Übergreifende technische und organisatorische Maßnahmen (TOM) nach DSGVO mit Stand vom November 2022

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO. Diese TOM sind Anlage der Rahmenvereinbarung zur Auftragsverarbeitung.

1 Auftragnehmer

AVENTUM GmbH
Spandauer Straße 46
57072 Siegen

Vertreten durch Geschäftsführer:
Herr Dr. Markus Weyerke

2 Vertraulichkeit gem. Art. 32 Abs. 1 lit. b) DSGVO

2.1 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.

Der allgemeine Zutritt zum Gebäude erfolgt über ein manuelles Schließsystem mit Sicherheitsschlössern. Die Ausgabe/Rückgabe der Schlüssel wird in der Arbeitsmittelverwaltung der Personalverwaltungssoftware HRworks dokumentiert.

Besucher dürfen die Büroräume nur in Begleitung von Mitarbeitern betreten.

Die Gebäudereinigung wird durch ein beauftragtes Reinigungsunternehmen durchgeführt. Reinigungskräfte haben keinen Zutritt zur IT-Anlagen und Schränken mit personenbezogenen Daten.

2.2 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).

Alle Arbeitsrechner werden verschlüsselt, um ein Auslesen von Festplatten bei Verlust zu unterbinden.

Die Benutzerauthentifizierung und -verwaltung wird mittels zentraler Verzeichnisdienste abgebildet. Für die Anmeldung an den IT-Systemen sind komplexe Kennwörter sowie 2FA erforderlich. Bei Ausscheiden eines Mitarbeiters werden alle IT-Systeme gesperrt.

Der Zugriff auf die IT-Systeme wird u.a. durch eine Firewall gesteuert und überwacht. Eine Antivirus-Software auf Systemebene der Server und Clients ist ständig aktiv. Es werden ausschließlich IT-Systeme eingesetzt, die vom Hersteller durch regelmäßige Sicherheitsupdates unterstützt werden.

Remote-Zugriffe werden durch den Einsatz von abgesicherten VPN-Verbindungen durchgeführt.

2.3 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.

Durch den Einsatz eines zentralisierten Berechtigungskonzeptes wird gewährleistet, dass die Beschäftigten nur die Zugriffe erhalten, die sie zur Erfüllung ihrer Arbeit benötigen.

Zugriffe auf Anwendungen werden protokolliert.

Die Festplatten in Notebooks der Beschäftigten sind mit Bitlocker verschlüsselt.

2.4 Trennung

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

Sofern eine getrennte Verarbeitung und Auswertung der Datenbestände erforderlich sind, wird diese entsprechend eingerichtet. Eine Trennung wird nach Wahl des Auftragnehmers oder durch besondere Weisung des Auftraggebers erreicht durch den Einsatz von getrennten Datenbanken, getrennten virtuellen Maschinen, unterschiedliche Mandanten und/oder Berechtigungssteuerung in der Anwendung selbst.

2.5 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.

Es existiert eine Arbeitsanweisung zum Umgang mit nicht verschlüsselten Verbindungen, nach der personenbezogene Daten bei Weitergabe möglichst zu anonymisieren/pseudonymisieren sind. Eine Abweichung hiervon ist ausschließlich bei ausdrücklich erteiltem Einverständnis des Auftraggebers gestattet.

3 Integrität Art. 32 Abs. 1 lit. b) DSGVO

3.1 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, Netzwerk, 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.

Alle Netzwerkanmeldungen und -abmeldungen sowie sämtliche Transaktionen (z. B. Neuanlagen, Veränderungen, Löschungen) werden protokolliert. Die Protokolle werden bei Verdacht hinsichtlich unberechtigter Zugriffe analysiert und nach frühestens sechs Monaten gelöscht.

Manuell ausgefüllte Formulare, von denen Daten in automatisierte Verarbeitungen übernommen wurden, werden archiviert.

