TECHNISCH UND ORGANISATORISCHE MAßNAHMEN (TOMs)

Gem. Anlage zum Vertrag zur Auftragsdatenverarbeitung, Art. 32 DSGVO resp. § 64 BDSG n.F.

Inhalt

Vorwort 2
Technische und organisatorische Maßnahmen 2
1. Vertraulichkeit (Art. 32 Abs. 1 b DSGVO) 2
2. Integrität (Art. 32 Abs. 1 b DSGVO) 4
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b DSGVO) 5
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 d DSGVO, Art. 25 Abs. 1 DSGVO) 5

Stand: Februar 2019
Version: 1.1.2

Vorwort

Der Schutz personenbezogener Daten und die Sicherheit der EDV sind für die Veda Group zentrale Anliegen. Die Verarbeitung von personenbezogenen Daten erfolgt unter Einhaltung der DSGVO.
In diesem Dokument wird beschrieben, wie die VEDA Group personenbezogene Daten verarbeitet und mit welchen technischen und organisatorischen Maßnahmen Daten, insbesondere personenbezogene Daten, nach den Maßgaben der DSGVO vor Zerstörung, unbefugter Kenntnisnahme oder ungewollter Manipulation schützt. Die Angabe der technischen und organisatorischen Maßnahmen ist nur dann erforderlich, wenn die Pflege oder Wartung der Systeme außerhalb der Geschäftsräume des Verantwortlichen stattfindet, wie z.B. bei einer Fernwartung.

Technische und organisatorische Maßnahmen

Alle Personen, die personenbezogene Daten verarbeiten, sind auf das Datengeheimnis verpflichtet. In regelmäßigen Schulungen werden diese Personen für den sorgsamen Umgang mit Daten und zu den Grundsätzen des Datenschutzes nach DSGVO sensibilisiert und unterwiesen. Darüber hinaus werden alle Mitarbeiter zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse und den sorgfältigen Umgang mit Datenträgern und Dateien verpflichtet. Um personenbezogene Daten gegen zufällige oder vorsätzliche Manipulation, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen, setzt die VEDA Group technische und organisatorische Sicherheitsmaßnahmen um. Diese Sicherheitsmaßnahmen werden entsprechend der technologischen Entwicklung fortlaufend verbessert. Dazu zählen u.a. folgende Maßnahmen:

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

1.1. Zugangskontrolle

1.1.1. Räumlichkeiten

Das Betriebsgebäude / -gelände des Auftragnehmers in Alsdorf liegt in einem Gewerbegebiet und bildet nach außen hin eine geschlossene Einheit. Türen der Gebäude sind mit Sicherheitsschlössern versehen, außen- und bereichsabschließende Türen mit Legic-Lesern versehen. Die Gebäude sind durch eine Alarmanlage mit Anschluss an eine Notrufzentrale geschützt.

Zu den Räumlichkeiten, in denen hauptsächlich Auftragsdaten verarbeitet bzw. in denen personengebundene Daten in Papierform aufbewahrt und bearbeitet werden, befinden sich die Schlüssel ausschließlich in Obhut der Geschäftsleitung sowie der zuständigen Mitarbeiter des Auftragnehmers. Dritte haben zu den Räumlichkeiten keinen Zutritt.

Die EDV-Anlage ist in einem fensterlosen Innenraum untergebracht. Die Tür zu diesem Raum verfügt über eine eigene Zutrittskontrollanlage. Zutritt zu diesem Raum haben nur die Geschäftsleitung sowie die zuständigen Mitarbeiter.

1.1.2. Besucher

Besucher müssen generell angemeldet / angekündigt werden. Sowohl angemeldete, wie auch unangemeldete Besucher haben sich am Empfang zu melden. Der Auftragnehmer verfügt über einen Empfangs- resp. Wartebereich, der von den Empfangsmitarbeitern vollständig einsehbar ist. Zutritt / Bewegung im Gebäude ist ausnahmslos in Begleitung eines Mitarbeiters möglich; Besucher sind durch Namensschild ausdrücklich als solche gekennzeichnet. Sensible Bereiche im Gebäude sind zudem durch geschlossene Zwischentüren (Zutritt nur mittels Legic möglich) abgetrennt.

1.1.3. EDV-System

Der Zugang zum EDV-System ist nur mit personengebundenen Benutzerkennungen und sicheren Passwörtern geschützt. Erfolgt ein Zugang remote, so ist eine verschlüsselte Verbindung Voraussetzung. Für sichere remote-Zugänge werden Token verwendet.

1.2. Zugriffskontrolle

Die Zugriffsberechtigung der EDV-Systeme ist rollenspezifisch definiert. Zusätzlich sind die Systeme logisch (Partitionen) oder physikalisch nach Aufgabengebieten getrennt und / oder in verschiedene Netzwerksegmente unterteilt, die durch Firewall Regeln getrennt sind.

