der Technik ein. Dieses stellt unter anderem sicher:

- Verwendung von starken Passwörtern
- Rollenbasiertes Rechtekonzept für den Zugang und Zugriff pro Passwort oder Passwort Gruppe
- Protokollierung aller Änderungen
- Protokollierung aller Zugriffe

Die Pflicht das Passwort Tool in allen Fällen zu verwenden ist durch entsprechende Richtlinien festgelegt.

### 4.1.18 A.5.18 - Zugangsrechte

>> Zugangsrechte zu Informationen und anderen zugehörigen Werten sollten in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.

Siehe auch A.5.16 - Identitätsmanagement

Bei Eintritt, Austritt sowie Verantwortungswechsel (wie z.B. Rollenwechsel, Teamwechsel, ...) werden automatisch Aufgaben in der Personalverwaltungssoftware und/oder im internen Ticketing angelegt, in welchen auch die Rollen und Rechte überprüft werden.

Regelmäßig (mindestens jährlich) werden Accounts und Rechte in allen für den Zugriff auf Informationen relevanten Objekten (Verzeichnissen, Konten, Rollen, Anwendungen, ...) durch die jeweiligen Verantwortlichen geprüft.

Außerdem werden führt in regelmäßigen Abständen (mindestens jährlich) Überprüfungen auf ungenutzte Zugangsdaten durchgeführt. Nach Bekanntwerden einer Kompromittierung wird das Zurücksetzen betroffener Accounts über einen organisatorischen Prozess geregelt.

### 4.1.19 A.5.19 - Informationssicherheit in Lieferantenbeziehungen

>> Es sollten Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu beherrschen.

AEB hat Frameworks im Partnermanagement und Applikationsmanagement geschaffen, die das entsprechend sicherstellen.

- Die Integriertes Management System (IMS) Guideline berücksichtigt auch die Lieferantenbeziehungen für die Bereiche Qualität und Sicherheit
- Ausdruck finden die Sicherheitskriterien in den jeweiligen Verträgen für Systemzugänge durch Partner je Zugangstiefe - diese werden regelmäßig geprüft und Partner entsprechend auditiert.
- Bezüglich Vertraulichkeit stehen Standard-Verträge zur Verfügung - Es werden zusätzlich NDA genutzt, die z.B. auch in der Gästeanmeldung vorgeschlagen werden.

- Entsprechende AV Verträge sind geschlossen

### 4.1.20 A.5.20 - Behandlung von Informationssicherheit in Lieferantenvereinbarungen

>> Je nach Art der Lieferantenbeziehung sollten die entsprechenden Anforderungen an die Informationssicherheit festgelegt und mit jedem Lieferanten vereinbart werden.

Lieferanten und Partner werden klassifiziert und abhängig von dieser Klassifizierung und ggf. eine Schutzbedarfsermittlung sind Anforderungen an die Informationssicherheit der Lieferanten und Partner festgelegt. Das Integriertes Management System (IMS) Guideline berücksichtigt auch die Lieferantenbeziehungen für die Bereiche Qualität und Sicherheit

Ausdruck finden die Sicherheitskriterien auch z.B. in den jeweiligen Verträgen für Systemzugänge durch Partner je Zugangstiefe.

Partner werden regelmäßig geprüft und gemäß der Klassifizierung entsprechend auditiert

Bezüglich Vertraulichkeit stehen Standard-Verträge zur Verfügung; NDA, die auch in der Gästeanmeldung vorgeschlagen werden.

### 4.1.21 A.5.21 - Umgang mit der Informationssicherheit in der IKT-Lieferkette

>> Es sollten Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen. (IKT = Informations- und Kommunikationstechnologien)

AEB hat ein Partnermanagement und ein Applikationsmanagement etabliert, die sicherstellen, dass Anforderungen in Vereinbarungen mit Lieferanten aufgenommen werden. Diese enthalten und definieren den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen sowie der Produktlieferkette verbunden sind.

Siehe dafür auch A.5.20 - Behandlung von Informationssicherheit in Lieferantenvereinbarungen

### 4.1.22 A.5.22 - Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen

>> Die Organisation sollte regelmäßig die Informationssicherheitspraktiken der Lieferanten und die Erbringung von Dienstleistungen überwachen, überprüfen, bewerten und Änderungen steuern.

Dienstleistungserbringung durch Lieferanten sowie deren Änderungen werden überwacht, regelmäßig überprüft und auditiert. Dies wird gesteuert und sichergestellt durch das Partnermanagement und die dort etablierten Prozesse.

### 4.1.23 A.5.23 - Informationssicherheit für die Nutzung von Cloud-Diensten

>> Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten sollten in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt werden.

Cloud -Dienste unterliegen ebenso wie alle anderen Applikationen einem ausführlichen Applikationmanagement, das einen besonderen Fokus auf Sicherheit und Datenschutz sowie eine Analyse und regelmäßige Überprüfung der Anbieter. legt.

Zusätzlich hat AEB für Cloud Services die AEB nutzt besondere Rahmenbedingungen festgelegt.

### 4.1.24 A.5.24 - Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen

>> Die Organisation sollte die Handhabung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.

Der Prozess zur Sicherheitsvorfallmeldung ist organisiert und wird regelmäßig kommuniziert. Die Meldung erlaubt dazu mehrere Möglichkeiten zur Auslösung und wird toolgestützt prozessiert. Mögliche Empfänger (etwa zu IT-Sicherheitsvorfällen, Datenpannen, Emergencies) sind durch Rollen verankert und geschult.

Für den Cloud-Betrieb gilt zusätzlich: AEB hat einen internen Prozess zur Meldung und Behandlung von Datenpannen aufgesetzt. Dabei wird u.a. die Kritikalität entsprechend den Sicherheitskriterien analysiert und im weiteren Vorgehen berücksichtigt. Im Bedarfsfall sieht der Prozess vereinbarungsgemäß eine Zusammenarbeit mit den betroffenen Kunden vor.

### 4.1.25 A.5.25 - Beurteilung und Entscheidung über Informationssicherheitsereignisse

>> Die Organisation sollte Ereignisse im Bereich der Informationssicherheit beurteilen und entscheiden, ob sie als Vorfälle im Bereich der Informationssicherheit eingestuft werden sollen.

AEB hat Prozesse für Sicherheitsereignisse implementiert, die sicherstellen, dass diese so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet und bearbeitet werden.

Dies umfasst sowohl Prozesse für den Regelbetrieb (den Prozess Security Event Management) als auch für Ausnahmesituationen (Prozess Security Incident Management und Prozesse im Emergency Guide sowie im Business Continuity Management (BCM) und bei Datenpannen im Datenschutz-Bereich).

Darüber hinaus finden regelmäßige Termine statt, bei denen die Meldungen bzgl. Kritikalität bewertet werden.

### 4.1.26 A.5.26 - Reaktion auf Informationssicherheitsvorfälle

>> Auf Informationssicherheitsvorfälle sollte entsprechend den dokumentierten Verfahren reagiert werden.

AEB hat Prozesse für Sicherheitsvorfälle implementiert, die sicherstellen, dass Informationssicherheitsereignisse so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet und bearbeitet werden.

Dies umfasst sowohl Prozesse für den Regelbetrieb (den Prozess Security Event Management) als auch für Ausnahmesituationen (Prozess Security Incident Management und im Emergency Guide sowie im Business Continuity Management (BCM) und Datenpannen im Datenschutz-Bereich).

### 4.1.27 A.5.27 - Erkenntnisse aus Informationssicherheitsvorfällen

>> Aus Informationssicherheitsvorfällen gewonnene Erkenntnisse sollten zur Verstärkung und Verbesserung der Informationssicherheitsmaßnahmen genutzt werden.

AEB hat einen Security Incident Prozess etabliert. Zu diesem gehört auch, dass sich um die Erkenntnisse aus Sicherheitsereignissen gekümmert wird und diese nachhaltig bearbeitet werden. Gleiches gilt auch für den Emergency Prozess oder die Bearbeitung von Datenpannen.

Auch regelmäßige Termine stellen zusätzlich die Auswertung und Beschäftigung mit Erkenntnissen sicher.

### 4.1.28 A.5.28 - Sammeln von Beweismaterial

>> Die Organisation sollte Verfahren für die Identifizierung, Sammlung, Beschaffung und Aufbewahrung von Beweismitteln im Zusammenhang mit Informationssicherheitsvorfällen einführen und umsetzen.

AEB hat Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, festgelegt und wendet diese an.

### 4.1.29 A.5.29 - Informationssicherheit bei Störungen

>> Die Organisation sollte planen, wie die Informationssicherheit während der Störung auf einem angemessenen Niveau gehalten werden kann.

AEB betreibt ein Prozess-Management, das bzgl. Security verschiedene Phasen kennt. Die jeweiligen Zustände und zugehöriges Verhalten sind dokumentiert und werden geschult. Ab einer Störung greift der Prozess Security Incident Management. Besonderer Wert wird gelegt auf die jeweiligen Übergänge Richtung weiterer Eskalation Richtung Notfallmanagement sowie die jeweiligen zu verwendenden Instrumente wie Hinzuziehung weiterer Rollen und Anleitungen wie z.B. Notfallplänen.

AEB hat ihre Anforderungen an die Informationssicherheit und zur Aufrechterhaltung des Informationssicherheitsmanagements bei widrigen Situationen, z. B. Krise oder Katastrophe festgelegt und sich dazu entsprechend aufgestellt.

Ein Managementsystem für BCM ist eingerichtet; es beachtet die Perspektiven Notfallprävention und Notfallbewältigung.

Dies ist unter anderem hier dokumentiert:

- https://www.aeb.com/de/trust-center/sicherheit.php#Notfallvorsorge

Für die Beachtung der Anforderungen des BCM ist ein Notfallbeauftragter eingerichtet, der in Abstimmung mit der Geschäftsleitung und betroffenen Ressourcen, etwa aus Infrastruktur und IT geeignete Vorkehrungen trifft. Regelmäßig eingeplante und durchgeführte Übungen helfen, mit Notfällen möglichst gut vorbereitet umzugehen und etwaige Lücken zu schließen. Im Zuge dessen werden Notfallpläne erarbeitet bzw. gepflegt.

Auch die Überprüfung auf Wirksamkeit ist Teil des Notfall-Konzepts. Notfallvorsorgekonzept und zugehöriges Projekt für das BCM sehen z.B. Notfall-Übungen vor. Mit Blick auf Kritikalitäten werden diese Übungen gemeinsam konzipiert, durchgeführt und mit Blick auf Nachhaltigkeit ausgewertet. Regelmäßige Verfügbarkeitsberichte belegen den Status der Kontinuität. Auch die Termine für geplante Wartungsarbeiten enthalten immer wieder auch Tests in Richtung Ausfallsicherheit.

Zum BCM gibt es regelmäßiges Reporting (Notfallbeauftragter gemeinsam mit IT-Security und GL).

Durch regelmäßigen Austausch wird der Bedarf für neue Notfall-Übungen festgelegt.

### 4.1.30 A.5.30 - IKT-Bereitschaft für Business Continuity

>> Die IKT-Bereitschaft sollte auf der Grundlage von Business-Continuity-Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.

