Anlage 1: Technische und organisatorische Maßnahmen

Vertraulichkeit

Zutrittskontrolle

Es sind folgende Maßnahmen umgesetzt, um den Zutritt Unbefugter zu Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden, einzuschränken bzw. zu unterbinden.

- Geschlossene Türen und Fenster
- Sicherheitsschlösser
- Absicherung der Gebäudeschächte
- Kontrollierte Schlüsselvergabe
- Begleitung von Besuchern

Zugangskontrolle

Es sind folgende Maßnahmen umgesetzt, die verhindern, dass Datenverarbeitungseinrichtungen von Unbefugten benutzt werden können.

- Einsatz einer aktuellen Firewall
- Einsatz eines aktuellen Virenschutzes
- Verwendung individueller Benutzerkennungen
- Verwendung komplexer Passwörter
- Verwendung biometrischer Verfahren
- Zwei-Faktor-Authentisierung
- Automatische Bildschirmsperre
- Verschlüsselung von Daten bei Übertragung und Speicherung

Zugriffskontrolle

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass Zugriffe auf personenbezogene Daten ausschließlich entsprechend den zugeordneten Berechtigungen möglich sind. Zudem wird sichergestellt, dass personenbezogene Daten nicht unbefugt verarbeitet, d.h. nicht unbefugt erfasst, gelesen, kopiert, verändert oder gelöscht werden können.

- Anwendungsbezogene Authentifizierung und Autorisierung
- Protokollierung der Anwenderzugriffe
- Verschlüsselung von Daten bei Übertragung und Speicherung
- Aktenvernichter gem. DIN 66399 der Stufe P-4 oder höher

- Profilery ermöglicht dem Auftraggeber die Konfiguration einer spezifischen Rollen- und Rechteverwaltung mit differenziertem Berechtigungskonzept und datenbezogener Zugriffstrennung

Pseudonymisierung

Sofern erforderlich sind folgende Maßnahmen umgesetzt, um zu verhindern, dass personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen einer spezifischen betroffenen Person zugeordnet werden können.

- Eine Pseudonymisierung erfolgt im Verarbeitungsprozess so früh wie möglich

Trennungskontrolle

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Daten des Auftraggebers werden innerhalb eines Systems mittels Mandantentrennung gespeichert
- Trennung von Produktiv- und Testsystemen
- Keine Verarbeitung von Produktivdaten in Testumgebung

Integrität

Weitergabekontrolle

Es sind folgende Maßnahmen zur Gewährleistung der Datenintegrität umgesetzt, die generell zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung beitragen.

- Verschlüsselte Übertragung von Daten
- Protokollierung
- E-Mail-Verschlüsselung auf Wunsch

Eingabekontrolle

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass überprüft und festgestellt werden kann, von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.

- Protokollierung erfolgreicher und gescheiterter Anmeldeversuche
- Protokollierung bei der Erfassung, Änderung und Löschung personenbezogener Daten
- Nachvollziehbarkeit von Eingabe, Änderung, Löschung durch individuelle Benutzerkennungen
- Überwachung und Protokollierung von automatisierten Datenverarbeitungen
- Automatisierte Kontrolle von Logfiles

- Sicherung der Protokolldaten gegen Verlust und Veränderung

Auftragskontrolle

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Sorgfältige Auswahl von Auftragsverarbeitern unter Informationssicherheitsgesichtspunkten
- Abgeschlossener Auftragsverarbeitungsvertrag
- Dokumentation der Verarbeitungstätigkeiten
- Regelmäßige Kontrolle der Vertragsausführung
- Vernichtung von Daten nach Beendigung des Auftrags

Verfügbarkeit und Belastbarkeit

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und System und Dienste ausreichend belastbar sind.

- Feuer- und Rauchmeldeanlagen, Feuerlöscher
- Unterbrechungsfreie Stromversorgung
- Regelmäßiges und automatisiertes Patch-Management
- Einsatz redundanter Systeme
- Konzept zur Datensicherung und Wiederherstellung
- Regelmäßige Prüfung der Datensicherung
- Überwachung der Verfügbarkeit und Auslastung

Verfahren zur regelmäßigen Überprüfung, Bewertung und Validierung

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten regelmäßig, hinsichtlich ihrer Wirksamkeit bewertet und evaluiert werden.

- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der mit Datenverarbeitung Beschäftigten auf den Datenschutz und Vertraulichkeit
- Regelmäßige Schulung der mit der Datenverarbeitung Beschäftigten
- Regelmäßige Auditierung der Verfahren
- Regelmäßige Überprüfung des Stands der Technik gemäß Artikel 32 DSGVO

Datenschutzfreundliche Voreinstellungen

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass personenbezogene Daten nur erhoben und verarbeitet werden, sofern dies für das zu erbringende Ergebnis tatsächlich notwendig ist.

- Produkte werden nach dem Prinzip „Privacy by design“ entwickelt und betrieben
- Personenbezogene Daten werden zweckbezogen erhoben und verarbeitet
- Es erfolgt eine transparente und nachvollziehbare Verarbeitung personenbezogener Daten

Notfallmanagement

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass Datenschutzvorfälle erkannt, gemeldet und behoben werden können.

- Dokumentiertes Verfahren zur Erkennung und Meldung von Datenschutzvorfällen
- Unverzügliche Benachrichtigung des Auftraggebers bei Datenpannen gemäß Art. 33 Abs. 2 DSGVO
- Wiederherstellungsverfahren zur Sicherstellung der Verfügbarkeit personenbezogener Daten gemäß Art. 32 Abs. 1 lit. c DSGVO

Version: 2026-03-10