Anlage 1 - technische und organisatorische Maßnahmen

Gemäß Art. 32 DS-GVO zu treffende technische und organisatorische Maßnahmen, die für die Erfüllung des Auftrags durch den Auftragsverarbeiter relevant sind

Unter Berücksichtigung des

- Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und
- der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Die folgenden Maßnahmen sind diejenigen, die froach in seiner eigenen Einflusssphäre ergreift. Soweit wir für froach Unterauftragnehmer einsetzen, gelten ergänzend deren eigene technisch-organisatorischen Maßnahmen.

Der Auftragsverarbeiter ergreift folgende Maßnahmen:

1. Pseudonymisierung

Personenbezogene Daten des Verantwortlichen können in einer Weise verarbeitet werden, sodass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die eine unbefugte Identifizierung der Betroffenen ausschließen.

Gleichwohl bleiben derart pseudonymisierte Daten personenbezogene Daten im Sinne der DS-GVO. Die Pseudonymisierung ist eine technische und organisatorische Maßnahme, und kann vom Auftragsverarbeiter wie folgt umgesetzt werden:

x getrennte Speicherung von Zusatzinformationen zur Identifikation

2. Maßnahmen zur Verschlüsselung

x Verschlüsselte Aufbewahrung von Passwörtern
x Verschlüsselung von Email bzw.- Email-Anhängen
x Gesicherte Datenweitergabe (z.B. SSL, FTPS, TLS)
x Gesichertes WLAN

3. Maßnahmen zur Sicherstellung von Vertraulichkeit

a. Zutrittskontrolle *(Maßnahmen durch die Unbefugten der Zutritt verwehrt wird)*

x Sicherheitstüren / -fenster
x Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
x Spezielle Schutzvorkehrungen des Serverraums
x Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
x Nicht-reversible Vernichtung von Datenträgern
x Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)

Weitergehende Anmerkungen:

- Das externe Rechenzentrum ist durch Video-Überwachung sowie Zugangskontrollen mittels Kennkarte und Vereinzelungsanlage optimal gesichert.
- Die geschützte Lage unter der Erde, Brandfrüherkennungssysteme sowie Notstrom mittels mehrerer Dieselaggregate sorgen für zusätzliche Sicherheit.
- Hochsicherheitsrechenzentrum mit Standort in München unterliegt deutschem Recht/ Datenschutz

b. Zugangskontrolle *(Maßnahmen die verhindern, dass Unbefugte die Verarbeitungssysteme nutzen können)*

x Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
x Autorisierungsprozess für Zugangsberechtigungen
x Begrenzung der befugten Benutzer
x Single Sign-On
x Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
x Protokollierung des Zugangs
x Zusätzlicher System-Log-In für bestimmte Anwendungen
x Firewall

Weitergehende Anmerkungen:

- Login-Daten sind nur dem Geschäftsführer sowie dem technischen Leiter bei froach zugängig und werden verschlüsselt aufbewahrt
- Für die generierten Passwörter gelten strenge, definierte Anforderungen (min. 12 Zeichen, min. 1 Sonderzeichen + Zahlen)
- Automatische Beendigung von Login-Sessions

c. Zugriffskontrolle *(Maßnahmen die gewährleisten, dass nur berechtigte Personen auf die Verarbeitungssysteme zugreifen und personenbezogene Daten nicht unbefugt lesen, kopieren, verändern oder entfernen können)*

x Verwaltung und Dokumentation von differenzierten Berechtigungen
x Auswertungen/Protokollierungen von Datenverarbeitungen
x Autorisierungsprozess für Berechtigungen

x Genehmigungsroutinen
x Profile/Rollen
x Vier-Augen-Prinzip
x Funktionstrennung „Segregation of Duties“
x Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
x Nicht-reversible Löschung von Datenträgern

Weitergehende Anmerkungen:

- Firewalls serverseitig im Hochsicherheitszentrum sowie clientseitig im froach Office
- Die Anwendung trennt zwischen Usergruppen (Admin, normale User) mittels ACL-Zugriffsrechten

d. Trennungskontrolle *(Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können)*

x Zugriffsberechtigungen nach funktioneller Zuständigkeit
x Mandantenfähigkeit von IT-Systemen (über Lizenzmanagement)
x Verwendung von Testdaten
x Trennung von Entwicklungs- und Produktionsumgebung

4. Maßnahmen zur Sicherstellung von Integrität

x Zugriffsrechte
x Systemseitige Protokollierungen
x Dokumenten Management System (DMS) mit Änderungshistorie
x Protokollierung des Kopierens, Veränderns oder Entfernens von Daten

Weitergehende Anmerkungen:

- Protokollierung der Softwaresystem-Änderungen in einer Versionsverwaltung
- Protokollierung von Systemzugriffen in Logdateien

5. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

x Sicherheitskonzept für Software- und IT-Anwendungen
x Back-Up Verfahren
x Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
x Bedarfsgerechtes Einspielen von Sicherheits-Updates
x Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
x Brand- und/oder Löschwasserschutz des Serverraums
x Klimatisierter Serverraum
x Virenschutz
x Firewall
x Notfallplan
x Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)

6. Maßnahmen zur Sicherstellung der Belastbarkeit

- x Redundante Stromversorgung
- x Ausreichende Kapazität von IT-Systeme und Anlagen
- x Logistisch gesteuerter Prozess zur Verhinderung von Leistungsspitzen

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- x Konzept für regelmäßige Überprüfung, Bewertung und Evaluierung

8. „Weisungskontrolle/Auftragskontrolle“

- x Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 Abs. 3 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen
- x Prozess zur Erteilung und/oder Befolgung von Weisungen
- x Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- x Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- x Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragsverarbeiter
- x Verpflichtung der Mitarbeiter zur Vertraulichkeit
- x Benennung eines Datenschutzbeauftragten gemäß Art. 37 ff. DS-GVO
- x Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO
- x Dokumentations- und Eskalationsprozess für Verletzungen des Schutzes personenbezogener Daten
- x Richtlinien/Vorgaben zur Gewährleistung von technisch-organisatorischer Maßnahmen zur Sicherheit der Verarbeitung
- x Prozess zur Weiterleitung von Betroffenenanfragen