Anlage zur AV-Vereinbarung

Allgemeine technische und organisatorische Maßnahmen

gemäß Art. 32 Abs. 1 DSG-VO

Firma: Certado GmbH
Datum der Erstellung: 01.02.2022

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

1.1 Zugangskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten den Zugang zu den Datenverarbeitungssystemen zu verhindern:

- Login mit Benutzername + Passwort
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Firewall Server
- Firewall Clients
- Verschlüsselung bei WLAN-Benutzung (WPA2)
- Verwaltung von Benutzerberechtigungen
- Anleitung „Manuelle Desktopsperre“

1.2 Zugriffskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten das Lesen, Kopieren, Verändern oder Löschen innerhalb der Datenverarbeitungssysteme zu verhindern:

- Protokollierung von Zugriffen auf Anwendungen in Log-Dateien
- Berechtigungskonzept(e)
- Minimale Anzahl an Administratoren
- Verwaltung Benutzerrechte durch Administratoren

1.3 Trennungskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um die zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten zu trennen:

- Trennung von Produktiv- und Testumgebung
- Mandantenfähigkeit relevanter Anwendungen
- Bedarfsgerechte Zugriffsberechtigungen der Mitarbeiter
- Festlegung von Datenbankrechten

1.4 Pseudonymisierung (Art. 32 Abs. 1 lit. a) & Art. 25 Abs. 1 DSGVO)

Die Pseudonymisierung von Datensätzen wird durch folgende Maßnahmen umgesetzt:

- Interne Anweisung, personenbezogene Daten möglichst zu pseudonymisieren / anonymisieren

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

2.1 Weitergabekontrolle

Personenbezogene Daten müssen bei der elektronischen Übermittlung ausreichend geschützt werden, um nicht unbefugt gelesen, kopiert, verändert oder entfernt zu werden. Folgende technische und organisatorische Maßnahmen haben wir hierfür ergriffen:

- Bereitstellung verschlüsselter Verbindungen
- Nutzung von elektronischen Signaturverfahren
- Protokollierung der Zugriffe und Abrufe in Log-Dateien
- Weitergabe in anonymisierter oder pseudonymisierter Form

2.2 Eingabekontrolle

Zur Kontrolle, ob und von wem personenbezogene Daten in das Datenverarbeitungssystem eingegeben, geändert, gesperrt oder gelöscht werden, setzen wir folgende Maßnahmen ein:

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe individueller Benutzernamen
- Berechtigungskonzept mit Vergabe von bedarfsgerechten Benutzerrechten
- Sichere Aufbewahrung von Dokumenten in Papierform

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)

Zur Gewährleistung der Verfügbarkeit personenbezogener Daten gegen zufällige oder mutwillige Zerstörung oder Verlust, setzen wir folgende Maßnahmen ein:

- Regelmäßige Archivierung / Backup der Daten
- Backup-Konzept (online)
- Recovery-Konzept
- Kontrolle des Sicherungsvorgangs

4. Verfahren zur regelmäßigen Überwachung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit d) DSGVO & Art. 25 Abs. 1 DSGVO)

Datum der Evaluierung der technischen und organisatorischen Maßnahmen:
01.02.2022

4.1 Datenschutz-Management

Zur Gewährleistung des Datenschutzes in unserem Unternehmen setzen wir folgende Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung ein:

- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich

4.2 Incident-Response-Management (gemäß Art. 33 DSGVO)

Im Falle des Erkennens und der Meldung von Datenschutzverletzungen setzen wir folgende Maßnahmen ein:

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen

Im Rahmen datenschutzfreundlicher Voreinstellungen (Art. 25 Abs. 2 DSGVO) setzen wir folgende Maßnahmen ein:

- Datenminimierung und Zweckbindung
- Einfache (technische) Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

4.4 Auftragskontrolle (Outsourcing)

Im Rahmen des Outsourcings der Verarbeitung personenbezogener Daten durch Auftragsverarbeiter setzen wir für die Gewährleistung eines angemessenen Schutzniveaus folgende Maßnahmen ein:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfalts-Gesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
- Schriftliche Weisungen an den Auftragnehmer

- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Hiermit bestätige ich, dass ich die Beschreibung der technischen und organisatorischen Maßnahmen nach bestem Wissen und Gewissen erstellt habe und die angegebenen Maßnahmen dem tatsächlichen Stand in dem von mir vertretenen Unternehmen entspricht.

Friedberg, 01.02.2020

(Ort, Datum)

(Unterschrift Verantwortlicher)