Anlage B: Technische und organisatorische Maßnahmen zum Datenschutz

gemäß Art. 28 Abs. 3 lit. c, 32 DSGVO i.V.m. Art. 5 Abs. 1, Abs. 2 DSGVO

1. Vertraulichkeit

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der ihm übertragenen
Leistungen genutzten technischen Einrichtungen zu verwehren.
→ Beim Auftragnehmer umgesetzte Maßnahmen:

Türsicherung durch elektrischen Türöffner
Zutrittskontrolle (schlüsselbasiert)
Manuelles Schließsystem mit Sicherheitsschlössern

1.2 Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.
→ Beim Auftragnehmer umgesetzte Maßnahmen:

Anwendung von Maßnahmen zur Verschlüsselung von lokalen Daten (Server)
Arbeitsplätze werden bei Nichtbenutzung gesperrt (Automatisches Sperren von PCs)
Verwendung personalisierter Logins in Unternehmensanwendungen
Verwendung sicherer und individueller Passwörter
Sichere Aufbewahrung von Datenträgern inkl. Kennzeichnung von Kundendaten

Robert Freigang Tzschimmerstraße 34 01309 Dresden
Telefon: +49 (0)175 49 18 361 | www.streetworkapp.de | info@streetworkapp.de

1.3 Zugriffskontrolle

Es ist sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

→ Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation eingerichteter Zugänge für Mitarbeiter
Sperrung von Zugängen nach Austritt von Mitarbeitern
Berechtigungskonzept (zentrale Verwaltung von Benutzerzugängen und -rechten durch Systemadministrator)
Einführung von Benutzer- und Rollenkonzepten für interne Systeme (Zuordnung von Benutzerrechten mit restriktiver, differenzierter Rechtevergabe)
Passwortrichtlinie
eindeutige Authentifizierung mit Benutzer/Passwort
Remote-Zugänge sind verschlüsselt und in der Anzahl auf das Notwendigste beschränkt
Protokollierung Userzugriffe auf Anwendungen

1.4 Weitergabekontrolle

Es muss dafür gesorgt werden, 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 welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

→ Beim Auftragnehmer umgesetzte Maßnahmen:

Nutzung SSL-verschlüsselter Übertragungswege im Internet
Verschlüsselter Versand von E-Mails (sofern möglich/notwendig)
Werden personenbezogene Daten in Ausnahmefällen per E-Mail versandt, werden die personenbezogenen Daten ausschließlich in einem mit einem Passwort geschütztem Anhang oder getrennt voneinander versendet.
Verschlüsselung von Datenträgern
Sicherung von Dokumenten beim Versand auf dem Postweg (undurchsichtige Versandhüllen, Einschreiben zur Nachverfolgung)

Robert Freigang Tzschimmerstraße 34 01309 Dresden
Telefon: +49 (0)175 49 18 361 | www.streetworkapp.de | info@streetworkapp.de

1.5 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

→ Beim Auftragnehmer umgesetzte Maßnahmen:

Einführung von Zugriffsberechtigungen für interne Systeme
Logische Mandantentrennung (softwareseitig)
Trennung von Entwicklungs-, Test- und Produktivsystem (dev, stage, prod)
Festlegung von Datenbankrechten
Trennung von Daten verschiedener Auftraggeber

1.6 Pseudonymisierung

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

→ Beim Auftragnehmer umgesetzte Maßnahmen:

Trennung von Namen und nutzerbezogenen Daten
Verwendung von Pseudonymen (IDs) statt personenbezogener Daten

1.7 Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

→ Beim Auftragnehmer umgesetzte Maßnahmen:

Verwendung verschlüsselter Übertragungswege für den Datenaustausch
Maßnahmen zur verschlüsselten Datenspeicherung
Verwendung von SSL-Zertifikaten für Hostingumgebungen

Robert Freigang Tzschimmerstraße 34 01309 Dresden
Telefon: +49 (0)175 49 18 361 | www.streetworkapp.de | info@streetworkapp.de

2. Integrität

2.1 Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

→ Beim Auftragnehmer umgesetzte Maßnahmen:

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
Einführung individueller Zugänge für interne Systeme
Protokollierung der Eingabe, Änderung und Löschung von Daten
Festlegung von Rechten bei der Verarbeitung personenbezogener Daten

2.2 Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem. 1.4 dienen auch der Sicherstellung der Integrität.

Robert Freigang Tzschimmerstraße 34 01309 Dresden
Telefon: +49 (0)175 49 18 361 | www.streetworkapp.de | info@streetworkapp.de

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

→ Beim Auftragnehmer umgesetzte Maßnahmen:

Durchführung von Code-Reviews in der Entwicklung
Nutzung von Testverfahren (z. B. Unittests) in der Entwicklung
Nutzung einer Versionskontrolle in der Entwicklung
Regelmäßige Durchführung von Datensicherungen
Regelmäßige Überprüfung der erstellten Datensicherungen
Regelmäßige Durchführung von Updates (Windows, Mac, Linux, Desktopanwendungen)
Einsatz einer Hardware-Firewall

3.2 Rasche Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

→ Beim Auftragnehmer umgesetzte Maßnahmen:

Backup- und Recovery-Konzept erstellt und getestet
Testen von Datenwiederherstellung
Nutzung einer Versionskontrolle in der Entwicklung
RAID/Festplattenspiegelung
Nutzung von zertifizierten Rechenzentren
Dem Stand der Technik entsprechende Sicherheit im Rechenzentrum (USV, Klima, Brandschutz im Serverraum, Zugangssicherheit, Zutrittssicherheit usw.)

Robert Freigang Tzschimmerstraße 34 01309 Dresden
Telefon: +49 (0)175 49 18 361 | www.streetworkapp.de | info@streetworkapp.de

4. Weitere Maßnahmenbereiche

4.1 Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.
→ Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation von datenschutzrelevanten Zwischenfällen
Information an Auftraggeber gemäß AV-Vertrag
Regelung zu Meldepflichten an Geschäftsführer und Gesellschafter
Löschen nicht mehr benötigter Daten (unter Einhaltung ggf. vorliegender Fristen)
Sichere Entsorgung defekter/nicht mehr benötigter Hardware
Einsatz von Aktenvernichtern zur sicheren Entsorgung von Dokumenten

4.2 Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
→ Beim Auftragnehmer umgesetzte Maßnahmen:

Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
Sorgfältige Auswahl der eigenen
Mitarbeiter Regelmäßige Unterweisungen zum Datenschutz, Verpflichtung der Mitarbeiter auf das Datengeheimnis
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
Sicherstellung Rechteentzug bei Ausscheiden eines Mitarbeiters

Datum: 09.03.2022

Robert Freigang Tzschimmerstraße 34 01309 Dresden
Telefon: +49 (0)175 49 18 361 | www.streetworkapp.de | info@streetworkapp.de