Leitlinie

Datenschutz

Version 3.0

Januar 2022

www.aeb.com

Die Datenschutz-Leitlinie der AEB

Mit den nachfolgenden Angaben benennt die AEB Eckpunkte, die wir als Datenschutz-Leitlinie zum Umgang mit personenbezogenen Daten (kurz: pbD) bezeichnen.

Kern dieser Leitlinie sind

- die korrekte Anwendung der relevanten Datenschutz-Gesetze (insbesondere der EU-Datenschutz-Grundverordnung (kurz: DS-GVO) und nationaler Gesetze wie etwa des Bundesdatenschutzgesetzes),
- das Bekenntnis zu den Datenschutz-Prinzipien (wie in ISO 29100 formuliert)
- sowie die Erfüllung der Pflichten gegenüber Verantwortlichen im Verhältnis der Auftragsverarbeitung.

Diese Leitlinie umfasst folgende wesentlichen Eckpunkte und **Grundsätze**:

Datenschutz ist Chefsache; der Verwaltungsrat der AEB ist Verantwortlicher im Sinne Art. 4 DS-GVO und Eigentümer dieser Leitlinie; er bekennt sich entsprechend zu den Grundsätzen aus Art. 5 DS-GVO und den **Datenschutz-Prinzipien**, wie sie u. a. in der ISO 29100 festgehalten sind:

Datenschutz-Prinzip	Kern-Botschaft der AEB, Hinweise zur Umsetzung
Einwilligung und Wahlfreiheit	AEB ist es wichtig, dass Benutzer (als Betroffene) in den AEB-Anwendungen nur wirklich fachlich erforderliche Angaben zur Person angeboten bekommen. Daher sehen wir dieses Prinzip verbunden mit den Geboten von Datenminimierung, Zweckgebundenheit und Transparenz.
Zulässigkeit und Zweckorientierung	AEB stellt in ihren Anwendungen Daten in dem Umfang zur Verfügung, wie sie fachlich erforderlich sind. Die Verwendung pbD stützt sich daher i. d. R. auf überwiegende berechtigte Interessen oder rechtliche Pflichten des Verantwortlichen. Hier treibt uns auch der Wille, dass Anwendungen schlank, verständlich und gut beherrschbar sind. Produkt-Design beinhaltet immer die Berücksichtigung des fachlichen Erfordernisses. AEB führt eine Aufstellung von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO; damit werden pbD identifiziert und ihre Verarbeitung nach entsprechender Regelung untersucht, regelmäßig geprüft und dokumentiert. Wichtige Schritte dabei sind die Prüfung auf Zulässigkeit entsprechend anwendbaren Rechtsgrundlagen sowie die integrierte zweistufige Risikobetrachtung.
Beschränkung der Erhebung, Datenvermeidung und -sparsamkeit	Der Satz personenbezogener Daten wird auf das wirklich Erforderliche beschränkt. Der Ansatz ist, möglichst keine personenbezogenen Daten zu erheben. Die Anwendungen der AEB sehen keine privaten und sensiblen Angaben der Benutzer vor. In Prozesse der Produkt-Entwicklung sind Prüfungen auf die genannten Gebote eingebaut. Die Mitarbeiter der AEB sind entsprechend geschult.

