Anlage – Technisch-Organisatorische-Maßnahmen

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

Zutrittskontrolle - Kein unbefugter Zutritt zu Datenverarbeitungsanlagen,

- Unbefugten wird der Zugang zu den Einrichtungen sowohl durch Zaunanlagen als auch an den Zugangsstellen des Gebäudes verwehrt. Der Zugang zu den Einrichtungen ist reglementiert und erfordert entweder eine Validierung an den elektronischen Zutrittskontrollanlagen (z. B. Kartenzugriffssysteme) oder eine Validierung durch das Sicherheitspersonal. Mitarbeiter und Dienstleister müssen während des Aufenthaltes in den Einrichtungen Lichtbildausweise tragen. Besucher sind verpflichtet, sich beim Sicherheitspersonal anzumelden, sich auszuweisen und erhalten einen Besucherausweis. Der Besucherausweis muss während des Aufenthaltes in den Einrichtungen getragen werden. Besucher werden während ihres Aufenthaltes in den Einrichtungen von autorisierten Mitarbeitern begleitet.
- Einsatz von elektronischen Einbruchsmeldesystemen, die darauf ausgelegt sind unautorisierten Zugang zu den Einrichtungen, einschließlich Überwachungspunkte (z. B. primäre Eingangstüren, Notausgangstüren, Dachluken, usw.) mit Hilfe von Türkontakten, Glasbruchvorrichtungen, Innenbewegungsdetektion u. ä. zu melden.
- Der gesamte physische Zugang zu den Einrichtungen sowohl durch Mitarbeiter als auch Dienstleister wird protokolliert und regelmäßig überprüft.
- ISO 27001-Zertifizierung von AWS dem Bereitsteller der Server und der Infrastruktur.

Zugangskontrolle - Keine unbefugte Systembenutzung,

- Der Zugang wird nur für Mitarbeiter und Dienstleister, elektronisch zugänglich gemacht, die zur Erbringung von Dienstleistungen erforderlich sind.
- Alle Benutzer sind auf Systemprozesse und Transaktionen beschränkt, für die sie speziell autorisiert sind.
- Desktop Security-Prozeduren werden durch das Domänen-Setup erzwungen.
- Sperrung des Benutzerdesktops nach einem bestimmten Zeitraum der Inaktivität.
- automatische und manuelle Sperrschaltung des Arbeitsplatzes.
- Anwenderkennung (Name, persönliches Passwort, periodischer Passwortwechsel).
- Abweisung unberechtigter Benutzer.
- Im Rahmen eines definierten Prozesses werden Benutzerrechte verwaltet (Erteilung, Entzug, Änderung).
- Viren-/ Malwareschutzlösungen sind auf Client-, Server- und Cloudsystemen installiert.
- Sicherheitsupdates werden regelmäßig auf Client-, Server- oder Firewallsystemen installiert.
- Cloud- bzw. Sicherheitssysteme werden regelmäßige auf Schwachstellen oder Konfigurationsfehler überprüft.

Zugriffskontrolle - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems,

- Zugriff auf eingeschränkte Ressourcen basierend auf einer Kombination aus Benutzerauthentifizierung und Zugriffslisten und auf der Basis von "Need-to-know".
- Passwortrichtlinie, Sperrrichtlinie für Benutzerkonten, Desktopeinstellungen, automatische, Überwachungsrichtlinie werden über Domain festgelegt.
- Alle Benutzer haben eine eindeutige Benutzer-ID auf Systemen für ihren offiziellen Gebrauch und sind allein für alle Vorfälle verantwortlich, die auf diese spezifische ID zurückzuführen sind.
- Umsetzung von Zugriffsrichtlinien, um den Zugriff aus anderen Netzwerken und durch Benutzer zu reglementieren.
- Benutzerrechte werden regelmäßig überprüft und ggf. angepasst.

Trennungskontrolle - Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden,

- zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet.
- Trennung zwischen Produktiv- und Testdatenbank.
- Eine Datenverarbeitung erfolgt nur auf Weisung des Auftraggebers und ist immer zweckgebunden, z.B. Support-Unterstützung.
- Es ist sichergestellt, dass nur berechtigte Personen mit geeigneter Identifizierung und Authentisierung Zugriff auf die Daten erhalten, Mandantenfähigkeit.

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

Weitergabekontrolle - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport,

- durch Verschlüsselung beim Datentransfer sowie Einsatz von Virtual Private Networks (VPN).
- Übermittlungsberechtigte sind festgelegt (Sender), Übermittlungsempfänger ebenfalls, Geschützter Übermittlungsweg (secure file transfer).
- Überprüfung der Authentizität des Empfängers (Nutzername, Passwort).
- Protokollierung der Datenübermittlung.
- Endgeräte, z.B. Notebooks oder Smartphones, sind verschlüsselt.
- Mitarbeiter werden regelmäßig zu Datenschutz und Informationssicherheit geschult.
- Die Weitergabe von Daten ist durch organisatorische Regelungen abgesichert.

