Technisch- organisatorische Maßnahmen

der Ricoh Austria GmbH

Stand: April 2025

Die folgenden Technisch- organisatorische Maßnahmen der Ricoh Austria GmbH dienen dazu, personenbezogene Daten vor Verlust oder Zugriff durch unbefugte Personen zu schützen.

1. Pseudonymisierung und Verschlüsselung pers. Daten (Art. 32 Abs. 1 lit. a DS-GVO)

Pseudonymisierung

Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen.

- Pseudonymisierung in IT Systemen möglich über
  - Kundennummern
  - Personalnummern
- Bei Bedarf von Kunden bezüglich Pseudonymisierung von Kundendaten: Abfrage, Prüfung der technischen Machbarkeit und Umsetzung über das Kundenmanagement.

Verschlüsselung

Einsatz von Verfahren und Algorithmen, die personenbezogene Daten mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht lesbare Form umwandeln. Es kommen symmetrische und asymmetrische Verschlüsselungstechniken in Betracht:

- Verschlüsselte Speicherbereiche
- Regelungen zu kryptographischen Maßnahmen

2. Maßnahmen zur Sicherstellung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

- Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere zur Legitimation der Berechtigten:
- Grundregeln für das Verhalten in Betriebsgebäuden & Besucherregelung
- Besucheranmeldung
- Besucherverpflichtung - bzgl. Geheimhaltung und sichtbar zu tragenden Besucherausweis. Zusätzlich Begleitung durch Ricoh Mitarbeiter
- Verschlossene Türen
- Definierter Schlüsselvergabeprozess und -dokumentation

- Zutrittskontrollsysteme mit Identifikationskarte
- Regelmäßige Kontrollen der Zutrittsrechte
- Sicherheitsbereiche nur für autorisiertes Personal (IT, HR) über Schlüssel zugänglich.
- Serverraum: Keine Fenster oder Schächte vorhanden

Zugangskontrolle

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammdatensatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Eintritts-, Versetzungs- und Austrittsprozess
- Laptop: Zugang mit Benutzername und Passwort
- Zusätzlich Festplattenverschlüsselung
- Ultra Thin-Clients: Zugang mit SmartCard und zusätzlich Benutzername und Passwort
- Passwortverfahren mit festgelegten Komplexitätsanforderungen:
    - mind. 8 Zeichen
    - 3 von 4: Groß-/Kleinschreibung, Zahlen, Sonderzeichen
    - Wechsel nach 42 Tagen
    - Passworthistorie (letzte 24 nicht möglich)
    - Sperrung des Accounts nach 3 fehlgeschlagenen Anmeldeversuchen
    - keine unpersonalisierten Sammel-Accounts („Azubi1“)
- Automatische Bildschirm-Sperrung nach 15 Minuten
- Zugang zum Unternehmensnetz nur über VPN
- Regelmäßige Prüfungen der Zugangsrechte zum Netzwerk

Zugriffskontrolle

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Berechtigungskonzept
- Regelmäßige Kontrollen von Berechtigungen
- Genehmigungsprozess für Rechtevergabe
- Logging

Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Definierter Prozess zur Speicherung von Kundendaten
- Logisch getrennte Speicherbereiche für Daten verschiedener Kunden
- Getrennte Datenbanken [1)]
- Verschlüsselte Speicherbereiche
- Zugriffsregelung

- Regelmäßige Kontrolle spez. Zugriffsrechte
- Trennung von Entwicklungs- & Testsystemen von Produktivsystemen

3. Maßnahmen zur Sicherstellung der Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Klassifizierung von Informationen
- Unternehmensweite Handhabungsregeln zu den Kennzeichnungsklassen incl. Datenträgervernichtung
- Verpflichtung aller Mitarbeiter auf die Vertraulichkeit
- Datenschutz und ISMS Unterweisungen
- Ablage der erhaltenen Kundendaten über einen automatisierten Prozess in speziellem Verzeichnis. Zugriff nur für berechtigte Mitarbeiter.
- Keine USB-Schnittstellen an Ultra Thin-Clients. Keine Möglichkeit, Daten auf Datenträger zu kopieren
- Verpflichtung aller Besucher auf Geheimhaltung und keine Mitnahme und Weitergabe von Dokumenten, Datenträgern, etc.
- Vernichtung von nicht mehr benötigten physischen Dokumenten über die Reisswolf Österreich GmbH (Akten- und Dokumentencontainer)

Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Lediglich Mitarbeiter, die berechtigt sind, können Daten erheben, verarbeiten oder nutzen
- Auftragsbezogene Protokolle bzgl. Tätigkeiten mit von Kunden gelieferten Daten
- Die Ricoh Austria GmbH führt Änderungen von Kundendaten nur vor, sofern dies schriftlich vom Kunden angewiesen wird.

4. Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 lit. b DS-GVO)

Verfügbarkeitskontrolle

Maßnahmen zur Datensicherung (physikalisch / logisch):

- Definierte Backupstrategie
- BCM-Konzept zur Gewährleistung der Produktion auch in eintretenden Katastrophenfällen
- Regelmäßige Wiederherstellungstests
- Brandfrüherkennungsanlage im Serverraum

Verfügbarkeit der eingesetzten IT-Systeme

- Live Monitoring
- Zentral gemanagtes Antivirus-System, regelmäßige Aktualisierung von Antiviruspattern
- Antispam System
- Schwachstellenmanagement
- Firewalls, DMZ, Proxy
- Risikobewertung

5. Maßnahmen zur Wiederherstellung der Verfügbarkeit und dem Zugang zu pers. Daten bei einem technischen Zwischenfall (Art. 32 lit. c DS-GVO)

Recovery / Backup-Systeme

- Business Continuity Plan nach ISO 27001
- Regelm. Wiederherstellungstests
- Disaster Recovery Strategie für Rechenzentren

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technisch-organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DS-GVO; Art 25. Abs. 1 DS-GVO)

Datenschutzmanagement

- Zertifizierung nach ISO 9001, 14001 und 27001 durch die Zertifizierungsstelle SGS
- Datenschutzmanagementsystem als gemeinsames System im integrierten Managementsystem
- Interne Audits zum integrierten Managementsystem
- Lenkung von Dokumentationen, wie Arbeitsanweisungen, Tätigkeitsbeschreibungen, Richtlinien, Merkblättern
- Keine Verträge oder Kooperationen mit Drittländern
- Datenschutzmanager

Auftragskontrolle

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen AUFTRAGGEBER und AUFTRAGNEHMER:

- Vertragliche Regelungen mit Subunternehmen
- Eindeutige Vertragsgestaltung
- Schriftliche Beauftragung
- Vertraulichkeitsvereinbarungen
- Vereinbarungen zur Auftragsvereinbarung
- Prozess zur Lieferantenbewertung