- AEB zerlegt die Aufgabenstellung in Notfall-Prävention, weitere Vorsorge und -Bewältigung
- Ziele sind hohe Verfügbarkeit, Awareness und Resilienz in den Situationen Prävention (möglichst Vermeidung) und Bewältigung (größtmögliche Schadensminimierung hinsichtlich Dauer und Höhe); mit Blick auf AEB und ihre Kunden
- Führend ist unsere BCM-Leitlinie
- Ergebnis sind auch Security-KPI im Zshg. mit Notfällen
- Vorgaben sind u.a. Bereithalten aktueller unterstützender Notfallpläne, Durchführung von Notfall-Übungen samt zugehöriger Auswertung von Erkenntnissen zur Resilienz und Sensibilisierung und Schulung betroffener organisatorischer Einheiten bis hin zum Krisenstab
- zur Fokussierung auf kritische Prozesse dient ein Fahrplan zur BIA (Business Impact Analyse), die Daten des Risiko-Tools des ISMS nutzt. Im Fahrplan werden Einschätzungen zu RTO und RPO integriert.

### 4.1.31 A.5.31 - Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen

>> Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit relevant sind, und die Vorgehensweise der Organisation zur Erfüllung dieser Anforderungen sollten ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden.

Die AEB hat Verfahren und Maßnahmen festgelegt, um sicherzustellen, dass alle rechtlichen, gesetzlichen, behördlichen und vertraglichen Anforderungen, die für die Informationssicherheit von Bedeutung sind, stets erfüllt werden.

Dies umfasst sowohl die regelmäßige Überprüfung dieser Anforderungen und stellt sicher, dass sie identifiziert und dokumentiert werden als auch die kontinuierliche Überprüfung und Anpassung der entsprechenden Dokumentationen und Prozesse, um den aktuellen Standards und Vorschriften gerecht zu werden.

Ein Compliance-Officer ist installiert und mit dieser Aufgabenstellung betraut, die relevanten Regeln und Pflichten zu eruieren und in der Organisation dafür zu sorgen, dass sie gemanagt beachtet werden.

Viele Informationen erhält der Kunde, Partner oder Mitarbeitende bereits in unserem Trust Center https://www.aeb.com/TrustCenter/. Bei weiteren Fragen oder erweiterten Anforderungen vereinbaren wir individuelle Verträge mit den Kunden über das Team Legal oder geben weitere Informationen über das Compliance Team (hier auch ggf. das Tender Management).

Nachfolgend werden einige Bestandteile gelistet:

- ISMS (DE)
- Code of Conduct - Verhaltenskodex (DE)
- Anti-Korruption (DE)
- AGB 3.0

Zur Meldung von Verstößen gegen gesetzliche Vorschriften, unseren Code of Conduct oder unsere Compliance Richtlinien haben wir ein Hinweisgebersystem installiert. Unser rechtsanwaltlicher Ombudsmann nimmt Hinweise vertraulich entgegen.

Die Datenhaltung der AEB befindet sich in Deutschland. Bei der Daten-Übermittlung (einschließlich Nutzung) werden die anwendbaren datenschutzrechtlichen Erfordernisse beachtet. Näheres kann https://www.aeb.com/de/trust-center/rechenzentren.php entnommen werden.

Außerdem ist eine Richtlinie für den Gebrauch von kryptographischen Maßnahmen zum Schutz von Information ist entwickelt umgesetzt. Auf sie wird im internen Security Guide verwiesen.

### 4.1.32 A.5.32 - Geistige Eigentumsrechte

>> Die Organisation sollte geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.

Durch entsprechende Lizenzverträge oder entsprechenden Passus in der AGB der AEB SE sowie entsprechende Prozesse, kann die Einhaltung der Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützter Software sichergestellt werden. Die Verwendung und

Bedingungen der Open Source Software sowie proprietärer Software von Drittanbietern wird hier durch AEB transparent für die Vertragspartner dargestellt: http://documents.aeb.com/licenses/xnsg_nsg/de/index.html. Außerdem findet der Vertragspartner hier auch eine Auflistung der Third Party Komponenten.

### 4.1.33 A.5.33 - Schutz von Aufzeichnungen

>> Aufzeichnungen sollten vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.

Sofern keine abweichenden Aufbewahrungspflichten vorliegen, bewahren wir alles 10 Jahre auf. Es gelten für die elektronische Ablage die Regeln für Datensicherung. Dies ist dokumentiert im Security Guide; Abschnitt Kommunikation, Dokumente und Daten.

Diesbezügliche Anfragen von Kunden werden intern zielgerichtet an die zuständigen Rollen weitergeleitet.

### 4.1.34 A.5.34 - Datenschutz und Schutz personenbezogener Daten (pbD)

>> Die Organisation sollte die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten nach den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen ermitteln und erfüllen.

Ein betrieblicher Datenschutzbeauftragter ist bestellt, der auf die Einhaltung der relevanten Datenschutzgesetze hinwirkt. Dieser kann auf den internen Syndikus oder einen externen RA für IT-Recht zurückgreifen. Aus- und Weiterbildungsmaßnahmen zu diesen Themen und der Sicherstellung der Awareness sind für die Mitarbeitende eingerichtet. Für extern kann ein Kontakt über unser Trust Center hergestellt werden (https://www.aeb.com/de/trust-center/datenschutz.php).

In Prüf-Prozessen (etwa zu Applications oder im Verfahrensverzeichnis) sind Fragen nach der Rechtsgrundlage, Zulässigkeit und Angemessenheit integriert.

Ein regelmäßig überarbeitetes Sicherheitskonzept beinhaltet technische und organisatorische Maßnahmen, um auf Stand der Technik auch personenbezogene Daten zu schützen.

### 4.1.35 A.5.35 - Unabhängige Überprüfung der Informationssicherheit

>> Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung einschließlich der Mitarbeiter, Prozesse und Technologien, sollten auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft werden.

Dazu unterziehen wir unser ISMS einer regelmäßigen externen ISO-Zertifikatsüberprüfung nach ISO 27001.

Weitere Prüfungen durch Dritte werden vorgenommen etwa zur Überprüfung der Datensicherheit für unser Datenschutzmanagementsystem. Teilweise können auch die Prüfungen der technischen und

organisatorischen Maßnahmen (TOMs) gemäß Art. 28 DS-GVO durch unsere Geschäftspartner im Zuge Prüfungen zur Auftragsverarbeitung mit gewertet werden.

Für den Cloud-Betrieb gilt zusätzlich: AEB bietet ihren Kunden vielfältige Informationen, um sich vom ordnungsgemäßen Betrieb zu überzeugen. AEB lässt sich von unabhängigen, akkreditierten Stellen auditieren und stellt geeignete Belege wie Zertifikate zur Verfügung.

### 4.1.36 A.5.36 - Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit

>> Die Einhaltung der Informationssicherheitspolitik der Organisation, der themenspezifischen Richtlinien, Regeln und Normen sollte regelmäßig überprüft werden.

Dazu existiert bei AEB ein mehrstufiges Konzept:

- permanente Verantwortung und Prüfung durch Rollen aus Security- und Compliance-Umfeld
- regelmäßige Austausch-Runden u.a. im IS-Board, Compliance-Umfeld. Dabei sind auch Neuerungen im Umfeld Security-Vorgaben Thema.
- dabei Pflege einer dokumentierten Übersicht relevanter, ggf. auch potenzieller Vorgaben
- regelmäßige interne Audits; mit Gegenprüfung der relevanten Sicherheitsrichtlinien und Stichproben-Tests, Hausrundgängen
- regelmäßige Trainings zur Erinnerung und Auffrischung
- Projekt- und Ticket-getriebene Sicherstellung, dass die nötigen Aktivitäten laufen
- strategische Meetings des Arbeitskreises Security
- mindestens jährliches Review zum Bestand der Vorgaben durch den Verantwortlichen des Verwaltungsrats.
- sollte sich im Einzelfall herausstellen, dass eine Vorgabe nicht erkannt worden ist, wird entsprechend zeitnah nachgebessert

Zudem nutzen wir zur Überprüfung der Einhaltung u.a. von technischen Vorgaben mehrere Situationen:

- regelmäßige Tests im Rahmen des Change Managements durch IT-Operations
- neue Applications werden einem Freigabeprozess unterworfen
- permanente Verantwortung und Prüfung durch die Verantwortlichen der Leitlinien und die Rolle des Domänen Sicherheitsbeauftragten
- regelmäßige Überprüfung aus Datenschutz-Sicht durch den Datenschutzbeauftragten
- regelmäßige interne Audits zur ISO 27001; mit Gegenprüfung der relevanten Sicherheitsrichtlinien
- regelmäßige externe Audits
- regelmäßige Durchführung von Pentests durch externe Dienstleister
- regelmäßige Termine im Security-Netzwerk des Arbeitskreises Security

- regelmäßige Kontrolle und Pflege der Controls

### 4.1.37 A.5.37 - Dokumentierte Betriebsabläufe

>> Die Betriebsverfahren für Informationsverarbeitungsanlagen sollten dokumentiert und dem Personal, das sie benötigt, zur Verfügung gestellt werden.

Alle Änderungen unterliegen und werden durch Change Prozesse gesteuert. Sie sind in internen Guides (z.B. im Change Management Prozess, im Admin Guide oder im Security Guide) dokumentiert.

## 4.2 A.6 - Personenbezogene Maßnahmen

### 4.2.1 A.6.1 - Sicherheitsüberprüfung

>> Alle Personen, die in die Belegschaft aufgenommen werden, sollten vor dem Eintritt in die Organisation und fortlaufend unter Berücksichtigung geltender Gesetze, Vorschriften und ethischer Grundsätze einer Sicherheitsüberprüfung unterzogen werden und in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken stehen.

Alle Personen, die sich um eine Beschäftigung bewerben, werden einer Sicherheitsüberprüfung unterzogen, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist.

### 4.2.2 A.6.2 - Beschäftigungs- und Vertragsbedingungen

>> In den arbeitsvertraglichen Vereinbarungen sollten die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt werden.

Mitarbeitende sowie Partner unterzeichnen bei Vertragsbeginn Standardverträge mit entsprechender Verpflichtung zur Geheimhaltung, auch in der Datenverarbeitung. Die Übertragung von Verantwortungen ist intern fest an ein Rollenkonzept geknüpft und wird über die Zuweisung der Rollen geprüft und dokumentiert.

### 4.2.3 A.6.3 - Informationssicherheitsbewusstsein, -ausbildung und -schulung

>> Das Personal der Organisation und relevante interessierte Parteien sollten ein angemessenes Bewusstsein für die Informationssicherheit, eine entsprechende Ausbildung und Schulung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, die für ihr berufliches Arbeitsgebiet relevant sind.

Neue Mitarbeitende müssen festgelegte, sicherheitsrelevante Inhalte erlernen. Des Weiteren gibt es regelmäßige Sicherheitskampagnen, Veröffentlichungen und Schulungen für alle Mitarbeitenden. Diese werden aktiv kommuniziert und dabei an bestehende Regelungen zur Einhaltung von Sicherheitspflichten erinnert, sowie über Neuerungen und Änderungen informiert.

