centron

Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Beschreibung der technischen und organisatorischen Maßnahmen
(Art. 32 Abs. 1 lit. d, Art. 15 Abs. 1 DSGVO)

August 2026

Allgemeine Maßnahmen

Auf Basis der **ISO 27001** wird ein **ISMS** betrieben:

Erstzertifizierung: 05.07.2026

Gültigkeitsdauer: 04.07.2029

TrustedCloud Zertifizierung: 14.06.2014

- Die Informationssicherheits-, IT-Nutzungs- und Datenschutzrichtlinie ist für alle Mitarbeiter im Zugriff und wird regelmäßig oder bei Bedarf aktualisiert
- Ein Datenschutzbeauftragter ist gestellt und der Geschäftsführung direkt unterstellt
- Ein Risikomanagement ist etabliert und berichtet an die Geschäftsführung
- Eine Notfallplanung und ein Wiederanlaufplan ist etabliert
- Ein Incidentmanagement-System ist etabliert
- Alle Mitarbeiter werden auf die Einhaltung des Datenschutzes und Verschwiegenheit verpflichtet

Vertraulichkeit

Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

- Zugangskontrollsystem
  - Türsicherung im Bürogebäude (elektrische Türöffner mit Zugriffprotokollierung sowie protokollierte Schlüsselvergabe gemäß Schlüsselmanagement).
  - Zusätzliche biometrische Zugangssicherung zum Rechenzentrum und elektronische Türsicherung zwecks zweistufiger Zutrittskontrolle.
- Einrichtung von Schutzzonen und Festlegung von Zutrittsregeln
- Besucherregelung
  - Protokollierung sämtlicher Besucher
  - Besuche und Lieferanten unterliegen in Abhängigkeit der Schutzzone einer durchgängigen Aufsicht.
- Rundum Videoüberwachung des Gebäude-Außenbereichs mit Sabotageerkennung und Aufzeichnung. Lückenlose Videoüberwachung des Rechenzentrum-Innenbereichs.
- Einbruchmeldeanlage mit Aufschaltung des Sicherheitsdienstes.

Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Erteilung von Berechtigungen nach dem Rollen- und Berechtigungskonzept nach Notwendigkeit
- Festlegung von Berechtigungen durch Leitung der Technik und Geschäftsführung
- Protokollierte Vergabe von Berechtigungen durch die Leitung der Technik
- Arbeitsplatz-PCs sind durch lokale Passwörter der Mitarbeiter geschützt
- Im Intranet werden Passwortrichtlinien durch MS-AD umgesetzt (u. a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)

- Die lokalen Systeme der Mitarbeiter werden regelmäßig bei Erscheinen von Updates aktualisiert
- Automatische Sperrung (z. B. Kennwort oder Pausenschaltung)
- Vorschaltung einer physikalischen Firewall mit IDS und IPS
- Einsatz von Virenscannern
- Physikalische Trennung von Netzwerken
- Überwachung des Netzwerktraffics

Zugriffskontrolle

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

- Die Passwortvergabe erfolgt ausschließlich durch berechtigtes Personal an vom Auftraggeber benannte Personen
- Die Weisungskommunikation erfolgt auf Seiten des Auftragnehmers über ein ITIL-konformes Ticketsystem
- Die Berechtigung zur Datenverarbeitung personenbezogener Daten werden durch das Active-Directory gesteuert und protokolliert
- Protokollierung der Logins auf den Systemen
- Vernichtung von Datenträgern gemäß Datenträgervernichtungskonzept
- Sofern der Kunde auf seinen Systemen personenbezogene Daten verarbeitet, ist der Kunde primär selbst für die Absicherung der Daten zuständig. Wird diese Zuständigkeit abgetreten, so sind die Sicherungsmechanismen vom Kunden in unregelmäßigen Abständen zu überprüfen und gegebenenfalls zu bemängeln.

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Sämtliche Daten können aufgrund der Art ihrer Speicherung getrennt voneinander verarbeitet werden
- Ausschließliche Verwendung von Software, die eine Mandantenfähigkeit bereitstellt
- Trennung der verarbeitenden Systeme
- Trennung der Systeme in Produktiv- und Testumgebung
- Kunden haben gegenseitig keinen Zugriff auf andere Kundensysteme

Integrität

Weitergabekontrolle

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

- Eine Weitergabe von personenbezogenen Daten erfolgt nur auf Verlangen von berechtigten Personen oder Institutionen
- Sofern eine Übertragung von personenbezogenen Daten an berechtigte Personen oder Institutionen stattfindet, erfolgt diese verschlüsselt, auf ausdrücklichen Kundenwunsch auch unverschlüsselt.

Datenträger, die personenbezogene Daten enthalten, werden bei einer Entsorgung des Datenträgers mehrfach durch unterschiedliche Löschmethoden bereinigt, anschließend wird der Datenträger zerstört und ordnungsgemäß entsorgt.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Systemaktivitäten durch ein Monitoringsystem
- Teilautomatisierte Auswertung von Logdateien
- Protokollierung aller Arbeiten in ITIL-konformem Ticketsystem
- Neue personenbezogene Daten können nur von berechtigten Personen eingegeben werden

Zugriffe auf das Datenverarbeitungssystem werden (siehe Punkt Zugriffskontrolle) protokolliert.

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- RAID (redundante Datenschreibung auf Festplatten)
- Sicherungskopien werden, falls durch Auftraggeber beauftragt, in Form von Backups gemäß Backupkonzept erstellt
- Rhythmus: täglich oder nach Kundenwunsch
- Aufbewahrungszeit: redundant, 1–5 Wochen oder nach Kundenwunsch
- Dateiformat: binär, proprietär verschlüsselt
- Aufbewahrungsort: Je nach Auftrag, dedizierte Storage- oder Serversysteme des Auftraggebers im eigenen oder fremden Rechenzentrum oder globale Storagesysteme des Auftragnehmers, welche wiederum interne Fehlertoleranz aufweisen und mit Zugangskontrollen versehen sind
- Je nach Auftrag durch den Auftraggeber: Konfiguration der Serversysteme mit Hardware-RAID (Spiegelung der Festplatten), redundante Netzteile
- Regelmäßige Prüfung der Backups auf Funktionalität
- Umsetzung von Disaster- und Recovery-Konzept, Notfallkonzept und Wiederanlaufplan

Rechenzentrum: Unterbrechungsfreie Stromversorgung (USV), Notstrom-Dieselanlage, redundante Klimaversorgung, Brandfrüherkennungsanlage, regelmäßige Brandbekämpfungsschulungen der Mitarbeiter.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement

- Jährliche Überprüfung der Risikoabschätzung für die Verarbeitung personenbezogener Daten
- Jährliche Prüfung der technischen und organisatorischen Maßnahmen auf Angemessenheit und Stand der Technik
- Führen eines zentralen Datenschutzmanagementsystems
- Regelmäßige interne Datenschutz-Audits
- Regelmäßige Schulungen und Sensibilisierungsmaßnahmen zu den Themen Datenschutz und Informationssicherheit

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle):

- Aufträge durch Kunden, die eine Verarbeitung von personenbezogenen Daten verlangen, werden in einem Ticketsystem protokolliert; für das Ticketsystem ist eine Zugriffskontrolle konfiguriert
- Aufträge sind elektronisch nur von verifizierten Kontaktadressen möglich (E-Mail und Fax)
- Aufträge sind ebenfalls per Post in Schriftform nur durch verifizierte Adressen möglich
- Personen, die Aufträge erteilen, müssen vom Vertragspartner für die Erteilung von Aufträgen autorisiert worden sein