Anlage 3– Technisch-organisatorische Maßnahmen

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

1.1. Zutrittskontrolle

Mit dem Begriff „Zutritt“ ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT-Systeme (z.B. Rechenzentren, Applikationsserver, Datenbanken, Speichersysteme o.ä.) betrieben werden.

Der Zutritt wird durch die nachfolgenden Vorkehrungen überwacht und sichergestellt:

- Automatisches Zugangskontrollsystem mit Transponder-/Chip-Karten
- Alarm- und Brandmeldeanlage
- Schließsystem mit Codesperre
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser mit Schlüsselregelung in zutrittsbeschränkten Räumen (protokollierte Schlüsselausgabe)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal

1.2 Zugangskontrolle

Die Zugangskontrolle hindert Unbefugte an der Benutzung der IT-Systeme in denen personenbezogene Daten gespeichert oder verarbeitet werden.

Hierfür werden Maßnahmen wie folgt ergriffen:

- Erstellen von Benutzerprofilen für Mitarbeiter
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Zuordnung von Benutzerrechten zu berechtigten Profilen
- Passwortvergabe Regeln für komplexe und nicht wiederkehrende Passwörter
- Einfache Authentifikation mit Benutzername / Passwort bei einfachem bis mittlerem Schutzniveau
- Zwei-Faktor-Authentifizierung ab hohem Schutzniveau
- Automatische Zugangssperre der Arbeitsstation nach fünf Minuten Inaktivität Manuelle Zugangssperrung durch Mitarbeiter bei vorübergehendem Verlassen des Arbeitsplatzes
- Sperre von externen Schnittstellen (USB u.ä.)
- Schlüsselregelung für IT-Schränke u.ä. (Schlüsselausgabe und Protokollierung in anderer organisatorischen Abteilung)
- Einsatz von Intrusion-Detection-Systemen

- Einsatz von zentraler Smartphone-Administrations-Software
- Einsatz von Anti-Viren-Software
- Verschlüsselung aller Datenträgern
- Einsatz einer Hardware-Firewall
- Bei allen mobilen Arbeitsplätzen zusätzlicher Einsatz von VPN-Technologie und Einsatz einer lokalen Software-Firewall

1.3 Zugriffskontrolle

Die die Zugriffskontrolle ist darauf ausgerichtet sicher zu stellen, dass durch Berechtigte auf ausschlie0lich diejenigen Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht, sowie Daten nicht durch Unbefugte manipuliert oder gelesen werden können.

Die folgenden Maßnahmen werden hierfür genutzt:

- Verwendung eines Berechtigungskonzepts mit Rollen und Benutzergruppen
- Verwaltung der Rechte durch wenige ausgewählte Systemadministratoren
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung aller Datenträgern
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Akten und Datenträgern nach DIN 66399 über den Dienstleister documentus GmbH
- Protokollierung der Vernichtung von Akten und Datenträgern

1.4 Trennungskontrolle

Mittels der Trennungskontrolle wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten auch getrennt verarbeitet werden können.

Zur Sicherstellung werden Schritte wie folgt eingesetzt:

- Trennung von Produktiv- und Testsystemen
- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- logische Mandantentrennung softwareseitig innerhalb eines Systems
- Verwendung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Speicherung von pseudonymisierten Daten
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

1.5 Pseudonymisierung

(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten geschieht in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.
Verkehrsdaten werden nicht direkt für einer spezifischen betroffenen Person erfasst, sondern für ein Benutzerkonto / Buchungskonto.
Eine Zuordnung Buchungskonto zu spezifisch betroffener Person gelingt, indem diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

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

2.1 Weitergabe Kontrolle

Die Weitergabe Kontrolle stellt sicher, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport auftritt. Die nachstehenden Maßnahmen stellen die Weitergabe Kontrolle sicher:

- Nutzung von sicherer Datenübertragung zwischen Server und Client (Transportverschlüsselung)
- Transportverschlüsselung im Backend
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Netzseparation in logische Netzsegmente zwischen den verbundenen IT-Systemen
- Definition von Schnittstellen und den übermittelten personenbezogenen Datenfeldern
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Firewall Regelwerke die Kommunikationsbeziehungen zwischen den Netzsegmenten steuern und alle außer den notwendigen Zugriffen und Datenströmen unterbinden
- Weitergabe von Verkehrsdaten möglichst in pseudonymisierter Form
- Ablage von personenbezogenen Daten nur auf mit höchstem Schutzniveau verschlüsselten Datenträgern
- Sichere Löschung, Entsorgung und Vernichtung von Daten- und Informationsträgern in Papierform
- E-Mail-Verschlüsselung

2.2 Eingabekontrolle

Mittels der Eingabekontrolle wird die Feststellung getroffen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
Die nachstehenden Maßnahmen stellen die Eingabekontrolle sicher:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

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

3.1 Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle stellt den Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, sicher. Die “Rasche Wiederherstellbarkeit” (Art. 32 Abs. 1 lit. c DS-GVO) wird ebenfalls von der Verfügbarkeitskontrolle überwacht, respektive geschaffen.

Die nachstehenden vom Auftragnehmer betriebenen Maßnahmen stellen die Verfügbarkeitskontrolle sicher:

Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Überspannungsschutz in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Backup-Strategie (online/offline; on-site/off-site) & Recoverykonzept
- Testen von Datenwiederherstellung

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

4.1 Organisationskontrolle

Die Organisationskontrolle beinhaltet grundsätzliche Anforderungen an die Verarbeitung von Daten im Unternehmen des Auftragnehmers und definiert Prozesse und Arbeitsabläufe. Die Umsetzung und Einhaltung dieser wird garantiert mittels der nachfolgenden Mittel:

- Datenschutz-Management System
- ISO 9001:2015 (Re-)Zertifizierung
- IT-Störungsmanagement: Trouble Ticket System, Vorfallreaktionspläne
- System Monitoring und proaktives System Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Möglichkeit der Daten Portabilität und der Löschbarkeit von Daten,
- Protokollierung von Eingabe, Änderung und Löschung von Daten

4.1 Auftragskontrolle

Es darf keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers stattfinden.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- schriftliche Weisungen an den Auftragnehmer (z.B. Auftragsverarbeitungsvertrag)
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- es werden wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- vorherige Prüfung der Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG) Ab 25.05.2018 Datengeheimnis nach §53 Bundesdatenschutzgesetz Neu
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

5. Unterschrift

Wir versichern, dass die hier getätigten Angaben dem aktuellen Stand der bei uns umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutzniveau und zur Datensicherheit entsprechen. Abweichungen der hier getätigten
Angaben sind unmittelbar an den Auftraggeber des Rahmenvertrages gem. Satz 1 dieser Checkliste zu melden.

Köln den 03.04.2018,

Alexander Spahl Bernd Schlägel
Vorstände