Für Cloud-Betrieb gilt zusätzlich: AEB monitort IT-Sicherheitsvorfälle und Datenpannen. Die Mitarbeitenden werden regelmäßig über das Vorgehen bei Sicherheitsvorfällen und Datenpannen sowie über die Bedeutung und mögliche Konsequenzen von Verstößen informiert.

### 4.2.4 A.6.4 - Maßregelungsprozess

>> Ein Maßregelungsprozess sollte formalisiert und kommuniziert werden, um Maßnahmen gegen Mitarbeiter und andere interessierte Parteien zu ergreifen, die einen Verstoß gegen die Informationssicherheitspolitik begangen haben.

Der Maßregelungsprozess ist implementiert und dokumentiert.

### 4.2.5 A.6.5 - Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

>> Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sollten festgelegt, durchgesetzt und den betreffenden Mitarbeitern und anderen interessierten Parteien mitgeteilt werden.

Durch die Personalverwaltungssoftware werden beim Austritt von Mitarbeitenden oder Änderung der Beschäftigung automatisch die zu erledigenden Aufgaben bezüglich der Informationssicherheit angelegt und deren Erfüllung überwacht.

### 4.2.6 A.6.6 - Vertraulichkeits- oder Geheimhaltungsvereinbarungen

>> Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, sollten identifiziert, dokumentiert, regelmäßig überprüft und von den Mitarbeitern und anderen interessierten Parteien unterzeichnet werden.

Vereinbarungen zur Geheimhaltung liegen vor sowohl für den internen als auch für den externen Einsatz.

Die Inhalte werden von Verantwortlichen (aus Recht, Datenschutz und Personal) verantwortet und regelmäßig gepflegt.

Quelle für Änderungen können sein u.a.: Audits, Gesetzgebung, Bedarfe im Austausch mit den Geschäftspartnern (Lieferanten, Kunden), Änderungen im Bestand schutzbedürftiger Werte.

Regelmäßiger Austausch im Umfeld Recht, ISMS und Datenschutz stellt die Beschäftigung mit den Vereinbarungen sicher.

Für den Cloud-Betrieb gilt zusätzlich: siehe auch ISO27018 A.10.1 - Vertraulichkeits- oder Geheimhaltungsvereinbarungen (Mitarbeitende der AEB werden im Rahmen ihres Arbeitsvertrags auf Geheimhaltung verpflichtet und hierzu regelmäßig geschult.)

### 4.2.7 A.6.7 - Telearbeit

>> Es sollten Sicherheitsmaßnahmen ergriffen werden, wenn Mitarbeiter extern arbeiten, um Informationen zu schützen, die außerhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.

Telearbeit (HomeOffice / Mobiles arbeiten) ist bei AEB grundsätzlich zugelassen. Sicherheitsmaßnahmen finden sowohl technisch als auch organisatorisch statt. Eine Freigabe erfolgt prozessgesteuert. Eine entsprechende Richtlinie ist etabliert.

### 4.2.8 A.6.8 - Meldung von Informationssicherheitsereignissen

>> Die Organisation sollte einen Mechanismus bereitstellen, der es den Mitarbeitern ermöglicht, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit über geeignete Kanäle rechtzeitig zu melden.

AEB hat Prozesse für Sicherheitsvorfälle implementiert, die sicherstellen, dass Informationssicherheitsereignisse so schnell wie möglich über geeignete, bekannte Kanäle zu deren Handhabung gemeldet und bearbeitet werden.

Dies umfasst sowohl Prozesse für den Regelbetrieb (z.B. den Prozess Security Event Management) als auch für Ausnahmesituationen (Prozess Security Incident Management, aber auch Prozesse im Emergency Guide sowie im Business Continuity Management (BCM) oder zu Datenpannen im Datenschutz-Bereich).

Mitarbeitende und Auftragnehmer, welche die Informationssysteme und -dienste der Organisation nutzen, werden angehalten, jegliche beobachteten oder vermuteten Schwächen in der Informationssicherheit in Systemen oder Diensten festzuhalten und zu melden. Dies geschieht in einem Ticketing System.

Mitarbeitende werden im internen Security Guide und in entsprechenden Schulungen auf die Mitwirkungspflicht hingewiesen.

Kunden können sich mit allen Sicherheitsanliegen und -meldungen an den AEB Support auf den ihnen jeweils zur Verfügung stehenden Kanälen wenden. Von hier werden erste Reaktionen aber auch Eskalationen ausgesteuert.

AEB meldet sich bei festgestellten eigenen Sicherheitsvorfällen umgehend bei den betroffenen Kunden.

## 4.3 A.7 - Physische Maßnahmen

### 4.3.1 A.7.1 - Physische Sicherheitsperimeter

>> Zum Schutz von Bereichen, in denen sich andere zugehörige Werte befinden, sollten Sicherheitsperimeter festgelegt und verwendet werden.

Die AEB Gebäude sind in Bereiche aufgeteilt. Es gibt

- öffentliche Bereiche
- private Bereiche
- besonders geschützte Bereiche.

Je nach Bereich gibt es unterschiedliche berechtigte Personenkreise und entsprechende Sicherheitsvorkehrungen wie z.B. protokollierte Zutritte, Videoüberwachung oder Alarmierung.

Weitere Dokumentation finden sich unter anderem in dem im Trust Center hinterlegten Dokument zu Zutritt, Zugriff und Zugang.

### 4.3.2 A.7.2 - Physischer Zutritt

>> Sicherheitsbereiche sollten durch eine angemessene Zutrittssteuerung und Zutrittsstellen geschützt werden.

Für den Hauptsitz Stuttgart (Rechenzentrum) gilt:

- Es gibt drei Bereiche: öffentlicher Bereich, private Bereich und besonders geschützte Bereich. Alle Zugänge sind gesichert durch Schlösser mit Transponder
- Die Ausgabe und Rücknahme von Transpondern wird dokumentiert
- Mitarbeitende werden im Zuge des Security Guide auf den Umgang mit Gästen unterwiesen
- Alle öffentlichen Zugänge, Liefer- und Ladebereiche befinden sich außerhalb der Sicherheitszonen. Die Anlieferungen in Sicherheitszonen erfolgen ausschließlich unter Aufsicht.

Für andere Standorte gelten gesonderte Regelungen zu Sicherheitsmaßnahmen am Standort, die den AEB Standard nicht unterschreiten. Regelungen stehen auch im Security Guide.

### 4.3.3 A.7.3 - Sichern von Büros, Räumen und Einrichtungen

>> Die physische Sicherheit für Büros, Räume und Einrichtungen sollte konzipiert und umgesetzt werden.

Büros werden durch Absicherungsvorkehrungen an Gebäudekomplex geschützt, dazu gehören:

Für den Hauptsitz Stuttgart (Rechenzentrum) gilt:

- Abschließbare Zugänge (Personalisierte Transponder)
- Videoüberwachung
- Sicherheitsdienst

Für weitere Standorte gelten gesonderte Regelungen zu Sicherheitsmaßnahmen am Standort, die den AEB Standard zum Security Guide nicht unterschreiten.

Datacenter

Datacenter, IT-Einrichtungen (Providerraum, Unterverteiler, etc.) werden durch Absicherungsvorkehrungen an Gebäudekomplex geschützt, dazu gehören.

Für Stuttgart gilt:

- Abschließbare Zugänge (Personalisierte Transponder)
- Videoüberwachung
- Sicherheitsdienst
- Personalisiert PINs (Zugang zu DataCenter)

### 4.3.4 A.7.4 - Physische Sicherheitsüberwachung

>> Die Räumlichkeiten sollten ständig auf unbefugten physischen Zugang überwacht werden.

Die Räumlichkeiten sind ständig auf unbefugten physischen Zugang überwacht

Für den Hauptsitz Stuttgart (Rechenzentrum) gilt:

- Videoaufzeichnung
- Sicherheitsdienst

Für weitere Standorte gelten gesonderte Regelungen zu Sicherheitsmaßnahmen am Standort, die den AEB Standard zum Security Guide nicht unterschreiten.

### 4.3.5 A.7.5 - Schutz vor physischen und umweltbedingten Bedrohungen

>> Der Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen physischen Bedrohungen der Infrastruktur sollte geplant und umgesetzt werden.

Für den Standort Stuttgart gilt:

- Brandmeldeanlage, Sprinkleranlage, Notstromversorgung, Schließanlage, Sicherheitsdienst
- E-Check und weitere Prüfungen nach Vorgaben der Berufsgenossenschaft

- Es gibt weitere interne Dokumentationen zum Wach- und Schließdienst sowie zur Videoüberwachung.

Andere Arbeitsorte erfüllen den Standard zu Sicherheitsmaßnahmen am Standort.

Für die Datacenter gilt:

- Brandmeldeanlage und Brandfrüherkennung,
- Selbsttätige Löschanlage
- Einbruchmeldeanlage und 24x7 Sicherheitsdienst
- Wassermeldeanlage
- Videoüberwachung

### 4.3.6 A.7.6 - Arbeiten in Sicherheitsbereichen

>> Es sollten Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen konzipiert und umgesetzt werden.

- Eigenes Personal wurde für das Arbeiten in Sicherheitszonen über die Richtlinien und Verhaltensregeln für normalen Betrieb, als auch für den Betrieb in Ausnahmensituationen unterwiesen.
- Fremdpersonal ist nur befugt, Arbeiten in Sicherheitszonen nach Anmeldung und Genehmigung sowie unter Aufsicht durchzuführen.
- Es gelten die Vorgaben des Security Guides für Sicherheitsbereiche sowie die Regelungen zur Zutrittskontrolle

### 4.3.7 A.7.7 - Aufgeräumte Arbeitsumgebung und Bildschirmsperren

>> Es sollten klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und klare Regeln für Bildschirmsperren für informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.

(siehe u.a. A.8.1 - Endpunktgeräte des Benutzers), und es wird das Prinzip von Clean- u. Clear-Desk Policy gelebt und schon in der Grundausbildung geschult und vermittelt.

### 4.3.8 A.7.8 - Platzierung und Schutz von Geräten und Betriebsmitteln

>> Die Geräte und Betriebsmittel sollten sicher und geschützt aufgestellt werden.

Dies ist durch die baulichen Maßnahmen der Infrastruktur und der Gebäudekonzeption gegeben. Regelmäßige Hausrundgänge dienen der weiteren Sicherstellung.

### 4.3.9 A.7.9 - Sicherheit von Werten außerhalb der Räumlichkeiten

>> Werte außerhalb des Standorts sollten geschützt werden.

Geräte sind grundsätzlich durch Passwörter, PIN, o.ä. gesichert. Festplatten in Notebooks und PCs sind grundsätzlich verschlüsselt.

### 4.3.10 A.7.10 - Speichermedien

>> Speichermedien sollten während ihres gesamten Lebenszyklus - Erwerb, Verwendung, Transport und Entsorgung - in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.

