Anlage 2

Technisch-organisatorische Maßnahmen des Auftragnehmers, gem. Art. 32 DSGVO

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

a) Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Die Zugänge sind abgesichert über ein Zutrittskontrollsystem

· Für sensible Bereiche wird neben der Zutrittskarte auch ein Code benötigt

· Elektrische Tür- und Toröffner sind vorhanden

· Schlüsselregelung, Generalschlüssel sind vorhanden

· Die Zutrittskontrolle wird zusätzlich durch Alarmanlage, Bewegungsmelder und Videoüberwachung gesichert

· Es finden Besucherregelungen statt. Besucher werden empfangen und von einem Betriebsangehörigen persönlich abgeholt. Besucher dürfen sich im Gebäude nie-mals alleine aufhalten oder bewegen

· Getrennte und abgestufte Bereiche (Eingangsbereich, Büroräume, Serverraum) gewährleisten, dass nur befugte Personen Zutritt zu den Räumen haben

· Der Zutritt zum Serverraum ist stets verschlossen und allein der IT und dem Vorstand des Unternehmens vorbehalten

· Auf- und Abschließen der Räume bei Arbeitsbeginn bzw. Arbeitsende

· Die Zugangstüren sind außerhalb der Betriebszeiten verschlossen

· Für die Überwachung wird ein Sicherheitsdienst eingesetzt

· Sorgfalt bei Auswahl des Reinigungsdienste; Verpflichtung auf Vertraulichkeit

b) Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Einsatz von Firewall und Virenschutz

· Sämtliche Systeme sind passwortgeschützt

· Automatische Sperrung der Bildschirme bei Pausen mit Passwortschutz

· Ein Benutzerstammsatz pro User wird eingerichtet

· Im Einsatz befindliche Notebooks sind hardwareverschlüsselt mittels Bitlocker

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Differenzierte Berechtigungen (Zugriffsrechte) sind vorhanden

· Gewährleistung des Schutzes gegen unberechtigte externe sowie interne Zugriffe

· Datenträgerverwaltung

· Vollständische Löschung verwendeter Datenträger vor neuer Verwendung bzw. Weitergabe

· Die Vernichtung von Akten und harten Datenträgern erfolgt grundsätzlich über einen externen zertifizierten Entsorger

d) Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Interne Mandantenfähigkeit / Zweckbindung

· Regelungen für getrennte Speicherung, Veränderung, Löschung und Übermittlung sind getroffen.

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Pseudonymisierungsverfahren nach Abstimmung

· Nach Notwendigkeit findet eine Anonymisierung von Daten statt

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

a) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transport-behälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Es erfolgt eine Verschlüsselung von Daten auf dem Transportweg (z.B. SFTP, HTTPS zum Dateitransfer)

· Versand von sensiblen, insbesondere personenbezogenen Daten nur auf Basis von zuvor getroffenen, vertraglichen Vereinbarungen

· Beim physischen Transport ist die sorgfältige Auswahl von Transportpersonal und -fahrzeugen gewährleistet

· Beim physischen Transport: verschlossene Transportbehälter, Legitimation der Abholer

b) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netz-werk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Zur berechtigten Dateneingabe sind Berechtigungsprofile bzw. –gruppen festgelegt

· Differenzierung des Zugriffs erfolgt durch differenzierte Berechtigungen.

· Definition von Aufbewahrungszeiträumen durch Festlegung von Vernichtungszeit-punkten bzw. von Löschfristen für personenbezogene Daten.

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

a) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brand-schutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid-Systeme, Plattenspiegelungen etc..

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Unterbrechungsfreie Stromversorgung (USV)

· Klimaversorgung im Serverraum

· Rauchmelder und Temperaturüberwachung im Serverraum installiert

· Feuer- und Rauchmeldeanlagen im gesamten Unternehmen

· Feuerlöscher im Serverraum sowie im gesamten Unternehmen

· Rauchverbot

· Backup Verfahren (BackUps werden täglich durchgeführt.)

· Rücksicherungstests werden durchgeführt

· Storage: RAID System

· Synchronisierte Server (Spiegelung der Festplatten)

· Funktionstrennung zwischen Fachabteilung und IT

· Zentrale Beschaffung von Hard- und Software

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

a) Datenschutz-Management

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Verzeichnis von Verarbeitungstätigkeiten

· Datenschutz-Folgenabschätzung (DSFA) bei Notwendigkeit

· Technische und organisatorische Maßnahmen

· AV-Verträge

· Verpflichtung auf das Datengeheimnis

· Informationspflichten nach Art. 13 und 14 DSGVO

· Regelmäßige Sensibilisierung der Mitarbeiter

· Externer Datenschutzbeauftragter

· Prozess für die Wahrnehmung von Betroffenenrechten

· Prozess für die Meldung von Datenschutzverstößen

· Einhaltung von Löschfristen

· Weitere Dokumentationen

b) Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Einsatz von Firewall und regelmäßige Aktualisierung.

· Einsatz von Spamfilter und regelmäßige Aktualisierung.

· Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen (in Arbeit).

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

· Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind, d.h. der Grundsatz der Datenminimierung wird umgesetzt.)

d) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Daten-verarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Beschreibung der vorhandenen / getroffenen Maßnahmen des Auftragnehmers:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich der Datensicherheit)
- Formalisierte Auftragserteilung (Auftragsformular)
- Detaillierte schriftliche Regelungen der Auftragsverhältnisse