Datenschutz-Prinzip	Kern-Botschaft der AEB, Hinweise zur Umsetzung
Beschränkung bei der Nutzung, Aufbewahrung, Offenlegung	AEB sieht die Löschung pbD vor, wenn der Zweck der Verarbeitung der pbD endet und keine gesetzlichen oder vertraglichen Anforderungen an ihre Aufbewahrung bestehen. Die Aufbewahrungspflichten ergeben sich aus den Datenarten der Anwendungen in Verbindung mit geschäftlichen Interessen des Verantwortlichen. Die Lösch-Routinen orientieren sich an den Angaben des AEB-Löschkonzepts.
Genauigkeit und Qualität	AEB stellt den Betroffenen selbst die Möglichkeit zur Erfassung, Kontrolle und bedarfsweisen Korrektur zur Verfügung. Art und Umfang der Daten (Kontaktdaten im Austausch von Meldungen) führen zu guter Kontrolle über die Korrektheit der Angaben.
Offenheit, Transparenz und Benachrichtigung	AEB geht ihren Informationspflichten als Verantwortlicher in ihrer ausführlichen Datenschutz-Erklärung nach, die auch in die Fälle möglicher Erhebung von pbD einbezogen wird. Für die Auftragsverarbeitung stellt AEB Informationen an diversen Stellen (Leistungsbeschreibungen, Vereinbarung zur Auftragsverarbeitung sowie im AEB Trust Center) zur Verfügung.
Persönliche Teilnahme und Zugang	AEB stellt den Betroffenen selbst die Möglichkeit zur Erfassung, Kontrolle und bedarfsweisen Korrektur zur Verfügung. Der beschränkte Umfang und die Art der Daten (Kontaktdaten) führt zu guter Kontrolle über die Korrektheit der Angaben.
Verantwortlichkeit	AEB gibt extern wie intern Auskünfte, wie sie gestützt auf ein Datenschutz- Managementsystem (DSMS) ihren datenschutzrechtlichen Pflichten nachkommt. Für intern bietet das AEB-Intranet Direkteinstieg mit Auskünften zum DSMS. Für extern bietet AEB Einstiege mit ihrer Datenschutzerklärung sowie mit ihrem Datenschutz-Auftritt im Trust Center.

Informationssicherheit	AEB betreibt ein ISMS auf Basis der ISO 27001. Als wesentliche Sicherheitskriterien werden Vertraulichkeit, Verfügbarkeit und Integrität berücksichtigt. Besondere Bedeutung haben die integrierten regelmäßigen Kontrollen und die Risikobetrachtung.
	Mitgeltend für die Risikobetrachtung im Umfeld des DSMS sind aus dem ISMS:
	• der Kontext zum Verständnis der Organisation, samt technischem Umfeld und Einflussfaktoren wie
	  • gesetzliche und regulatorische Faktoren (inkl. internationales Umfeld, Gerichtsentscheidungen)
	  • vertragliche Faktoren
	  • geschäftliche Faktoren (z.B. spezifische Merkmale oder Nutzungskontext einer geplanten Anwendung, oder relevante Normen)
	• Methodik der Risikobetrachtung
	• Methodik der Risikobehandlung
	Überwachung und Überprüfung, indem Risiken und Steuerungsmaßnahmen verfolgt werden und der Prozess verbessert wird.

Einhaltung der Datenschutzpflichten	AEB betreibt ein ISMS auf Basis der ISO 27001 und ISO 27018. Besondere Bedeutung haben die integrierten regelmäßigen Kontrollen und die Risikobetrachtung im engen Austausch zwischen Geschäftsleitung, Security-Rollen und Datenschutzbeauftragtem.

Die Hauptziele im Zusammenhang mit Datenschutz sind:

- Der **Schutz der Betroffenen**; etwa durch intensive Beschäftigung mit Privacy-by-Design und Privacy-by-Default, sowie den Geboten zu Datenvermeidung und -sparsamkeit. Erste Betrachtungen werden stets den Fragen nach **Erforderlichkeit und Rechtmäßigkeit der Datenverarbeitung** gewidmet. Eine **regelmäßige und prozessorientierte Risikobetrachtung** nimmt die Sicht des Betroffenen ein.
- **Schutz der Daten bzgl. der Sicherheitsziele:** Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit. Zur Realisierung eines guten, angemessenen Datenschutzniveaus sowohl für Kunden als auch im Innenverhältnis für Beschäftigte.
- **Transparenz** und Bewusstsein zu den **Informationspflichten** im Innen- und Außenverhältnis.
- **Dokumentation** von Verarbeitungstätigkeiten mit integrierter **Risikobetrachtung** und Kontrolle u. a. zur Rechtsgrundlage und Einhaltung der Zweckbindung.
- **Aus- und Weiterbildung** der AEB-Mitarbeiter zu Datenschutz und Sicherheitsbewusstsein (Awareness).
- Unterstützung der AEB-Kunden, sofern **AEB als Auftragsverarbeiter** (gemäß Art. 28 DS-GVO) agiert.
- Zusammenarbeit mit den zuständigen Aufsichtsbehörden.
- Bereitstellung ausreichender Ressourcen.