3.2 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 Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Für einen Transport von personenbezogenen Daten nach außerhalb des Netzwerks des Auftragnehmers werden die Daten grundsätzlich verschlüsselt. Hierzu werden starke Verschlüsselungsalgorithmen eingesetzt. Die Übermittlung der Passwörter zur Entschlüsselung erfolgt auf getrenntem Weg.

Für die Übermittlung von Daten des Auftraggebers stellt der Auftragnehmer ein abgesichertes Kundenportal als https im Rechenzentrum Siegen bereit.

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

4.1 Verfügbarkeit

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

Personenbezogene Daten sind grundsätzlich in der Serverstruktur des Auftragnehmers abzulegen. Dazu existiert eine IT-Richtlinie. Die Server des Auftragnehmers befinden sich in einem Rechenzentrum und werden regelmäßig gesichert. Ausgenommen sind Beschäftigte, welche Daten, i. d. R. Kopien, zur Auftragserfüllung lokal auf ihrem Gerät benötigen, z. B. Consultants. Die Festplatten dieser Notebooks sind mit Bitlocker verschlüsselt.

Eine vollständig virtualisierte und abgesicherte Serverumgebung sowie eine USV und Überspannungsschutz verhindern einen ungewollten Datenverlust.

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

5.1 Datenschutz-Management

Der Geschäftsführung obliegt die Verantwortung für die Datenschutz- und Informationssicherheit.

Alle Beschäftigten sind auf Vertraulichkeit verpflichtet. Es erfolgt eine regelmäßige Sensibilisierung der Beschäftigten hinsichtlich des Datenschutzes.

Für die Bearbeitung von Auskunftsanfragen seitens Betroffener existiert ein formalisierter Prozess. Die eingesetzten IT-Systeme und Prozesse sind dokumentiert.

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird mindestens einmal jährlich überprüft.

Es ist ein externer Datenschutzbeauftragter benannt. Es erfolgt eine regelmäßige Überprüfung der IST-Situation.

5.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Es werden Firewalls, Spamfilter, Virenscanner und Systeme zur Intrusion Detection eingesetzt und regelmäßig aktualisiert.

Es gibt Notfallpläne für Sicherheitsvorfälle und Datenpannen. Die Geschäftsführung ist stets involviert.

5.3 Datenschutzfreundliche Voreinstellungen Art. 25 Abs. 2 DSGVO

Privacy by design / Privacy by default

Die Beschäftigten sind sensibilisiert und angewiesen, nur die personenbezogenen Daten zu verarbeiten, die für den jeweiligen Zweck erforderlich sind.

Benutzer- und Zugriffsrechte sind pessimistisch vorbelegt. Einschränkungen werden bei berechtigtem Interesse zurückgenommen.

Für die Übermittlung von Daten des Auftraggebers stellt der Auftragnehmer ein abgesichertes Kundenportal als https im Rechenzentrum Siegen bereit.

5.4 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 Datenverarbeitung 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.

Sollte das Unternehmen Dienstleister im Sinne einer Auftragsverarbeitung nach Art. 28 DSGVO einsetzen, findet im Vorfeld eine Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation statt.

Die Auswahl des Auftragnehmers wird unter Sorgfaltsgesichtspunkten, gerade in Bezug auf Datenschutz und Datensicherheit, durchgeführt. Ein Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung wird berücksichtigt.

Die Weisungen des Auftraggebers an den Auftragnehmer erfolgen in Textform.

Der Auftragnehmer verpflichtet seine Beschäftigten auf Vertraulichkeit.

Der Auftragnehmer hat aufgrund der gesetzlichen Vorgaben einen Datenschutzbeauftragten benannt.

Es findet eine Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer statt. Regelungen zum Einsatz weiterer Subunternehmer werden vereinbart.

Es werden Regelungen vereinbart, die sicherstellen, dass Daten nach Beendigung des Auftrags beim Auftragnehmer vernichtet werden.