Allgemeine technische und organisatorische Maßnahmen nach Artikel 28, 32 DSGVO

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

Zutritts-/Zugangskontrolle
Durch nachstehende Maßnahmen verwehren wir Unbefugten den Zutritt zu den Geschäftsräumen:

- Zutrittskontrollsystem (Codekarte)
- Schlüsselberechtigungssystem für sensible Bereiche (Datenverarbeitung, Personaldaten)
- Türsicherung über verschiedene Schließkreise
- Schlüsselregelung (Ausgabe von Schlüsseln)
- Überwachungseinrichtung (Alarmanlage, Kameras)
- Sicherheitsverglasung
- Protokollierung Besuche Externer (Besucherliste und -ausweise)
- Serverräume gesondert gesichert, Zutritt nur durch autorisierte Personen
- Videoüberwachung der Zugänge

Das Eindringen in die DV-Systeme wird verhindert. Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Kennwortverfahren
- Automatische Sperrung
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern
- Verschlüsselung von Datenträgern in Laptops/Notebooks
- Festplattenverschlüsselung bei mobilen Rechnern
- Firewall
- Einsatz von Anti-Viren-Software/Spam-Filtern

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden verhindert. Bedarfsorientierte Ausgestaltung des Berechtigungskonzeptes und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Kennwortverfahren
- Datenträgerverwaltung
- Protokollierung Systemzugriffe
- Einsatz von Dienstleistern zur Aktenvernichtung
- ordnungsgemäße Vernichtung von Datenträgern

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

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

- Verschlüsselung/Tunnelverbindung (VPN=Virtual Private Network)
- Beim physischen Transport: Sichere Transportbehälter/-verpackungen
- Regelung für den Transport von Datenträgern
- Verschlüsselung von USB Sticks
- Übertragungsweg bei E-Mail-Versand wird mit TLS verschlüsselt, wenn Empfänger TLS aktiviert hat
- Verschlüsselung von E-Mails und deren Anhängen
- Papierunterlagen mit personenbezogenen Daten werden von Spezialfirmen entsorgt
- Datenträger werden qualifiziert vernichtet, Festplatten gelöscht

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird durch Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, gewährleistet:

- Protokollierungs- und Protokollauswertungssystematiken
- Benutzeridentifikation
- Archivierung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- 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)

Die Daten werden gegen zufällige Zerstörung oder Verlust mittels Maßnahmen zur Datensicherung (physikalisch/logisch) geschützt:

- Backup-Verfahren
- Spiegeln von Festplatten
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung von Datensicherungen
- Datensicherungen auf Festplatten und spiegeln dieser ins Ausfallrechenzentrum
- Virenschutz / Firewall
- Notfallplan
- Feuerlöscher und Brandmeldeanlage
- Externes Ausweichrechenzentrum für Notfälle
- Überspannungsschutz
- Klimaanlage in Serverräumen
- Regelmäßige Penetrationstests der eigenen IT-Systeme

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden auch getrennt verarbeitet. Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Interne Mandantenfähigkeit
- Funktionstrennung Produktion/Test mit getrennten Datenbanken

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DGVO, Art. 25 Abs 1 DSGVO)

Datenschutzmanagement

- Es wurde eine Datenschutzbeauftragte bestellt
- Alle Mitarbeiter wurden auf die Einhaltung datenschutzrechtlicher Vorschriften sowie auf ihre Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse verpflichtet
- Die Mitarbeiter werden durch regelmäßige Schulungen und andere Informationen zum Datenschutzrecht für das Thema sensibilisiert
- Interne Verhaltensrichtlinien
- Regelmäßige Überprüfung der TOM's
- Meldeprozess für Datenschutzverletzungen
- Durchführung von Datenschutzfolgeabschätzungen soweit erforderlich
- Dokumente werden in unserem sicheren Kundenportal zur Verfügung gestellt

Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung wird durch folgende Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer gewährleistet:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung
- Kontrolle der Vertragsausführung

Stand: September 2022