Stand 25.10.2018

Allgemeine technische und organisatorische Maßnahmen nach Artikel 28, 32 DSGVO

1. Zutrittskontrolle

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)
- Gesonderte Sicherung des Rechenzentrums
- Serverräume gesondert gesichert, Zutritt nur durch autorisierte Personen
- Videoüberwachung der Zugänge

2. Zugangskontrolle

Das Eindringen Unbefugter 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

3. Zugriffskontrolle

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

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten werden geregelt. Maßnahmen bei 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
- eigene Cloudlösung
- Papierunterlagen mit personenbezogenen Daten werden von Spezialfirmen entsorgt
- Datenträger werden qualifiziert vernichtet, Festplatten gelöscht

5. Eingabekontrolle

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

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung wird durch folgende Maßnahmen (technisch/organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer gewährleistet:

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

7. Verfügbarkeitskontrolle

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
- Externe Lagerung von Datensicherungen
- Virenschutz / Firewall
- Notfallplan
- Feuerlöscher und Brandmeldeanlage
- Externes Ausweichrechenzentrum für Notfälle
- Überspannungsschutz
- Klimaanlage in Serverräumen

8. Trennungskontrolle

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 sowie aktuellen Verschlüsselungsverfahren

9. 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

10. Maßnahmen zur Belastbarkeit der IT-Systeme

- Regelmäßige Penetrationstests der eigenen IT-Systeme

11. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM's zur Gewährleistung der Sicherheit der Verarbeitung

- Interne Verhaltensrichtlinien
- Regelmäßige Überprüfung der TOM's
- Meldeprozess für Datenschutzverletzungen
- Durchführung von Datenschutzfolgeabschätzungen soweit erforderlich