Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Der Firma
avanti GreenSoftware GmbH
Blumenstr. 19
70182 Stuttgart

V 1.1.1 vom 13.06.2018

1. Zutrittskontrolle zu den Arbeitsbereichen

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen	
Technisch	***Organisatorisch***
Manuelles Schließsystem	Personenkontrolle beim Empfang
Sicherheitsschlösser	Sorgfältige Auswahl von Reinigungspersonal
Tür mit Knauf Außenseite	Besucher in Begleitung durch Mitarbeiter
Schließung aller Gebäudeeingänge wie Fenster und Türen	Zutritt Externer nur nach Anmeldung
Büroräume sind außerhalb der Arbeitszeit verschlossen	Schlüsselregelung (Schlüsselausgabe etc.)

2. Zugangskontrolle zu Datenverarbeitungssystemen

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen	
Technisch	***Organisatorisch***
Login mit Benutzername und Passwort	Zuordnung von Benutzerberechtigungen
Anti-Virus-Software Server und Rechner	Erstellen von Benutzerprofilen
Schutz durch Software-Firewall	Zentrale Passwortvergabe
Schutz durch Hardware-Firewall	Regelmäßige Software-Updates
Einsatz von VPN bei Remote-Zugriffen mit doppelter Authentifizierung	
Automatische Desktop-Sperre	
Verschlüsselung von Notebooks	

3. Zugriffskontrolle auf bestimmte Bereiche der Datenverarbeitungssysteme

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.

Maßnahmen	
Technisch	***Organisatorisch***
Nutzung eines Aktenvernichters	Einsatz Berechtigungskonzepte
Physische Löschung von Datenträgern	Minimale Anzahl an Administratoren
Verschlüsselung von Datenträgern	Verwaltung Benutzerrechte durch Administratoren
	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Löschung von Daten
	Geregeltes Löschen/Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks

4. 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.

Maßnahmen	
Technisch	***Organisatorisch***
Einsatz von VPN	Weitergabe von Daten in anonymisierter Form
Bereitstellung über verschlüsselte Verbindungen wie https	

5. 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.

Maßnahmen	
Technisch	***Organisatorisch***
Nachvollziehbarkeit von Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
Rollenabhängige Zugriffsbeschränkungen	

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen	
Technisch	***Organisatorisch***
Fern-Zugriff erfolgt per VPN nur mit starker Verschlüsselung, erfordert eine Benutzerauthentifizierung	Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers
	Definition von Rollen für unterschiedliche Aufgaben
	Aufteilung der Zuständigkeiten
	Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
	Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung
	Schriftliche Weisung an den Auftragnehmer
	Verpflichtung der Mitarbeitenden des Auftragnehmers auf Datengeheimnis
	Verpflichtung zur Bestellung eines Datenschutzbeauftragten bei Vorliegen Bestellpflicht
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen	
Technisch	***Organisatorisch***
Feuerlöscher	Notfallplan
Erstellung von Backups	

8. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen	
Technisch	***Organisatorisch***
Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	Erstellung eines Berechtigungskonzepts
Trennung von Produktiv- und Testsystem	Festlegung von Datenbankrechten

13.06.2018
Datum

Unterschrift des Verantwortlichen

avanti
GreenSoftware
Blumenstraße 19, 70182 Stuttgart