Datenträger für technische Speicherung werden grundsätzlich über ein externes zertifiziertes Entsorgungsunternehmen vernichtet. Diese Datenträger werden gesammelt und zur Vernichtung weitergegeben. Die Vernichtung erfolgt gem. standardisierter / aktueller Verfahren zur Löschung oder Vernichtung von Daten (z. Zt.: Richtlinie BSI-TL 03420).

1.3. Trennungskontrolle

Die Abschottung der Datenbestände wird durch Speicherung in getrennten physischen Dateien, Verzeichnissen bzw. Datenbanken erreicht. Produktivdaten wer-den getrennt von Entwicklungs- und Testumgebungen in verschiedenen demilitarisierten Zonen (DMZ) vorgehalten.

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

Die Pseudonymisierung von personenbezogenen Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

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

2.1. Weitergabekontrolle

Daten werden über öffentliche Netze nur verschlüsselt und / oder mit VPN Tunneln übertragen. Sicherungsbestände werden ausschließlich von eigenen Mitarbeitern transportiert. Datenträger sind eindeutig benannt und die Vollständigkeit wird regelmäßig überwacht. Für die externe Auslagerung von Datenbeständen wird ein Bankschließfach genutzt. Datenträger und Papierdokumente werden am Nutzungsende an einen gewerblichen Aktenvernichter zur Vernichtung übergeben.

Gegenständen aus dem Eigentum des Auftraggebers, werden vom Auftragnehmer, nach Erfüllung resp. Beendigung der vertraglichen Beziehung, auf Verlangen an diesen heraus- oder zur Vernichtung an ein zertifiziertes Entsorgungsunternehmen weitergeben. Vorliegend wird dies durch den nach DIN Norm DIN 66399 Teil 1 und DIN Norm SPEC 66399 Teil 3 zertifizierten Entsorgungsfachbetrieb:

A & P. Drekopf GmbH & Co. KG

Boettgerstraße 33

41066 Mönchengladbach

Telefon: 02161 6894-0

Telefax: 02161 6894-44

Mail: info@drekopf.de

Web: www.drekopf.de

sichergestellt.

2.2. Eingabekontrolle

Jeder Mitarbeiter des Auftragnehmers arbeitet mit einer eindeutigen Benutzerkennung. Erfassung und Veränderung von Daten werden über Systemfunktionen und über Protokollfunktionen in den genutzten Softwaresystemen protokolliert. Die Veränderung resp. Erfassung ist nur für berechtigte Personen möglich.

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

3.1. Verfügbarkeitskontrolle

Alle Daten auf den Systemen des Auftragnehmers werden täglich auf einem Backupmedium gesichert. Laut der Backup Strategie werden Datensicherungen in einem abschließbaren Stahlschrank und zusätzlich in einem Schließfach der Hausbank ausgelagert. Die Möglichkeit der Rücksicherbarkeit wird im Zufallsverfahren getestet. Die allgemein übliche Schutzeinrichtungen (z.B. Virenscanner, Firewall) werden auf jeweils aktuellem Stand betrieben.
Gegen Stromausfall ist der Auftragnehmer durch unterbrechungsfreie Stromversorgung (USV) und Ersatzstromversorgung mittels Dieselaggregat (AEV) abgesichert. Die Absicherung gegen Elementarschäden erfolgt mittels Brandmeldern und Aufschaltung auf eine externe Alarmzentrale.

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

4.1. Datenschutzmanagement

Das Datenschutzmanagement umfasst eine koordinierte Vorgehensweise aller beteiligten zur Überprüfung der umgesetzten Maßnahmen in Bezug auf die Sicherheit der Daten. Insbesondere gehören hierzu:

- Interne und externe Datenschutzaudits in Kooperation mit dem Datenschutzbeauftragten zur Überprüfung und Wirksamkeit der technisch- und organisatorischen Maßnahmen
- Zertifizierung der umgesetzten Maßnahmen
- Regelmäßige Belastungs- resp. Penetrationstests der Systeme
- Regelmäßige Schulung der Mitarbeiter

4.2. Incident-Response-Management

Es wurde ein organisatorischer Prozess zum Umgang mit Sicherheitsvorfällen implementiert, damit eine koordinierte Vorgehensweise für alle Beteiligten und Mitarbeiter sichergestellt werden kann.

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

Informationelle Gewaltentrennung innerhalb und zwischen verantwortlichen Stellen (Nicht jeder Mitarbeiter kann auf alle Daten zugreifen).
Reduzierung von erfassten Attributen der betroffenen Personen (nur erforderliche Daten werden gespeichert).

Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten (Berechtigungskonzepte).
Bevorzugung von automatisierten Verarbeitungsprozessen, die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen.
Implementierung von Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren in den Anwendungen.
Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren (Nur berechtigte Mitarbeiter können grundlegende Prozesse anpassen / verändern).

4.4. Auftragskontrolle

Es erfolgt keine Auftragsdatenverarbeitung i. S. v. Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers. Dies wird u. a. durch eindeutige Vertragsgestaltung und formalisiertes Auftragsmanagement durch den Auftragnehmer sichergestellt.