Der Umgang mit Wechselmedien ist im internen Security Guide festgelegt:

- Daten bleiben wann immer möglich in ihrem Kontext und werden nicht auf mobile Datenträger kopiert.
- Sollten doch Daten auf mobile Datenträger verbracht/gespeichert werden müssen, dann gilt:
  Daten, die auf mobile Datenträger abgelegt werden (insbesondere diejenigen, die interne, vertrauliche oder streng vertrauliche Informationen beinhalten), müssen durch entsprechende Techniken (z.B. Bitlocker) verschlüsselt und gesichert werden.
- Dies gilt insbesondere für Datenträger, die für den Transport vorgesehen sind (z.B. Bandsicherungen).
- Für diese Datenträger existiert ein zusätzlicher Prozess, der dies sicherstellt.

Datenträger werden sicher vernichtet:
Ein Vertragspartner sammelt sie ein, vernichtet sie sicher und zertifiziert dies und den gesamten Prozess gegenüber AEB.

Die Vernichtung ist in der DIN 66399 beschrieben:

- Schutzklasse: 2 (=hoher Schutzbedarf für vertrauliche Daten) (DIN 66399-1)
- Securitylevel: für Festplatten u.ä.: H-4 (DIN 66399-2)

Die Vernichtung wird jeweils durch ein Zertifikat bestätigt.

### 4.3.11 A.7.11 - Versorgungseinrichtungen

>> Informationsverarbeitungseinrichtungen sollten vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt werden.

Der Hauptsitz Stuttgart (Rechenzentrum) verfügt über

- eine moderne, zertifizierte und abgenommene Elektroinstallation
- Elektroinstallation mit Überspannungsschutz und Energieverteilung pro Bereich

- gespiegelte USV-Anlage 230/400V (A-B Konfiguration)
- Netzersatzanlage (Diesel-Generator) für autonomen Betrieb
- Das beim Bau umgesetzte Energiekonzept ermöglicht es, teilweise autark ohne externe Energie / Stromversorgung zu arbeiten (Photovoltaik Anlage, DC Wärmerückgewinnung über Wärmepumpe, Freiluftkühlung, Sprinklertank)
- Alle Anlagen werden vom VdS turnusmäßig abgenommen

Die nationalen AEB Standorte verfügen über

- USV gesicherte Netzwerkinfrastruktur
- Provideranbindungen über je zwei Glasfaseranbindungen und separater Übertragungstechnik.

### 4.3.12 A.7.12 - Sicherheit der Verkabelung

>> Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, sollten vor Unterbrechung, Störung oder Beschädigung geschützt werden.

Für den Hauptsitz Stuttgart (Rechenzentrum) gilt:

- Separate Kabelführungen für Strom u. Datenleitungen
- Strukturierte Cat. 7 Verkabelung und Glasfaser
- Datenleitungsarten gekennzeichnet durch unterschiedliche Farben der Kabel und Beschriftung
- Dokumentation der Switch-Ports und Kabelverläufe
- Redundante Anbindung aller wichtigen Komponenten
- Strukturierte Cat. 7 Verkabelung und Glasfaser
- WiFi 6
- baurechtliche Vorgaben für Neubau mit Stand 2015-2017
- Elektrorevision nach VdS (jährliche Prüfung) und DGUV V3 des Errichters
- computergesteuertes Überwachungssystem der Verbindungen
- Elektrorevision nach VdS (jährliche Prüfung) und DGUV V3 des Errichters

Für nationale AEB Standorte

- Strukturierte Cat. 7 Verkabelung und Glasfaser
- Separater "Netzwerkschrank" für Anbindung und Netzwerk in eigener AEB Fläche
- Dokumentation der Switch-Ports
- computergesteuertes Überwachungssystem der Verbindungen

### 4.3.13 A.7.13 - Instandhaltung von Geräten und Betriebsmitteln

>> Geräte und Betriebsmittel sollten ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.

- E-Check aller ortsveränderlichen und ortsfesten Geräte
- regelmäßige Wartung und Funktionsprüfung
- Wartungsverträge
- Regelmäßige (min. Jährliche Überprüfung der Anlagen (USV, Klima, etc.)
- regelmäßige Wartung und Funktionsprüfung
- Wartungsverträge
- turnusmäßiger Austausch der Infrastruktur

### 4.3.14 A.7.14 - Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

>> Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, sollten überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.

Papier, Discs und andere Geräte mit Daten darauf werden sicher vernichtet. Die Entsorgung von Datenträgern ist so gestaltet, dass davon ausgegangen wird, es seien personenbezogene Daten enthalten:

Ein Partner sammelt sie ein, vernichtet sie sicher (vor Ort) und AEB lässt sich dies, wie den gesamten Prozess, zertifizieren.

Die Vernichtung ist in der DIN 66399 beschrieben:

- Schutzklasse: 2 (=hoher Schutzbedarf für vertrauliche Daten) (DIN 66399-1)
- Securitylevel
  - für Festplatten u.ä.: H-4 (DIN 66399-2)
  - für Papier: P-4 (DIN 66399-2)

Dies gilt auch für den Cloud-Betrieb.

## 4.4 A.8 - Technologische Maßnahmen

### 4.4.1 A.8.1 - Endpunktgeräte des Benutzers

>> Informationen, die auf Endpunktgeräten der Benutzer gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, sollten geschützt werden.

AEB erlaubt Zugriffe auf Daten, Anwendungen und Netze der AEB durch Geräte von Mitarbeitenden nur für

- Firmennotebooks die entsprechend gesichert sind
- Andere mobile Devices, die durch eine Enterprise Mobility Management (EMM) Lösung zentral durch AEB administriert und gesichert werden.

Dies umfassen umfasst unter anderem Techniken wie conditional access, MDM oder MAM. AEB erzwingt so zum einen die relevanten Sicherheitsmerkmale und stellt andererseits auch sicher, dass private Daten/Anwendungen nicht mit AEB Daten vermischt werden.

Eine entsprechende Richtlinie für BYOD ist implementiert und wird technisch durchgesetzt.

### 4.4.2 A.8.2 - Privilegierte Zugangsrechte

>> Zuteilung und Gebrauch von privilegierten Zugangsrechten sollte eingeschränkt und verwaltet werden.

Anwender mit besonderen administrativen oder privilegierten Rechten sind in geeigneten Rollengruppen zusammengefasst und unterliegen den entsprechenden Prozessen und Freigaben.

Der/Die Verantwortliche für diese Rollen ist üblicherweise der/die IT Leiter, der/die IT-Security Manager oder die Geschäftsleitung.

Für besonders privilegierte Rechte (z.B. Firewall-Zugriff, Admin Portale, etc.) muss der/die Anwender*in ein besonderes personalisiertes Administrator-Konto nutzen, sein „normales“ User-Konto bekommt diese Rechte nicht / kann nicht den entsprechenden Rollen zugeordnet werden.

### 4.4.3 A.8.3 - Informationszugangsbeschränkung

>> Der Zugang zu Informationen und anderen zugehörigen Werten sollte in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.

Die Zugangssteuerung wird über rollenbasierte Gruppen und entsprechende Gruppenzugehörigkeiten festgelegt und eingeschränkt. Die benötigten Rechte werden über die jeweiligen Rollen zugeteilt. Grundlegend gilt:

- Need-to-Know-Prinzip
- So viel Zugriff wie nötig, so wenig wie möglich

Sowohl die Richtlinie, das Einhalten der Zugangssteuerung, als auch die Rollen und deren Rechte werden regelmäßig mindestens einmal pro Jahr überprüft.

Für den Cloud-Betrieb gilt zusätzlich: AEB stellt sicher, dass bei der (Neu-)Vergabe von Speicherplatz dieser nicht mit Altdaten versehen ist. Anwender greifen in AEB-Anwendungen nicht direkt auf den Speicher zu, sondern ausschließlich auf per Datenbank bereitgestellte Informationen.

### 4.4.4 A.8.4 - Zugriff auf den Quellcode

>> Der Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken sollte angemessen verwaltet werden.

Der Zugang ist nur für die an der Entwicklung beteiligten Mitarbeiter*innen möglich, dies wird durch eine im Identity-Management integrierte, rollenbasierte, Zugangssteuerung sichergestellt.

### 4.4.5 A.8.5 - Sichere Authentifizierung

>> Sichere Authentifizierungstechnologien und -verfahren sollten auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung implementiert werden.

Der Zugang zu Systemen und Anwendungen wird stets durch ein sicheres Anmeldeverfahren gesteuert. Wo immer möglich wird ein zweiter Faktor erzwungen.

Diese Regelungen gelten einheitlich für folgende Konten-Arten: Mitarbeitende, Kunden und Dienste

Passwörter bei der AEB müssen folgende Kriterien erfüllen:

- Mindestens 11 Zeichen insgesamt

Zusätzlich müssen mindestens drei der vier Punkte erfüllt sein:

- Mindestens ein Großbuchstabe
- Mindestens ein Kleinbuchstabe
- Mindestens eine Zahl
- Mindestens ein Sonderzeichen (Nicht alphanumerische Zeichen)

Rotation:

- AEB folgt für die internen Konten den Erkenntnissen aktueller Sicherheitsforschung und sieht keine Passwortrotation für die Mitarbeiter*innen vor.
- In der AEB Plattform ist keine Passwortrotation vorgesehen.
- In allen anderen Anwendungen entscheiden die Kunden selbst über den Einsatz von Passwort Rotation. Beide Varianten sind möglich, aber AEB empfiehlt auf eine Passwortrotation zu verzichten.

Für privilegierte Konten gelten andere Regeln (SSH Keys Passphrase zählt mit dazu):

- Passwörter haben mindestens 14 (vierzehn) Zeichen

Passwörter müssen mindestens drei der folgenden vier Punkte erfüllen:

- Mindestens ein Großbuchstabe
- Mindestens ein Kleinbuchstabe
- Mindestens eine Zahl
- Mindestens ein Sonderzeichen (Nicht alphanumerische Zeichen)

Besonders zu beachten ist, dass die letzten 24 Kennwörter nicht wieder verwendet werden dürfen.

Dies gilt auch für den Cloud-Betrieb.

### 4.4.6 A.8.6 - Kapazitätensteuerung

>> Die Nutzung von Ressourcen sollte überwacht und entsprechend den aktuellen und erwarteten Kapazitätsanforderungen angepasst werden.

Alle Ressourcen (IT-Infrastruktur, wie Netzwerk) werden durch eine proaktive Überwachung 24/7 geprüft. Vorhersagen von System-Auslastungen und Auslastungs-Tendenzen werden über entsprechende Tools und Grafiken dargestellt und analysiert.

Planung von neuen Systemen, Systemerweiterungen und Leitungsupgrades werden im Rahmen von Projekten und in einem gesteuerten Change Management durchgeführt, woraus wiederum entsprechende Maßnahmen zur Kapazitätserweiterung entstehen.

Grundsätzlich wird mit einem, der Dynamik der letzten Jahre angemessenen und den Prognosen über die weitere Entwicklung angepasstem, vorausschauenden Puffer geplant.

### 4.4.7 A.8.7 - Schutz gegen Schadsoftware

>> Schutz gegen Schadsoftware sollte umgesetzt und durch angemessene Sensibilisierung der Benutzer unterstützt werden.

