Anlage 1

Allgemeine technische und organisatorische Maßnahmen

Stand 27. März 2018

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

a) Zutrittskontrolle

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.

Maßnahme:
Zutrittskontrollsystem mit persönlicher Chipkarte, Schlüssel/Schlüsselvergabe

b) Zugangskontrolle

Eine unbefugte Systemnutzung ist zu verhindern.

Maßnahme:
Firewalls, VPN-Tunnel mit AES-Verschlüsselung, Kennwortverfahren / Passwortschutz, Verschlüsselung von Datenträgern

c) Zugriffskontrolle / Benutzerkontrolle

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

Maßnahme:
Differenzierte Berechtigungen je nach Aufgabenbereich bzw. Person, Protokollierung von Zugriffen, wesentliche Kundendaten sind unabhängig von IT-Zugriffsrechten individuell mandantenabhängig verschlüsselt bzw. getrennt gespeichert

d) Trennungskontrolle

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

Maßnahme:
Mandantenfähigkeit / Zweckbindung, Funktionstrennung Produktion / Test

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.

Maßnahme:
Aggregierte Speicherung von Auswertungen (Anonymisierung), Speicherung von Datensatzteilen mit unterschiedlichen Schlüsseln (Pseudonymisierung)

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.

Maßnahme:
Datenverschlüsselung, VPN-Tunnel mit differenzierten Zugriffsberechtigungen, Protokollierung

b) Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

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

Maßnahme:
Protokollierungen, Mail-Archivierung von AV-Aufträgen

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

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

Maßnahme:
RAID-Systeme, zusätzliche Spiegelung von Datenclustern, Backup-Verfahren mit rascher Wiederherstellbarkeit (Art.32 Abs.1 lit.c EU-DS-GVO), Getrennte Aufbewahrung, Unterbrechungsfreie Stromversorgung (USV), Notfallplan

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

Maßnahme:
Datenschutzverfahren, Internes Kontroll System (IKS)

b) Incident-Response-Management

Maßnahme:
Incident Response Plan (IRP)

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

Datenvermeidung, begrenzte Speicherfrist, personenabhängige begrenzte Zugänglichkeit

d) Auftragskontrolle

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

Maßnahme:
Formalisiertes Auftragsmanagement, Vorabüberzeugungspflicht, Nachkontrollen