Allgemeine technische und organisatorische Maßnahmen (TOMs)

Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DS-GVO)

a) Zutrittskontrolle

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.

Maßnahmen:

- Besucher müssen sich am Empfang anmelden
- Pförtner, Zutrittsprotokollierung für Besucher und Fahrzeuge (außerhalb Geschäftszeiten)
- Gekennzeichnete Videoüberwachung (ohne Speicherung)
- Raumsicherung Rechenzentren: Schließanlage (Zutrittsregelung), Zutrittskontrolle über Transponder + PIN mit zentraler Protokollierung, keine Außenfenster
- Personal von Fremdfirmen ist der Zutritt zu Wartungszwecken nur in Begleitung gestattet

b) Zugangskontrolle

Eine unbefugte Systemnutzung ist zu verhindern.

Maßnahmen:

- Starke Kennwörter, die in regelmäßigem Turnus gewechselt werden, Passwortgenerator, One-Time-Secret zur Passwortübermittlung
- Automatische Bildschirmsperren
- Benutzerbezogene Zugänge
- Umsetzung von Benutzerrechte und Berechtigungsprofilen
- Verschlüsselung von Datenträgern bei hohem Schutzbedarf
- Verschlüsselung von Mobilgeräten
- Einsatz von VPN-Technolgie
- Einsatz von SSL-Verschlüsselung und Zertifikaten
- Einsatz eines Intrusion-Prevention-Systems (IPS)
- Einsatz von Hard- und Softwarefirewalls
- DMZ-Architektur

c) Zugriffskontrolle / Benutzerkontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein.

Maßnahmen:

- Zugriffsberechtigungskonzept, Zugriffsmöglichkeiten werden nach dem „Need to know"-Prinzip beschränkt.
- Verbot der Passwortweitergabe
- Rechteverwaltung durch spezielle Administratoraccounts
- Protokollierung von Zugriffen
- Sperrung von Konten nach max. erlaubter Anzahl von Fehlversuchen

- Auditierung von Dateisystemrechten und Benutzeraccounts
- Zertifizierte Datenträgervernichtung

d) Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden.

Maßnahmen:

- Trennung personenbezogener Daten des Auftraggebers von personenbezogenen Daten des Auftragnehmers durch Mandanten-/Account-abhängige Verwaltung
- Jeder Account hat über Benutzername und Passwort nur Zugriff auf ihm zugeordnete Daten. Für unterschiedliche Anwendungen gibt es separate Verzeichnisstrukturen, deren Verwaltung ebenfalls sicherstellt, dass nur berechtigte Zugriffe erfolgen können.
- Zweckgebundene Zugänge in Datenbanken
- Getrennte Produktions- und Testumgebungen
- Weitergehende Maßnahmen sind im Hauptvertrag zu regeln.

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DS-GVO, Art. 25 Abs. 1 EU-DS-GVO)

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

Maßnahmen:

- Pseudonymisierung von Protokolldateien oder sonstigen Daten erfolgt in Abstimmung / nach Zustimmung des Kunden nach dessen Auftrag

2. Integrität (Art. 32 Abs. 1 lit. b EU-DS-GVO)

a) Weitergabekontrolle / Übertragungskontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

Maßnahmen:

- Passwortschutz bei sensitiven Anhängen
- Passwortgeschützte, verschlüsselte Übertragung über betriebseigenen Cloudstorage
- Verschlüsselung von Datenträgern bei hohem Schutzbedarf
- Verschlüsselung von Mobilgeräten
- Einsatz von VPN-Technolgie
- Einsatz von SSL-Verschlüsselung (HTTPS/SFTP)
- Auswertbare Protokollierung von Übertragungen
- Benutzung sicherer Transportbehälter
- Datenschutzgerechte Entsorgung von Medien
- Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind schriftlich zur Verschwiegenheit verpflichtet.

b) Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- Protokollierung in Logfiles und zentrales Repository
- Bei Fernwartungen hat die Protokollierung auf der Auftraggeberseite zu geschehen.

3. Verfügbarkeit und Belastbarkeit / Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b EU-DS-GVO)

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

Maßnahmen:

- Backup-Strategie mit Offsite-Kopie
- Rasche Wiederherstellbarkeit über Restores auf VM-Ebene
- Getrennte Rechnerräume
- USV und Generator, A/B-Stromzuführungen an Racks
- Rauchverbot im Gebäude, Brandmelde- und automatische Löschanlage
- Raid-Sicherheit und Storage-Replikation
- Firewalls und UTM Viren-/Malwareschutz
- Redundanzen in Hardware und Leitungswegen
- Meldewege und Notfallszenarien

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DS-GVO, Art. 25 Abs. 1 EU-DS-GVO)

a) Datenschutz-Management

Maßnahmen:

- Zuweisung von Zuständigkeiten
- Risikobewertung
- Durchführung von Kontrollen
- Sensibilisierung und Schulung der Mitarbeiter
- Einheitliche Verfahrensdokumentation (VVT)
- Weisungen und Ausgeführte Tätigkeiten im Rahmen einer Auftragsverarbeitung werden kundenbezogen dokumentiert
- Bei Bedarf Durchführung von Datenschutz-Folgeabschätzungen
- Datenschutz-Management-System

Es gelten die Grundsätze:

- Datenschutz ist Aufgabe des gesamten Unternehmens.
- Es werden datenschutzfreundliche Technologien und Prozesse eingesetzt, wo immer das möglich und wirtschaftlich ist.

- Die IT-Sicherheit muss auf dem aktuellen Stand der Technik sein.

b) Incident-Response-Management

Maßnahmen:

- Es bestehen interne Richtlinien, Handlungsanweisungen und Prozesse zum Datenschutz, die bei Bedarf oder sich ändernden Voraussetzungen erweitert bzw. ergänzt werden.

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DS-GVO)

Maßnahmen:

- Prozess für Vorabkontrolle und im Bedarfsfall Datenschutzfolgeabschätzung bei neuen / geänderten Verfahrensweisen oder Einführung neuer technischer Systeme
- Customizing von eingesetzten Applikation nach den Grundsätzen „Privacy by Default“

d) Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers

Maßnahmen:

- Im Rahmen der Geschäftsprozesse liegt es in der Verantwortung der Führungskräfte, in deren Aufgabenbereich die jeweiligen datenschutzrelevanten Dienstleistungen fallen, sicherzustellen, dass personenbezogene Daten nur entsprechend der Weisungen der Auftraggeber (grundsätzlich schriftlich vereinbart) und in Einklang mit den geltenden Rechtsvorschriften verarbeitet werden.
- Ergänzend stellt der betriebliche Datenschutzbeauftragte sicher, dass der Auftragskontrolle genüge getan wird
- Abschluss schriftlicher Vereinbarungen zur Auftragsverarbeitung gemäß Art. 28 DS-GVO mit Regelungen zum Auftragsablauf.
- Eindeutige Vertragsgestaltung mit Regelung der Zuständigkeiten und Verantwortlichkeiten sowie zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- Sorgfältige Auswahl von Lieferanten und Unterauftragnehmern. Die angemessene Etablierung und die Einhaltung eines Datenschutz-Managements sind – nach Möglichkeit – durch die Einhaltung von Verhaltensregeln und / oder Zertifizierungen nachzuweisen.
- Regelmäßige Schulung und Weiterbildung der Mitarbeiter in Datenschutz-Themen zur Sicherstellung der Einhaltung von Datenschutzvorschriften und Einhaltung bestehender Weisungen.
- Prüfung der vereinbarten Regelungen durch den Datenschutzbeauftragten.