Technische und organisatorische Massnahmen (TOM) namentlich basierend auf Art. 3 Datenschutzverordnung (DSV)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Bearbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen die Verantwortliche und die Auftragsbearbeiterin geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. Pseudonymisierung und Verschlüsselung pers. Daten

Pseudonymisierung

Die Bearbeitung personenbezogener Daten erfolgt 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 über
  - Kundennummern;
  - Personalnummern.

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

Zugangskontrolle

Technische bzw. organisatorische Massnahmen zur Zugangskontrolle, insbesondere zur Legitimation der Berechtigten. Es sollen nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden:

- Grundregeln für das Verhalten in Betriebsgebäuden & Besucherregelung;
- Zutritt für Betriebsfremde nur mit personalisierter Anmeldung;
- Zutrittskontrollsysteme mit Identifikationskarte;
- Regelmässige Kontrollen der Zutrittsrechte von Sicherheitsbereichen;
- Einbruchmeldetechnik;
- Videoüberwachung mit Aufzeichnung;
- Wach- und Schliessgesellschaft.

Benutzerkontrolle

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammdatensatz) Massnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung. Es ist unbegfugten Personen zu verunmöglichen, automatisierte Datenbearbeiterungssysteme mittels Einrichtungen zur Datenübertragung benutzen zu können:

- Eintritts-, Versetzungs- und Austrittsprozess;
- Informationssystem zum User Provisioning;
- Passwortverfahren mit zentral festgelegten Komplexitätsanforderungen;
- Unternehmensweite Passwortpolicy;
- Monitoring;
- Automatische Sperrung;
- VPN;
- Regelmässige Prüfungen der Zugangsrechte zum Netzwerk.

Zugriffskontrolle

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung. Berechtigte Personen sollen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen:

- Berechtigungskonzept;
- Regelmässige Aktualisierung der Standardrechte;
- Genehmigungsprozess für Sonderrechte;
- Informationssystem zur Rechtevergabe;
- Regelmässige Kontrollen von Berechtigungen von definierten Systemen;
- Logging.

Trennungskontrolle

Massnahmen zur getrennten Bearbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Mandantentrennung;
- Getrennte Datenbanken;
- Verschlüsselte Speicherbereiche;
- Zugriffsregelung;
- Regelmässige Kontrolle spez. Zugriffsrechte;
- Trennung von Entwicklungs- & Testsystemen von Produktivsystemen.

3. Verfügbarkeit, Integrität und Belastbarkeit der Systeme und Dienste

Grundsätze zur Verfügbarkeit, Zuverlässigkeit und Datenintegrität

Es sind geeignete Massnahmen zu treffen, damit alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen, Fehlfunktionen gemeldet werden und gespeicherte Personendaten nicht durch Fehlfunktionieren des Systems beschädigt werden können.

Datenträgerkontrolle

Es sind geeignete Massnahmen zu treffen, damit unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können.

Speicherkontrolle

Es sind geeignete Massnahmen zu treffen, damit unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können.

Transportkontrolle

Es sind geeignete Massnahmen zu treffen, damit unbefugte Personen bei der Bekanntgabe von Perosonendaten oder beim Transport vom Datenträgern Personendaten nicht lesen, kopien, verändern, löschen oder vernichten können.

Verfügbarkeitskontrolle

Massnahmen zur Datensicherung (physikalisch / logisch):

- Definierte Backupstrategie;
- Schattenkopien;
- VM-Snapshots;
- Aufbewahrung von Sicherungen in zertifizierten, brandgeschützten Tresoren;
- Brandfrüherkennungsanlage und Löschanlage;

Verfügbarkeit der eingesetzten IT-Systeme

- Live Monitoring;
- Antivirus;
- Antispam;
- USV für RZ;
- Schwachstellenmanagement;
- Firewalls, DMZ, Proxy;
- Risikobewertung.

Systemsicherheit

Es sind geeignete Massnahmen zu treffen, damit Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden können.

4. Massnahmen zur Wiederherstellung der Verfügbarkeit und dem Zugang zu pers. Daten bei einem technischen Zwischenfall

Es gilt sicherzustellungen, dass die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können:

Recovery / Backup-Systeme

- Business Continuity Plan nach ISO 27001;
- Regelm. Wiederherstellungstests;
- DR-Strategie für RZ.

5. Massnahmen zur Sicherstellung der Nachvollziehbarkeit

Bekanntgabekontrolle

Massnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung. Es muss überprüft werden können, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden:

- VPN;
- MPLS;
- Klassifizierung von Informationen;
- Unternehmensweite Handhabungsregeln zu den Kennzeichnungsklassen incl. Datenträgervernichtung;
- Regelungen zu kryptographischen Massnahmen;
- Verpflichtung auf das Datengeheimnis für alle Mitarbeiter;
- ISMS Unterweisungen.

Eingabekontrolle

Massnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind. Es muss überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden:

- Protokollierung spezifischer Systeme;
- Session Logs;
- Aktuelle Systemzeit durch Synchronisation mit Timeserver.

Erkennung und Beseitigung

Es sind geeignete Massnahmen zu treffen, um Verletzungen der Datensicherheit rasch erkennen und zur Minderung bzw. Beseitigung allfälliger eintretender Folgen ergreifen zu können.

6. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der technisch-organisatorischen Massnahmen

Datenschutzmanagement

- Internationale Zertifizierung der RICOH Landesgesellschaften nach ISO 9001, 14001, ISO 27001;
- durch die Zertifizierungsgesellschaft SGS;
- Internes Kontrollsystem zur J-SOx Compliance;
- Interne Audits zum integrierten Managementsystem an allen Standorten.

Datenschutzfreundliche Voreinstellungen (Privacy by Default)

- Durch europäisches Datenschutzkonzept für Produkte sichergestellt;
- Unterschiedliche Sicherheitseinstellungen und Features für alle Produkte benutzerseitig auswählbar.

Auftragskontrolle

Massnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Verantwortliche und Auftragsbearbeiterin:

- Vertragliche Regelungen mit Subunternehmen;
- Eindeutige Vertragsgestaltung;
- Schriftliche Beauftragung;
- Vertraulichkeitsvereinbarungen;
- Vereinbarungen zur Auftragsdatenvereinbarung;
- Prozess zur Lieferantenbewertung;
- Lieferantenaudits.