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

- Netzwerkverbindungen und -vorgänge sind vollständig dokumentiert und werden aufrechterhalten. Die Protokollierung wird für Netzwerkkomponenten wie Firewalls und Router aktiviert und auf verdächtige Aktivitäten im Netzwerk überwacht.
- Audit-Trails werden bei Benutzertransaktionen und fehlgeschlagenen Zugriffsversuchen beibehalten.
- Benutzerrechte sind geregelt und differenziert.
- Einsatz von Software mit differenzierten Rechten, Protokollierung der Zugriffe.

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

Verfügbarkeitskontrolle - Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust,

- Dies geschieht unter Verwendung von Firewalls oder funktional gleichwertiger Technologien und Authentifizierungssteuerelementen sowie Authentifizierungskontrollen. Im Fall von potenziellen Sicherheitsbedrohungen hält AWS Reaktionspläne und Korrekturmaßnahmen bereit, um auf diese Bedrohungen reagieren zu können.
- Das Spiegeln von Festplatten erfolgt nach dem RAID-Verfahren.
- Die Datenverarbeitungsanlagen sind redundant aufgebaut und Backups werden regelmäßig erstellt. Sicherungsmedien werden getrennt aufbewahrt.
- Eine unterbrechungsfreie Stromversorgung verhindert den Verlust von Daten.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- · Ein Notfallplan sichert Verfügbarkeit und rasche Wiederherstellung organisatorisch ab.

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

Datenschutz-Management-System - Unternehmensrichtlinie zum Datenschutz für alle Mitarbeiter

- ·Die Sicherheit des Netzwerks und die Angemessenheit seines Informationssicherheitsprogramms wird regelmäßig im Hinblick auf Branchensicherheitsstandards und seine Richtlinien und Verfahren überprüft.
- Die Sicherheit des Netzwerks und der zugehörigen Dienste werden regelmäßig geprüft, um festzustellen, ob zusätzliche oder andere Sicherheitsmaßnahmen erforderlich sind und um auf neue Sicherheitsrisiken oder Erkenntnisse zu reagieren.
- Alle Mitarbeiter unterzeichnen eine Vertraulichkeitsvereinbarung und Sicherheitsrichtlinie, bei der die Verantwortung des Mitarbeiters für die Vertraulichkeit und die Sicherheitsmaßnahmen angegeben sind.
- Jeder Mitarbeiter unterzeichnet dafür, dass er die Sicherheitsrichtlinien gelesen und verstanden hat und akzeptiert, sie einzuhalten.
- Ein Personal Informations- Managementsystem ist implementiert, das die DSGVO-Anforderungen enthält. Dieses System umfasst unter anderem Aspekte wie: Umgang mit den persönlich identifizierbaren Informationen, Einholen und Verwalten der Zustimmung der betroffenen Person, das Verwalten des Inventars von PI-Daten und Datenflussinformationen in Projekten und Funktionen, die Durchführung von Datenschutzfolgenabschätzungen, die Festlegung und Umsetzung der Datenschutzmaßnahmen (sowohl technischer als auch verfahrenstechnischer Art) zum Schutz der PI-Daten und den Umgang mit Datenschutzverletzungen.

Incident-Response-Management – Verhalten bei Datenschutzvorfällen,

- Alle Sicherheitsvorfälle werden gemeldet und im Tracker "Security Incident Management" aufgezeichnet. Die

Mitarbeiter werden auf die Mittel zur Meldung von Sicherheitsvorfällen aufmerksam gemacht. Für den Fall eines Sicherheitsverstoßes / einer Verletzung durch einen Mitarbeiter wurden von HR disziplinarische Richtlinien aufgestellt, um geeignete Maßnahmen zu ergreifen.

- Sicherheitsvorfälle umfassen, z.B. Virusangriffe, Hackversuche, Nicht autorisiertes Kopieren / Weitergabe von Informationen, Manipulation, Sabotage).

Auftragskontrolle - Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers,

- Der Auftragnehmer wird nur nach Anweisung des Auftraggebers tätig.
- Nachkontrollen sind durch das Ticketsystem gegeben.
- Ein Datenschutzbeauftragter ist beim Auftragnehmer bestellt, wenn gesetzlich gefordert.
- Strenge Auswahl aller beteiligten Dienstleister und Abschluss eines Zusatzvertrages zur Auftragsverarbeitung mit allen Beteiligten.

Alle Beschäftigten, die im Sinne dieses Vertrages tätig werden, sind im Rahmen des Arbeitsverhältnisses zur Verschwiegenheit verpflichtet.