Die AEB setzt auf ein mehrstufiges Malware-Schutzkonzept:

Neben gängigen Betriebssystem Security Policies und Cloud Provider Schutzmaßnahmen ist auf allen internen AEB Clients eine aktuelle Next-Generation-Antimalware Software installiert, die u.a. das Verhalten von Prozessen überwacht und potenziell schädliche Aktivitäten unterbindet und zur weiteren Untersuchung meldet. Auf den Servern, die von der AEB betrieben werden, ist ebenfalls aktuelle Anti-Malware Software aktiv. Zusätzlich gibt es Netzwerk-Segmentierung mit Next-Generation-Firewalls dazwischen, die mit diversen Threat Prevention Features für zusätzliche Sicherheit sorgen.

Begleitend gibt es auch eine entsprechende interne Richtlinie für Mitarbeitende und Administratoren zum Umgang mit Malware.

### 4.4.8 A.8.8 - Handhabung von technischen Schwachstellen

>> Es sollten Informationen über technische Schwachstellen verwendeter Informationssysteme eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen werden.

Für die Information über technische Schwachstellen und deren Behandlung ist ein Schwachstellen Management Prozess etabliert. Dadurch ist sichergestellt, dass diese Informationen rechtzeitig eingeholt werden, die Gefährdung der Organisation durch derartige Schwachstellen bewertet werden und angemessene Maßnahmen ergriffen werden, um das dazugehörige Risiko zu behandeln.

So gilt unter anderem

- Für alle Geräte und auf ihnen laufenden Anwendungen ist eine kontinuierliche Schwachstellenüberwachung implementiert.
- Für Anwendungen werden zusätzlich regelmäßige Sicherheitsüberprüfungen in Form von gezielten Schwachstellenscans (mindestens einmal monatlich) und Penetrationstests (mindestens dreimal jährlich) durchgeführt.
- Schwachstellen sind gemäß ihrer Kritikalität u.a. basierend auf dem Common Vulnerability Scoring System (CVSS) klassifiziert.
- "Critical"-Schwachstellen werden umgehend, als „High“- klassifizierte binnen 4 Wochen behoben. Wobei eine Behebung eine komplette Beseitigung der Schwachstelle oder eine Mitigierung in die nächstniedrigere Stufe bedeutet.
- Alle übrigen Schwachstellen werden im Zuge geplanter Wartungsarbeiten adressiert.
- Kunden werden unverzüglich über als „high“ und „critical“ klassifizierte Schwachstellen informiert, sofern diese nicht in der angegebenen Zeit behoben werden können.

### 4.4.9 A.8.9 - Konfigurationsmanagement

>> Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken sollten festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.

AEB hat für alle relevanten Systeme und Hardwaren Richtlinien und Anleitungen zur sicheren Konfiguration festgelegt. Diese werden sowohl regelmäßig als auch bei Erkenntnissen oder größeren Veränderungen geprüft und ggf. angepasst.

Die ordnungsgemäße Konfiguration und das Einhaltung der Richtlinien wird automatisiert überwacht.

### 4.4.10 A.8.10 - Löschung von Informationen

>> Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, sollten gelöscht werden, wenn sie nicht mehr benötigt werden.

Daten / Informationen werden gemäß dem Sicherheitsstandard (ISO/IEC 27002) und gesetzlichen Vorgaben, sobald sie nicht mehr benötigt werden, nachhaltig gelöscht.

### 4.4.11 A.8.11 - Datenmaskierung

>> Die Datenmaskierung sollte in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugangssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden Rechtsvorschriften eingesetzt werden.

Auf der Grundlage der gesetzlichen, behördlichen und vertraglichen Anforderungen und der Risikobewertung hat AEB ein Informationsklassifizierungsschema umgesetzt. Dieses stellt sicher, dass Daten und Informationen entsprechend ihrem Schutzbedarf behandelt werden.

Interne Audits prüfen regelmäßig das Einhalten der entsprechenden Regelungen und den korrekten Umgang mit den Daten und Informationen.

### 4.4.12 A.8.12 - Verhinderung von Datenlecks

>> Maßnahmen zur Verhinderung von Datenlecks sollten auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.

Um Datenlecks zu verhindern sind unter anderem die folgenden Maßnahmen implementiert:

- Klassifizierung von Informationen (siehe auch Control A.5.12)
- Zugriffskontrollen (siehe auch Control A.5.18)
- Regelungen und Technische Maßnahmen zur Steuerung der Informationsübertragung (siehe auch Control A.5.14)
- Manuelles und automatisches Blockieren von Konten, Benutzeraktivitäten oder Übertragungen ganz generell bei ungewöhnlichem Verhalten
- Verschlüsslung von Data at Rest

### 4.4.13 A.8.13 - Sicherung von Information

>> Sicherungskopien von Informationen, Software und Systemen sollten in Übereinstimmung mit den vereinbarten themenspezifischen Richtlinien für Datensicherungen aufbewahrt und regelmäßig geprüft werden.

Sicherungen von Information, Software und Systemabbildern erfolgen über ein mehrstufiges Konzept spätestens alle 24h. Neben einer lokalen Sicherung auf Disk stehen entsprechende verschlüsselte Datenträger an einer sicheren, entfernten Location bereit.

Die Sicherungen werden regelmäßig, stichprobenartig mindestens einmal pro Monat, getestet. Ein Full Restore Test/DR Test findet mindestens jährlich statt.

Mehr Details zum Backupkonzept finden sich im Dokument "Auszug aus dem AEB Security Konzept: Details zum Backup", das im Trust Center der AEB bereit steht.

Für den Cloud-Betrieb gilt zusätzlich: Mehr Details finden sich in der Servicebeschreibung (AEB Cloud oder AEB Private Cloud) und in weiteren Dokumenten im AEB Trust Center.

### 4.4.14 A.8.14 - Redundanz von informationsverarbeitenden Einrichtungen

>> Informationsverarbeitende Einrichtungen sollten mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen realisiert werden.

Informationsverarbeitende Einrichtungen werden immer auch mit Hinblick auf Einhaltung der Verfügbarkeitsanforderungen realisiert. Verfügbarkeit ist ein wesentliches Sicherheitskriterium.

- AEB legt alle relevanten Systeme (mehrfach) redundant aus.
- AEB hat entsprechende Prozesse etabliert, die sowohl die regelmäßige Überprüfung als auch in besonderen Situationen die Verfügbarkeit sicherstellen.

### 4.4.15 A.8.15 - Protokollierung

>> Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, sollten erstellt, gespeichert, geschützt und analysiert werden.

Monitoring, Alerting und Protokollierung sowie das Einrichten und Betreiben der Protokollierung der Tätigkeiten von Systemadministratoren und Systembedienern wird gesteuert durchgeführt. Sie sind im Applikationsmanagement verankert. Die dazu gehörenden Richtlinien sind von AEB dazu im internen Admin Guide und im Logging und Monitoring Konzept festgelegt.

Die Zugriffsrechte auf die Protokollinformationen sind beschränkt und vor unbefugtem Zugriff oder Manipulation geschützt.

Protokoll-Informationen werden nur zu beauftragten Zwecken und dazu befugten Mitarbeitenden genutzt. Die Daten werden regelmäßig nach Ablauf von angemessenen und dokumentierten Fristen gelöscht.

Entsprechende Loginformationen stehen für 30 Tage zur Verfügung.

Für den Cloud-Betrieb gilt zusätzlich: AEB bietet ihren Kunden administrative Möglichkeiten, ihre relevanten Logdaten selbst auszulesen. Die Regelmäßigkeit und Tiefe der Prüfung liegt dabei in der Verantwortung des Kunden.

### 4.4.16 A.8.16 - Überwachung von Aktivitäten

>> Netzwerke, Systeme und Anwendungen sollten auf anormales Verhalten überwacht und geeignete Maßnahmen ergriffen werden, um potentielle Informationssicherheitsvorfälle zu bewerten.

Verdächtige Ereignisse werden automatisiert verarbeitet sowie den verantwortlichen Mitarbeitenden gemeldet, um die Netzwerk- und Betriebsintegrität so aufrecht zu erhalten, dass die Geschäftskontinuität gewahrt bleibt. (Siehe Control A.5.25 für den Umgang damit) Sie helfen außerdem unter anderem die folgenden Prozesse zu verbessern: Auditing, Sicherheits- und Risikobewertung, Vulnerability Management, Netzwerk Performance, Capacity Management, ...

Dies passiert durch zentrales Logging und Monitoring. Unterstützt von Intrusion Prevention und Detection Systemen sowie weiteren dedizierten Threat-Intelligence-System

Die Überwachung passiert im Einklang mit allen behördlichen Anforderungen sowie der geltenden Gesetzgebung und alle Aufzeichnungen werden im Einklang mit den Aufbewahrungsrichtlinien der AEB aufbewahrt (Siehe dazu den internen Admin Guide).

### 4.4.17 A.8.17 - Uhrensynchronisation

>> Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme sollten mit zugelassenen Zeitquellen synchronisiert werden.

Die Uhren aller relevanten informationsverarbeitenden Systeme werden mit einer einzigen Referenzzeitquelle per NTP synchronisiert.

### 4.4.18 A.8.18 - Gebrauch von Hilfsprogrammen mit privilegierten Rechten

>> Der Gebrauch von Hilfsprogrammen, die fähig sein können, System- und Anwendungsschutzmaßnahmen zu umgehen, sollte eingeschränkt und streng überwacht werden.

Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und streng überwacht.

Technische Unterstützung bieten dabei unter anderem:

- Überprüfung und Analyse von installierten oder genutzten Softwaren
- Next Generation Firewalls mit IDS/IPS, die auch den Zugriff über interne Netzwerkzonen hinweg überwachen und entsprechend eingreifen
- (Next Generation) Malwareprotection Mechanismen. Diese verhindern jeweils lokal die Ausführung solcher Tools.

Zusätzlich ist organisatorisch ein Applikationsmanagement Prozess im Einsatz, der festlegt welche Tools von der AEB freigegeben sind. Security und Datenschutz sind integrale Bestandteile des Prozesses.

### 4.4.19 A.8.19 - Installation von Software auf Systemen im Betrieb

>> Es sollten Verfahren und Maßnahmen umgesetzt werden, um die Installation von Software auf Betriebssystemen sicher zu verwalten.

Ein strukturiertes Applikationsmanagement für alle Business relevanten Software, Hardware und Cloud Lösungen ist im Einsatz.

Entsprechende Prozesse und Richtlinien sind implementiert, kommuniziert und werden regelmäßig geschult und überprüft.

Darauf wird im internen Security Guide und im Admin Guide hingewiesen. Hier sind auch Hinweise zur Verwendung erlaubter Software samt Hinweisen zu verbotener Software sowie entsprechende Richtlinien zur Sicheren Installation und Konfiguration von Anwendungen.

Die Vermittlung dieser Pflichten ist auch Gegenstand des Onboardings für neue Mitarbeitende zu Informations- und Datensicherheit sowie des regelmäßigen Updates dazu.

### 4.4.20 A.8.20 - Netzwerksicherheit

>> Netzwerke und Netzwerkgeräte sollten gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.

AEB hat für Netzwerke ein mehrstufiges DMZ-Konzept sowie konsequentes, kleinteiliges "Zoning" etabliert. Übergänge zwischen den Zonen sind durch entsprechende Next Generation Firewalls auch mit IDS und IPS abgesichert. Die Netzwerke der AEB werden ausschließlich durch Mitarbeitende der AEB administriert.

