Technische und organisatorische Maßnahmen beim Auftragnehmer

Die hier beschriebenen technischen und organisatorischen Maßnahmen (entsprechend Art. 32 DSGVO) gelten als Mindest-Standard und dürfen nicht unterschritten werden.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

a) Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass unbefugte Personen Zutritt zu den Datenverarbeitungsanlagen haben:

- Geschlossene Türen
- Sicherheitsschloss
- Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- Überwachung der Zu- und Abgänge durch entsprechende technische Vorkehrungen

b) Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass unbefugte Personen Zugang zu den Datenverarbeitungssystemen haben:

- Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- Anti-Virus-Software Clients
- Firewall
- Einsatz VPN bei Remote Zugriffen
- Verschlüsselung von Datenträgern
- BIOS Schutz (separates Passwort)
- Sperre externer Schnittstellen
- Automatische Desktopsperre
- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Zentrale Passwortvergabe

c) Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Need-to-know Prinzip
- Verwaltung der Benutzerrechte durch Systemadministrator
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten

d) Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung (Systeme/Datenbanken/Datenträger)
- Mandantenfähigkeit relevanter Anwendungen
- Festlegen von Datenbankrechten

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

a) Weitergabe- und Eingabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Verschlüsselung von E-Mail bzw.- E-Mail-Anhängen (z.B. PGP, WinZip) oder gesicherter File-Transfer (z.B. SFTP)
- Einsatz von VPN
- Nutzung von Signaturverfahren
- Protokollierung der Zugriffe und Abrufe
- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle oder automatisierte Kontrolle der Protokolle
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit

(Art. 32 Abs. 1 lit. b DSGVO)

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- Hochverfügbare Anwendungs- und Datenbankcluster
- Verfahren für Datensicherungen
- Sicherung der Daten an verschiedenen Standorten
- Kontrolle des Sicherungsvorgangs
- Aufbewahrungsprozess für Datensicherungen
- Bedarfsgerechtes Einspielen von Sicherheits-Updates
- Virenschutz und regelmäßige Aktualisierung
- Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfiltern und regelmäßige Aktualisierung
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten
- Einsatz von USVs

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Folgende Maßnahmen zur regelmäßigen Evaluation der Wirksamkeit sind beim Auftragnehmer umgesetzt:

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- Einsatz eines externen Datenschutzbeauftragten
- Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- Das Unternehmen kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)