Technisch-organisatorische Maßnahmen

Stand: 04.06.2020

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

Zutrittskontrolle
- Der Zugang zu den Räumlichkeiten, in denen sich Datenverarbeitungsanlagen befinden, wird effektiv gegen Unbefugte geschützt. Zutrittsrechte werden restriktiv und abhängig von der Rolle eines bestimmten Mitarbeiters vergeben. Jeder Mitarbeiter erhält nur diejenigen Zutrittsrechte, die er zur Erfüllung seiner betrieblichen Aufgaben benötigt.
- Besucher, Handwerker und andere fremde Personen dürfen sich nicht frei und unkontrolliert im Gebäude bewegen.
- Bereiche, in denen hoch vertrauliche Informationen verarbeitet werden, sind besonders zu sichern. Nur berechtigte, namentlich benannte Personen haben Zutritt zu diesen Bereichen.
- Die Authentisierung der Zugangsberechtigung erfolgt durch ein elektronisches Zugangskartensystem.
- Serverräume unterliegen besonders hohen Zutrittsbeschränkungen, mit separaten PIN Codes, zusätzlich zum üblichen elektronischen Zugangskartensystem.
- Werkschutz
- Videoüberwachung

Zugangskontrolle
- Der Zugang zu Datenverarbeitungssystemen wird durch Passwörter geschützt.
- Es wird sichergestellt, dass Passwörter in regelmäßigen Abständen (alle 90 Tage) geändert werden und Mindestanforderungen an ihre Komplexität erfüllen müssen (mindestens 8 Zeichen und Verwendung von mindestens drei der vier genannten Zeichen: Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen).
- Die Einräumungen von Zugangsberechtigungen sind durch Vorgesetzte zu autorisieren und zu überwachen.
- Externe Zugriffsmöglichkeiten auf die Datenverarbeitungssysteme werden restriktiv und unter strenger Überwachung gewährt, und zwar nur über gesicherte VPN-Gateways, Firewalls.
- Die Netz- und Computersicherheit vor unbefugten Zugriffen wird durch Next-Generation Firewall-Systeme, VPNs und tagesaktuelle Virenschutzsoftware gewährleistet.
- Der Zugang der Administratoren auf die IT-Systeme und den Serverraum wird speziell gesichert.
- Automatische Bildschirmsperre bei längerer Inaktivität.

Zugriffskontrolle
- Der Zugriff auf (sensible) Daten in Applikationen, Datenbanken und Dateien wird durch Benutzer- und Berechtigungsmanagement abgesichert (Passwörter, Active Directory und NTFS-Permissions) abgesichert.
- Es wird sichergestellt, dass Zugriffsrechte für externe Wartungstechniker auf das notwendige Minimum reduziert sind.

Trennungskontrolle
- Datensätze verschiedener Mandanten werden in logisch oder physikalisch getrennten Datenbanken gespeichert.
- Trennung von Test- und Produktionsdaten.

Pseudonymisierung und Verschlüsselung
- Trennung von Kundendaten und Auftragsdaten
- Es wird sichergestellt, dass Daten nur übermittelt bzw. versendet werden, wenn eine ausreichende Verschlüsselung gewährleistet ist. (Übertragung via sftp)
- E-Mails werden bei Bedarf Ende-zu-Ende verschlüsselt.
- Verschlüsselung von Datenträgern

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

Weitergabekontrolle
- Es wird sichergestellt, dass Daten nur übermittelt bzw. versendet werden, wenn eine ausreichende Verschlüsselung gewährleistet ist.
- E-Mails werden bei Bedarf Ende-zu-Ende verschlüsselt.

Eingabekontrolle
- An- und Abmeldevorgänge sowie Löschvorgänge an Systemen werden protokolliert.
- Administrator-Aktivitäten werden protokolliert.

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

Verfügbarkeitskontrolle
- Es wird sichergestellt, dass die IT-Systeme über eine unterbrechungsfreie Stromversorgung (USV) verfügen.
- Für alle geschäftskritischen Systeme wird redundante Hardware eingesetzt.
- Sämtliche betroffenen Wartungsverträge enthalten kurzfristige Reaktionszeiten für Störungsbeseitigungen.
- Es existiert ein Backup-Konzept und ein Desaster Recovery Plan.

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

Auftragskontrolle
- Qualitäts-, Datenschutz- und Informationssicherheitsmanagement
- Es wird sichergestellt, dass die Identität des Auftraggebers und seiner Mitarbeiter sowie deren Vertretungsbefugnis bei der Entgegennahme von Aufträgen und Weisungen geprüft wird.
- In Verträgen werden alle Aufgaben, Pflichten und Weisungen von Auftragnehmer und Auftraggeber schriftlich vereinbart.
- Kontrolle der Arbeitsergebnisse
- Schulung der Mitarbeiter
- Verpflichtung der Mitarbeiter auf das Datengeheimnis und Vertraulichkeit