### 4.4.21 A.8.21 - Sicherheit von Netzwerkdiensten

>> Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzwerkdienste sollten ermittelt, umgesetzt und überwacht werden.

Alle internen Netzwerke der AEB werden ausschließlich durch AEB Mitarbeitende administriert. Entsprechende Sicherheitsmechanismen und Rahmenbedingungen sind definiert, werden automatisiert überwacht und werden regelmäßig überprüft und ggf. angepasst.

Dort wo externe Netzwerke notwendig sind für die Erbringung der Services (z.B. Internet, Carrier) sind entsprechende Rahmenbedingungen in den Vereinbarungen mit den Externen festgelegt. Diese werden, wie die ganze Partnerschaft, überwacht und regelmäßig auditiert.

### 4.4.22 A.8.22 - Trennung von Netzwerken

>> Informationsdienste, Benutzer und Informationssysteme sollten in Netzwerken der Organisation gruppenweise voneinander getrennt gehalten werden.

AEB hat für Netzwerke ein mehrstufiges DMZ-Konzept sowie konsequentes, kleinteiliges "Zoning" etabliert. Übergänge zwischen den Zonen sind durch entsprechende Next Generation Firewalls auch mit IDS und IPS abgesichert.

### 4.4.23 A.8.23 - Webfilterung

>> Der Zugang zu externen Websites sollte verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.

Über Richtlinien und insbesondere über technische Maßnahmen stellt AEB sicher, dass Zugriffe auf extern Websites so eingeschränkt sind, dass Sicherheitsbedrohungen und Risiken für Daten der AEB verhindert werden.

Diese Richtlinien werden regelmäßig geprüft.

### 4.4.24 A.8.24 - Verwendung von Kryptographie

>> Es sollten Regeln für den wirksamen Einsatz von Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.

Richtlinien für den Gebrauch von kryptographischen Maßnahmen zum Schutz von Information sowie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln sind etabliert. Sie sind im internen Security Guide dokumentiert. Sie werden regelmäßig geschult und auf sie hingewiesen.

AEB informiert ihre Kunden über die eingesetzten Verschlüsselungsverfahren und möglichen Optionen.

### 4.4.25 A.8.25 - Lebenszyklus einer sicheren Entwicklung

>> Regeln für die sichere Entwicklung von Software und Systemen sollten festgelegt und angewendet werden.

Im Rahmen des Qualitätsmanagements ist die Berücksichtigung von Sicherheitsinteressen bei der Entwicklung und Pflege von Software und Systemen in Form von Prozessen und HowTos und im Security Guide geregelt und definiert. Diese sind in Entwicklungsguides und Kriterien für sicheres Coding umgesetzt. Für bestimmte Prozesse in der Softwareentwicklung sind Themenverantwortliche benannt.

### 4.4.26 A.8.26 - Anforderungen an die Anwendungssicherheit

>> Die Anforderungen an die Informationssicherheit sollten bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.

Im Rahmen des Qualitätsmanagements werden, Sicherheitsaspekte bei der Entwicklung und Wartung von Software und Systemen berücksichtigt. Dies wird durch Prozesse, Leitfäden und Anleitungen geregelt, die unter anderem im internen Security Guide und im Produktentwicklungs Guide festgelegt sind. Zu den Kernpunkten gehört die Anwendung sicherer Kodierungspraktiken. Entwickler müssen sichere Bibliotheken und Frameworks verwenden und Richtlinien befolgen, die darauf abzielen, gängige Schwachstellen zu vermeiden, um die Integrität und Sicherheit der Anwendungen zu gewährleisten.

Für die Beschaffung von Anwendungen ist ein Applikationsmanagement Prozess im Einsatz bei dem die Prüfung der Anforderungen von Security und Datenschutz sowie die Freigabe integrale Bestandteile des Prozesses sind.

Beispiele für die Prüfungen/Sicherstellungen umfassen neben einer allgemeinen Schutzbedarfsermittlung unter anderem:

- Authentifizierung und Zugriffskontrolle: Die Anwendungen müssen über Mechanismen zur Authentifizierung und Autorisierung von Benutzern sowie zur Kontrolle des Zugriffs auf sensible Daten und Funktionen verfügen.
- Datenverschlüsselung: Die Anwendungen müssen sensible Daten sowohl während der Übertragung als auch im Ruhezustand verschlüsseln, um sie vor unbefugtem Zugriff oder Offenlegung zu schützen.
- Validierung von Eingaben: Die Anwendungen müssen alle von externen Quellen eingehenden Eingaben validieren, um sicherzustellen, dass sie sicher und frei von bösartigem Code sind.

### 4.4.27 A.8.27 - Sichere Systemarchitektur und technische Grundsätze

>> Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sollten festgelegt, dokumentiert, aktuell gehalten und bei allen Entwicklungsaktivitäten eines Informationssystems angewendet werden.

Eine sichere Systemarchitektur und Technik in der Entwicklung, findet sich in entsprechenden Prozessen integriert. Dies ist Bestandteil der Anforderungen sowie zugehörigen Anleitungen und ist übergreifend durch die Vorgaben des Security Guides und die Bereitstellung des Frameworks sichergestellt.

### 4.4.28 A.8.28 - Sicheres Coding

>> Bei der Softwareentwicklung sollten die Grundsätze der sicheren Kodierung angewandt werden.

Wir definieren Kriterien zur Entwicklung sicherer Software, welche sich an etablierten Kriterienkatalogen orientieren. Diese werden durch Entwicklungsdokumentation und QM-Maßnahmen für die unterschiedlichen Tech-Stacks konkretisiert.

### 4.4.29 A.8.29 - Sicherheitsprüfung in Entwicklung und Abnahme

>> Sicherheitsprüfverfahren sollten definiert und in den Entwicklungslebenszyklus integriert werden.

Im Rahmen des Qualitätsmanagements und Changemanagements werden Neuentwicklungen und Weiterentwicklungen geplant und durchgeführt. Vor der Freigabe von neuen oder veränderten Informationssystemen werden diese mit manuellen oder automatischen Tests gegen die definierten Anforderungen sowie auf Anforderungen von Datenschutz und Sicherheit getestet. Für den Testprozess und als Ansprechpartner für das Testmanagement gibt es Testverantwortliche. Zudem sichern automatische Tests kontinuierlich gegen unbeabsichtigte Seiteneffekte der Entwicklung ab.

### 4.4.30 A.8.30 - Ausgegliederte Entwicklung

>> Die Organisation sollte die Aktivitäten im Zusammenhang mit der ausgelagerten Systementwicklung leiten, überwachen und überprüfen.

Im Rahmen des Partnermanagements ist geregelt und definiert, wie Tätigkeiten rund um ausgegliederter Systementwicklungen integriert und überwacht bzw. betrieben werden. Die Hauptverantwortung dafür trägt der jeweilige Partnermanager des jeweiligen Entwicklungspartners.

### 4.4.31 A.8.31 - Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen

>> Entwicklungs-, Prüf- und Produktionsumgebungen sollten getrennt und gesichert werden.

Die Bereitstellung, der Betrieb und die Pflege einer sicheren Entwicklungsumgebung ist durch entsprechende Themenverantwortliche sichergestellt. Sicherheit und Aktualität der Entwicklungsumgebung und der gesamten Applikationslandschaft werden dabei im Rahmen des Applikationsmanagements regelmäßig geprüft.

Entwicklungssysteme, Qualitätssicherungs-/Konsolidierungs-/Testsysteme und Produktivsysteme werden strikt getrennt. Dies ist durch entsprechende Prozesse und Richtlinien gesichert.

Wo AEB nicht die Entwicklung verantwortet (3rd Party Systeme) existieren ggf. keine Entwicklungssysteme. Trotzdem sind aber Qualitätssicherungs-/Konsolidierungs-/Testsysteme und Produktivsysteme auch hier strikt getrennt.

In Sonderfällen kann auch eine Umgebung zusätzlich weitere 2 voneinander getrennte Systeme umfassen (z.B. zwei getrennte Produktivsysteme für FirstCustomer Betrieb und Regelbetrieb, oder zwei getrennte Testsysteme, je eines für Smoketests und Implementierungstests).

Für den Cloud-Betrieb gilt zusätzlich: AEB berücksichtigt die datenschutzrechtlichen Maßnahmen einschließlich Risikobetrachtung auch für Situationen, in denen Testdaten verwendet werden sollten.

### 4.4.32 A.8.32 - Änderungssteuerung

>> Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen sollten Gegenstand von Änderungsmanagementverfahren sein.

Alle Änderungen von technischen Systemen unterliegen Change Prozessen. Diese steuern die jeweilige Änderung. Sie sind in internen Guides (z.B. im Change Management Prozess, im Admin Guide oder im Security Guide) dokumentiert.

Dies gilt insbesondere bei Änderungen an der Betriebsplattform. Dies stellt sicher, dass es bei Änderungen an der Betriebsplattform keine negativen Auswirkungen auf geschäftskritische Anwendungen gibt.

Bei Änderungen von kundenindividuellen Systemen werden Prozesse ggf. individuell mit den Kunden definiert.

Alle Änderungen an Softwareartefakten unterliegen einem Release Management. Hier werden neben der Release Planung, der Qualitäts- und Securitysicherung auch die Kommunikation zum Kunden koordinieren und Softwareveränderungen mit für Kunden bemerkbaren Auswirkungen bewerten.

### 4.4.33 A.8.33 - Prüfinformationen

>> Die Prüfinformationen sollten in geeigneter Weise ausgewählt, geschützt und verwaltet werden.

Im Rahmen des Qualitätsmanagements ist das Auswählen, Schützen und Steuern von Testdaten, in Prozessen und HowTos integriert. Tests finden in einer geschützten Umgebung statt, die sicherstellt, dass keine Sicherheitsbrüche passieren und keine Produktivdaten versehentlich modifiziert werden. Testdaten werden nicht in produktive Systeme übernommen.

Kundeneigene Hardwaregeräte werden in abgesicherten Räumen gelagert und auch nur dort administriert. Hier erfolgt Zutrittskontrolle nur für autorisierte Mitarbeitende.

Daten auf Kunden-Hardware werden sofort nach Erhalt und Testdaten vor der Inbetriebnahme gelöscht.

### 4.4.34 A.8.34 - Schutz der Informationssysteme während der Überwachungsprüfung

>> Auditprüfungen und andere Sicherheitstätigkeiten, die eine Beurteilung der betrieblichen Systeme beinhalten, sollten zwischen dem Prüfer und dem zuständigen Management geplant und vereinbart werden.

Managementsysteme (wie zu Informationssicherheit und Datenschutz) werden durch jeweils Zuständigen gemanagt. In deren Aufgabenbereich fällt auch das Organisieren von Audits und anderen Sicherheitsprüfungen, intern wie extern. Dabei wird auch der Erhalt der Betriebsfähigkeit und auch Geheimhaltung berücksichtigt.

Alle anstehenden Audits werden übersichtlich mit einer Auditplanung organisiert.

Es finden keine Audits/keine Überprüfungen von Informationssystemen ohne einen Verantwortlichen für das jeweilige Informationssystem statt. Der Verantwortliche stellt sicher, dass durch das Audit keine Veränderungen an den Systemen geschehen und reibungslose Betrieb trotz Audit gewährleistet bleibt.