Weitere Eckpunkte:

- Der Datenschutzbeauftragte (Kontakt: mailto:datenschutzbeauftragter@aeb.com) ist Bestandteil der Datenschutz-Leitlinie. Er ist zu Zwecken der Unterstützung, Beratung und Kontrolle intern beauftragt und ordentlich benannt.
- AEB erfüllt ihre **Anforderungen als Auftragsverarbeiter**
  - gemäß den gesetzlichen Verpflichtungen (aus u. a. Art. 28 DS-GVO),
  - gemäß den vertraglichen Verpflichtungen (etwa zur Unterstützung bei der **Datenschutz-Folgenabschätzung**), die sie mit ihren Kunden als Verantwortliche eingeht.
  - AEB stellt einen Standard-Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO bereit, zugeschnitten auf die Hauptleistungen (Hosting-Services, Support) der AEB als Auftragnehmer.
- Aufstellung und Pflege der **technischen und organisatorischen Maßnahmen** (gemäß Art. 32 DS-GVO) basierend auf **Stand der Technik**. Das ist unsere Zusammenstellung zur Datensicherheit, die fester Bestandteil unserer Verträge zur Auftragsverarbeitung gemäß Art. 28 DS-GVO ist. Das Sicherheitskonzept der AEB macht darüber hinaus Aussagen zu Sicherheitsmaßnahmen anhand der Controls der ISO 27001 (Erklärung zur Anwendbarkeit) sowie der ISO 27018.
- Durchführung von regelmäßigen **Selbst-Kontrollen, Audits** auf Einhaltung und Wirksamkeit der Maßnahmen. Mit Aufstellung und Auswertung von Befunden zur Beseitigung von Mängeln.
- **Verpflichtung unserer Mitarbeiter bei der Anstellung auf Geheimhaltung**; mit Hinweisen zur Rechtsverbindlichkeit.
- Regelmäßige Durchführung von grundlegenden und weiterführenden Schulungsmaßnahmen zum Datenschutz durch den Datenschutzbeauftragten. Auch mit Aufklärung zu den Rechten und Pflichten sowie Bereitstellung weiterführender, gut zugänglicher Informationen.
- Wahrnehmung von Auskunftspflichten nach innen und nach außen.

- AEB verwirklicht Datenschutz prozessorientiert durch ein **Datenschutz-Managementsystem**. Dieses stellt einen regelmäßigen Austausch in der Datenschutz-Organisation sowie die praktische Ausübung der **Rechenschaftspflicht, Kontrolle, Risikobetrachtung und kontinuierlichen Verbesserung** sicher.
- **Datenschutz ist Teil unserer Sicherheitskultur.** Die darin enthaltenen Regeln sind verbindlich und nachlesbar in unserem internen **Security-Guide**. Die Kultur wird belebt durch Security-Kampagnen und unterstützt und kontrolliert durch den Betrieb des ISMS zur ISO 27001. Das entsprechende Zertifikat kann unter https://www.aeb.com/de-de/trust-center/zertifikate.php/ abgerufen werden.

Transparenz meinen wir ernst. Besuchen Sie gerne unsere Webseiten mit weiteren Auskünften:

- Unsere Datenschutz-Erklärung
- Unser Trust Center mit Leitlinien und Zertifikaten zu Informationssicherheit und Datenschutz
- Unser Datenschutz-Auftritt im Trust Center

AEB SE . Hauptsitz . Sigmaringer Straße 109 . 70567 Stuttgart . Deutschland . +49 711 72842 0 . www.aeb.com . info.de@aeb.com . Registergericht: Amtsgericht Stuttgart . HRB 767 414 . Geschäftsführende Direktoren: Matthias Kieß, Markus Meißner . Vorsitzende des Verwaltungsrats: Maria Meißner

Standorte
Düsseldorf . Hamburg . Lübeck . Mainz . Malmö . Manila . München . New York . Prag . Amsterdam . Salzburg . Singapur . Soest . Stuttgart . Warwick . Zürich