# 5 Informationssicherheits-Controls der ISO 27018 / Anhang A

Die ISO 27018 bringt an zwei Stellen Anforderungen zu Controls mit:

- Aus Kapiteln vor dem Anhang A: Diese führen vereinzelt zu Ergänzungen direkt in den Controls der ISO 27001. Sie werden direkt im Kapitel "Informationssicherheits-Controls der ISO 27001 / Annex A / SoA" mit dem Zusatz "Für Cloud-Betrieb gilt zusätzlich: ..." abgebildet.
- Aus dem Anhang A der ISO 27018: Diese haben wir im Folgenden als eigene Controls, die den Datenschutz-Prinzipien zugeordnet sind, abgebildet.

Sie sind in ihrer Nomenklatur aufgebaut nach den Ebenen:

- Regelungsbereich (A.1 bis A.11)
- Control (z.B. A.05.1)

AEB nimmt hier zu den Anforderungen für alle Controls Stellung.
Jedes Control ist einem Control-Verantwortlichen zugewiesen. Die Pflege der Controls ist prozess-gesteuert und gemanagt. Dabei wird ein regelmäßiger Review, u.a. auch mit Blick auf Stand der Technik durchgeführt.

Umfassend gilt:

- Es gibt keine Ausschlüsse
- Alle Anforderungen sind umgesetzt und aktiv

## 5.1 A.1 - Einwilligung und Wahlmöglichkeit

### 5.1.1 A.01.1 - Verpflichtung zur Zusammenarbeit, wenn es um die Rechte Betroffener geht

>> Der Öffentliche-Cloud-Auftragsdatenverarbeiter sollte dem Cloud-Dienstleistungskunden Mittel zur Verfügung stellen, die ihn in die Lage versetzen, seinen Verpflichtungen bezüglich der Erleichterung der Ausübung der Rechte der Betroffenen auf Zugang zu ihren eigenen personenbezogenen Daten, zu deren Korrektur und/oder Löschung nachzukommen.

Die AEB unterstützt ihren Kunden als Verantwortlichen bei der Ausübung von Betroffenenrechten (gemäß Kapitel III DS-GVO). Dies wird mit dem Kunden im AEB-Standard-Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO vereinbart.

Der Umgang mit direkten Anfragen Betroffener an AEB als Auftragsverarbeiter ist im genannten Vertrag geregelt.

Darüber hinaus unterstützt AEB ihre Kunden mit Informationen in unserem Trust Center (https://www.aeb.com/de-de/trust-center/datenschutz.php) bei der Erfüllung z.B. seiner Informationspflichten als Verantwortlicher.

AEB schult ihre Mitarbeitende zur Unterstützung bei Vorgängen mit Betroffenen-Rechten.

## 5.2 A.2 - Zulässigkeit des Zwecks und Zweckbestimmung

### 5.2.1 A.02.1 - Zweck des Öffentlichen-Cloud-Auftragsverarbeiters von personenbezogenen Daten

>> Die im Rahmen eines Vertrages zu verarbeitenden pbD sollten für keine anderen als die mit den Anweisungen des Cloud-Dienstleistungskunden verbundenen Zwecke verarbeitet werden.

Zweckbindung ist ein wesentliches Prinzip im Datenschutz.

Im AEB-Standard-Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO werden die Zwecke, die Zweckgebundenheit und Weisungsgebundenheit vereinbart. Dabei werden die der Auftragsverarbeitung zugrunde liegende(n) Leistungsvereinbarung(en) einbezogen.

Zur Transparenz dienen auch Informationen in unserem AEB Trust Center (u.a. Verzeichnis von Verarbeitungstätigkeiten).

AEB gibt die Pflichten auf Zweck- und Weisungsgebundenheit auch an mögliche Unterauftragnehmer weiter. Ein Kapitel im AEB-Standard-Vertrag zur Auftragsverarbeitung widmet sich der möglichen Einschaltung von Subunternehmern inklusive Regelung zur Genehmigung durch den Verantwortlichen.

AEB gewährt selbstverständlich dem Verantwortlichen das Recht zur Kontrolle auf Einhaltung der gesetzlichen und vertraglichen Regelungen.

### 5.2.2 A.02.2 - Kommerzielle Nutzung durch den Öffentlichen-Cloud-Auftragsdatenverarbeiter

>> Öffentliche-Cloud-Auftragsdatenverarbeiter sollten die von ihnen im Rahmen eines Vertrages verarbeiteten pbD nicht ohne ausdrückliche Einwilligung für Marketing- oder Werbezwecke verwenden. Eine solche Einwilligung sollte keine Bedingung für die Nutzung des Dienstes sein.
ANMERKUNG: Diese Maßnahme ergänzt die allgemeineren Maßnahmen nach A.2.1 und ersetzt diese keinesfalls.

AEB wird die im Rahmen eines Vertrages verarbeiteten personenbezogenen Daten nicht ohne ausdrückliche Einwilligung für Marketing- oder Werbezwecke verwenden. Entsprechend finden Schulungen statt.

## 5.3 A.3 - Erhebungsbeschränkung

Für dieses Datenschutzprinzip gelten keine weiteren Maßnahmen.

## 5.4 A.4 - Datenvermeidung und Datensparsamkeit

### 5.4.1 A.04.1 - Sichere Löschung von temporären Dateien

>> Vorübergehend erzeugte (temporäre) Dateien und Dokumente sollten innerhalb eines festgelegten und dokumentierten Zeitraums gelöscht oder zerstört werden.

Es gibt zum Löschen von temporären Daten Prozesse, die das regelmäßige Löschen von Dateien nachhalten.

Die maximale Aufbewahrungsdauer solcher Dateien ist - sofern pro Service/Prozess/Kunde nicht anders vereinbart - auf 3 Monate festgelegt.

## 5.5 A.5 - Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung

### 5.5.1 A.05.1 - Mitteilung einer Offenlegung personenbezogener Daten

>> Der Vertrag zwischen dem Öffentlichen-Cloud-Auftragsdatenverarbeiter und dem Cloud-Dienst-Kunden sollte die Anforderung enthalten, dass der Öffentliche-Cloud-Auftragsverarbeiter den Cloud-Dienstleistungskunden entsprechend den im Vertrag vereinbarten Verfahren und Fristen über alle von einer Strafverfolgungsbehörde gestellten rechtsverbindlichen Anträge auf Offenlegung von pbD informiert, es sei denn, eine derartige Offenlegung ist an anderer Stelle verboten.

Der AEB-Standard-Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO vereinbart:
*„Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor.*

*(…)*

*Der Auftragnehmer informiert unverzüglich den Auftraggeber über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt."*

### 5.5.2 A.05.2 - Aufzeichnung der Offenlegung von pbD

>> Offenlegungen von pbD gegenüber Dritten sollten unter Angabe der offengelegten pbD, der Personen, gegenüber denen sie offengelegt wurden, und des Datums und der Uhrzeit der Offenlegung aufgezeichnet werden.

AEB hat einen Prozess zum Umgang mit behördlichen Durchsuchungen etabliert; dieser sieht eine Protokollierung vor.

AEB hat einen Prozess etabliert, der den Umgang mit unzulässiger Offenlegung personenbezogener Daten beschreibt (Stichwort: Datenpannen). Die AEB beachtet ihre Unterstützungspflicht gegenüber dem Verantwortlichen zu dessen Meldungen (gemäß Art. 33 und 34 DS-GVO). Dies ist im AEB-Standard-Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO vereinbart.

## 5.6 A.6 - Genauigkeit und Qualität

Für dieses Datenschutzprinzip gelten keine weiteren Maßnahmen.

## 5.7 A.7 - Offenheit, Transparenz und Benachrichtigung

### 5.7.1 A.07.1 - Offenlegung der im Unterauftrag ausgeführten Verarbeitung von pbD

>> Falls der Öffentliche-Cloud-Auftragsdatenverarbeiter für die Verarbeitung der pbD die Dienste von Unterauftragnehmern in Anspruch nimmt, sollte dies zuvor den betreffenden Cloud-Dienstleistungskunden mitgeteilt werden.

Der AEB-Standard-Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO vereinbart in einem Kapitel die Regelung zur Einschaltung von Subunternehmern. Diese schließt die frühzeitige, geeignete Information an den Verantwortlichen ein.

AEB präsentiert transparent die aktuelle Übersicht ihrer Subunternehmer im Trust Center unter https://www.aeb.com/de-de/trust-center/datenschutz.php.

## 5.8 A.8 - Persönliche Teilnahme und Zugang

Für dieses Datenschutzprinzip gelten keine weiteren Maßnahmen.

## 5.9 A.9 - Verantwortlichkeit

### 5.9.1 A.09.1 - Benachrichtigung über eine personenbezogene Daten betreffende Datenschutzverletzung

>> Im Falle eines nicht autorisierten Zugriffs auf pbD oder auf Verarbeitungsgeräte oder -einrichtungen, der zu einem Verlust oder zur Offenlegung oder Änderung von pbD führt, sollte der Öffentliche-Cloud-Auftragsdatenverarbeiter den betreffenden Cloud-Dienstleistungskunden umgehend informieren.

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten. Dies ist im AEB-Standard-Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO vereinbart.

Die AEB hat das Gerüst für die Meldung einer Datenpanne an den Kunden, orientiert an den Vorgaben von Art. 33 DS-GVO, vorbereitet.

Die AEB nutzt für die Meldung vorliegende geeignete Kontakte des Kunden.

Die AEB hat einen Prozess etabliert, der neben der Meldung auch die weiteren Schritte der Untersuchung und Nachbearbeitung geeignet dokumentiert, protokolliert und in erforderlichem Maße aufbewahrt.

### 5.9.2 A.09.2 - Aufbewahrungszeitraum für administrative Sicherheitsricht- und leitlinien

>> Nach einem Austausch (einschließlich Aktualisierung) sollten Kopien der neuen der Sicherheitsrichtlinien und Betriebsverfahren für einen festgelegten und dokumentierten Zeitraum aufbewahrt werden.

AEB archiviert ihre Sicherheitsrichtlinien über wenigstens 5 Jahre.

### 5.9.3 A.09.3 - Rückgabe, Übertragung und Löschung von pbD

>> Der Öffentliche-Cloud-Auftragsdatenverarbeiter sollte über Richtlinien zur Rückgabe, Übertragung und/oder Löschung von pbD verfügen und sie dem Cloud-Dienstleistungskunden zugänglich machen.

Die Thematik Löschung und Rückgabe von personenbezogenen Daten ist im AEB-Standard-Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO vereinbart.

Die AEB unterstützt den Kunden bei seiner Ausübung von Lösch-Verpflichtungen; hierzu bietet AEB auch eine Anleitung (Löschkonzept) im AEB Trust Center https://www.aeb.com/de-de/trust-center/datenschutz.php.

Die AEB berät auch für den Umgang mit Lösch-Anfragen seitens Betroffener.

Die AEB unterstützt den Kunden auch bei Anfragen zu Daten-Rückgaben.

# 5.10 A.10 - Informationssicherheit

## 5.10.1 A.10.1 - Vertraulichkeits- oder Geheimhaltungsvereinbarungen

>> Personen, die unter der Aufsicht des Öffentlichen-Cloud-Auftragsverarbeiters von personenbezogenen Daten Zugang zu pbD erhalten, sollten zur Geheimhaltung verpflichtet werden.

Mitarbeitende sowie Partner unterzeichnen bei Vertragsbeginn Standard-Verträge mit entsprechender Verpflichtung zur Geheimhaltung, auch in der Datenverarbeitung.
Diese Verträge enthalten Zweckbindung entsprechend der Weisungsgebundenheit im Rahmen vorliegender Auftragsverarbeitung.
Die Pflicht zur Geheimhaltung geht über die Dauer der Vereinbarung hinaus.
Obige Sachverhalte sind überdies Gegenstand des Weiterbildungsprogramms der AEB.

## 5.10.2 A.10.2 - Beschränkung der Erstellung von ausgedruckten Materialien

>> Das Recht zur Erstellung von ausgedruckten Materialien (en: hardcopy material), die pbD anzeigen, sollte beschränkt werden.

AEB verfolgt den Ansatz papierlosen Betriebs.
Die Prozesse mit Kundendaten enthalten keine Prozess-Schritte, die einen Druckvorgang enthalten.
Ausnahmen können sich im Einzelfall durch beauftragte Kunden-Anforderungen (etwa zu Test-Zwecken) ergeben.

Regelmäßige Hausrundgänge prüfen auf angemessenen Umgang u.a. zu Clean Desk.

## 5.10.3 A.10.3 - Überwachung und Protokollierung von Datenwiederherstellungsprozessen

>> Für alle Datenwiederherstellungsprozesse sollten entsprechende Verfahren zur Verfügung stehen, und diese Prozesse sollten protokolliert werden.

- Siehe zu Datensicherung: A.8.13 - Sicherung von Information
- A.5.29 - Informationssicherheit bei Störungen
- A.8.15 - Protokollierung
- dokumentierte Prozessbeschreibung in Datenwiederherstellungsprozesse

### 5.10.4 A.10.4 - Schutz von Daten auf Datenträgern, die die eigenen Räumlichkeiten verlassen

>> pbD auf Datenträgern, die die Räumlichkeiten der Organisation verlassen, sollten einem Autorisierungsverfahren unterzogen werden und für niemand anderen als das entsprechend berechtigte Personal zugänglich sein (z. B. durch Verschlüsselung der betreffenden Daten).

Siehe A.5.14 - Informationsübertragung

Dies gilt auch bei Datenträger-Transfers.

Physischen Zutritt in das Rechenzentrum der AEB haben ausgewählte, befugte Rollen aus IT und Facility.

Sicherheitsmaßnahmen (wie Verschlüsselung) sind Bestandteil des AEB Security Guides.

AEB verhält sich im Zweifel, als wären personenbezogene Daten auf den Datenträgern; entsprechend sind die Maßnahmen darauf abgestellt.

### 5.10.5 A.10.5 - Nutzung von unverschlüsselten tragbaren Speichermedien und Geräten

>> Es sollten keine tragbaren physischen Speichermedien oder Geräte verwendet werden, die keine Verschlüsselung erlauben, es sei denn, dies lässt sich nicht vermeiden, und jede Nutzung derartiger tragbarer Speichermedien und Geräte sollte dokumentiert werden.

Regelungen aus A.8.24 - Verwendung von Kryptographie und A.7.10 - Speichermedien

Die Mitarbeitenden beachten interne Hinweise im Security Guide zu „Daten außer Haus“.

Für den Fall, dass ein Datenträger unverschlüsselt eingeht, wird der Absender hierauf hingewiesen und entweder die Verschlüsselung nachgeholt oder die Situation samt Hintergründen dokumentiert.

### 5.10.6 A.10.6 - Verschlüsselung von über öffentliche Datenübertragungsnetzwerke gesendeten pbD

>> pbD, die über öffentliche Datenübertragungsnetzwerke gesendet werden, sollten vor der Übertragung verschlüsselt werden.

Siehe dazu A.5.14 - Informationsübertragung mit Aussagen zu Data on the move.

## 5.10.7 A.10.7 - Sichere Entsorgung von ausgedruckten Materialien

>> Falls ausgedruckte Materialien zerstört werden, sollte ihre Zerstörung unter Anwendung sicherer Verfahren, wie z. B. Querschneiden, Zerkleinern, Verbrennen, Aufschluss usw., erfolgen.

Verweis auf A.7.10 - Speichermedien

Der AEB-Standard bezieht sich auf die Referenz DIN 66399. Die Auswahl der Schutzklasse bzw. der Sicherheitsstufe berücksichtigt die Möglichkeit, pbD zu enthalten.

## 5.10.8 A.10.8 - Eindeutige Nutzung von User-IDs

>> Falls mehrere Personen Zugang zu gespeicherten pbD haben, sollten alle diese Personen für Identifizierungs-, Authentisierungs- und Autorisierungszwecke je eine eigene User-ID besitzen.

- A.5.16 - Identitätsmanagement
- A.8.2 - Privilegierte Zugangsrechte
- Alle MA haben (zumindest) eine eindeutige User-ID.
  Damit stellen wir auch die Eingabekontrolle sicher.

## 5.10.9 A.10.9 - Datensätze von berechtigten Benutzern

>> Es sollte ein Datensatz zu den Benutzern oder den Profilen von Benutzern, die berechtigten Zugang zum Informationssystem haben, geführt und aufbewahrt werden.

Siehe hierzu auch den Abschnitt Zugriffskontrolle und insbesondere den detaillierten Einblick "Auszug aus dem AEB Security Konzept: Details zu Zutritt, Zugang und Zugriff", der im Trust Center der AEB unter Sicherheit bei AEB zur Verfügung steht.

Das Rechte-Konzept der AEB beinhaltet die Stufen

- Ein Mitarbeitender hat 1-n Rollen
- Eine Rolle hat Berechtigung(en), einschließlich Zugriffsrechten.

## 5.10.10 A.10.10 - Verwaltung von User-IDs

>> Deaktivierte oder erloschene User-IDs sollten nicht an andere Personen vergeben werden.

Alle User erhalten auf Datenbankebene eine eindeutige, nicht wieder verwendbare ID.

## 5.10.11 A.10.11 - Vertragsmaßnahmen

>> In Verträgen zwischen Cloud-Dienstleistungskunden und Öffentlichen-Cloud-Auftragsverarbeitern von personenbezogenen Daten sollten technische und organisatorische Mindestmaßnahmen festgelegt werden, die sicherstellen, dass die vertraglich geregelten Sicherheitsvorkehrungen getroffen wurden und dass Daten nicht für andere als die mit den Anweisungen des Cloud-Dienstleistungskunden verbundenen Zwecke verarbeitet werden. Diese Maßnahmen sollten nicht einseitig vom Öffentlichen-Cloud-Auftragsdatenverarbeiter reduziert werden.

Siehe hierzu auch den Abschnitt Auftragskontrolle

Für AEB ist rechtsverbindliche Grundlage die DS-GVO. Auftragsverarbeitung findet auf Basis der Regelungen aus Art. 28 DS-GVO statt. Die AEB führt entsprechende Vereinbarungen mit ihren Kunden.

Mitgeltend zu dieser Vereinbarung sind die technischen und organisatorischen Maßnahmen der AEB als Auftragsverarbeiter. Die Aufstellung enthält Controls zu Art. 32 DS-GVO, ISO 27001 und ISO 27018.

Die Vereinbarung enthält die Regelung, das mit ihr erzielte Sicherheitsniveau nicht zu reduzieren.

Die Angaben werden transparent auf der Webseite der AEB (AEB Trust Center) in der stets aktuellen Fassung zur Verfügung gestellt.

Die AGB der AEB verweisen auf das Erfordernis, eine Vereinbarung zur AVV abzuschließen. Darin enthalten ist auch der Hinweis auf den Zugang erforderlicher Unterlagen.

## 5.10.12 A.10.12 - Im Unterauftrag erfolgende Verarbeitung von personenbezogenen Daten

>> In Verträgen zwischen Öffentlichen-Cloud-Auftragsverarbeitern von personenbezogenen Daten und ihren Unterauftragnehmern sollten technische und organisatorische Mindestmaßnahmen zur Erfüllung der Informationssicherheits- und Datenschutzverpflichtungen des Öffentlichen-Cloud-Auftragsverarbeiters von personenbezogenen Daten festgelegt werden. Diese Maßnahmen sollten nicht einseitig vom Unterauftragnehmer reduziert werden.

Die AEB regelt in ihrer Vereinbarung zur Auftragsverarbeitung die Thematik der Subunternehmer. Auf vorhandene Subunternehmer wird in unserem Trust Center hingewiesen und diese aufgelistet.

Vereinbarungen mit den Subunternehmern schließen die Prüfung entsprechender Sicherheitsmaßnahmen ein. Das den Cloud-Kunden zugesagte Sicherheitsniveau darf bei Hinzunahme von Subunternehmern nicht unterschritten werden.

Kontrollen beinhalten die Erkundigung nach Änderungen der Sicherheitsmaßnahmen.

### 5.10.13 A.10.13 - Zugang zu Daten in bereits genutzten Datenspeichern

>> Wann immer einem Cloud-Dienstleistungskunden Datenspeicherplatz zugeteilt wird, sollte der Öffentliche-Cloud-Auftragsdatenverarbeiter sicherstellen, dass keine der möglicherweise zuvor an dieser Stelle gespeicherten Daten für den Cloud-Dienstleistungskunden sichtbar werden.

Siehe DS-GVO_Control-Trennung

Die Anwendungen der AEB stellen Mandanten-Trennung sicher.

## 5.11 A.11 - Einhaltung der Datenschutzpflichten

### 5.11.1 A.11.1 - Geographischer Standort von pbD

>> Der Öffentliche-Cloud-Auftragsdatenverarbeiter sollte festlegen und dokumentieren, in welchen Ländern die betreffenden pbD möglicherweise gespeichert werden können.

- Siehe https://www.aeb.com/de-de/trust-center/rechenzentren.php
- in den Verfahren des Verfahrensverzeichnis der AEB werden die Orte der Verarbeitung dokumentiert
- Kunden erhalten Unterstützung zu ihrem Verfahrensverzeichnis unter https://www.aeb.com/de/trust-center/datenschutz.php#Weitere-Materialien
- Kunden erhalten Informationen zu etwaigen Daten-Übermittlungen mittels der Dokumentation zu AVV sowie mitgeltender Übersicht der Subunternehmer; auch zu finden unter Datenschutz. Auftragsverarbeitungs-Verträge (AVV). (aeb.com).

### 5.11.2 A.11.2 - Vorgesehener Bestimmungsort von pbD

>> In Bezug auf pbD, die über ein Datenübertragungsnetzwerk übermittelt werden, sollten geeignete Maßnahmen ergriffen werden, um sicherzustellen, dass diese Daten ihren vorgesehenen Bestimmungsort erreichen.

Die eingerichtete Ende-zu-Ende-Verschlüsselung stellt sicher, dass Daten nur - wie vorgesehen - im AEB-Rechenzentrum entschlüsselt und verarbeitet werden können.