Art. 32 DSGVO

Weisungsbefugte Personen

Weisungsbefugte Personen bei der Standpunkte GmbH sind:

Richard Schwimbersky, Geschäftsführung
Telefon +423 340 4242

Datenstandort

Datenstandorte sind in Liechtenstein und EU (Österreich, Deutschland)
Serverstandorte sind in Schweiz, Deutschland und Liechtenstein

Technische und organisatorische Maßnahmen

Die Standpunkte GmbH ergreift alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO.

Die Maßnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

Eingesetzte Software

- Die von der Standpunkte GmbH eingesetzte Software wird regelmäßig aktualisiert.

Hauptsoftware von der Standpunkte eingesetzt:

- FileMaker (Claris GmbH)
- Windows, Remote Desktop (Microsoft)
- MacOS (Apple)
- Teamviewer (Teamviewer GmbH)
- Nextcloud (OpenScource)

Zugangs- und Zugriffskontrolle

- Zu den Räumlichkeiten der Standpunkte GmbH haben nur autorisierte Personen Zugang.
- Eine Zugangskontrolle (Protokollierung) findet nicht statt.
- Es findet keine Zutrittskontrolle Anwendung, die über das Schliesssystem einer Wohnung hinausgeht.
- Nur Mitarbeiter der Standpunkte GmbH haben Zugriff auf die Daten der Kunden, dabei kommen unterschiedliche Zugriffsberechtigungen (Passworter, TouchID oder FaceID) zum Tragen.
- Die Kundendaten (CRM) werden in einer verschlüsselten Datenbank abgelegt (EaR).
- Kundendokumente werden in der Cloud abgelegt. Die Verbindung ist TLS verschlüsselt. Serverstandort ist Liechtenstein.
- Die Kommunikation zwischen Arbeitsplatzrechner und der Cloud, respektive der Kundendatenbank, ist verschlüsselt.
- Passwortwörter werden den Kunden separat mitgeteilt und nicht gemeinsam mit anderen Zugangsdaten.

Weitere Regulatorien

- Eine Weitergabe der Daten an Dritte, erfolgt nur nach ausdrücklicher Genehmigung, respektive Aufforderung der Kunden.

Eingesetzte Subunternehmen

- Die Standpunkte GmbH kann Subunternehmen mit der Erbringung diverser Dienstleistungen beauftragen. Dies sind:
  - Serverbase GmbH, Rümlang Schweiz (Bereitstellung von Serverinfrastruktur)
  - myloc managed IT AG, Düsseldorf Deutschland (Bereitstellung von Serverinfrastruktur)
  - Schubec GmbH, Salzburg Österreich (Programmierarbeiten)
  - Tek:Guides GmbH, Brugg, Schweiz (Programmierarbeiten)
  - T&M Hannson IT AB, Klagerup Sweden (Wartungsarbeiten Cloud-Dienste)

Anhang 4: Risikobewertung nach Art. 28 der Datenschutzgrundverordnung (EU)

1 Normal, 2 Hoch, 3 Sehr Hoch

- CRM-System der Standpunkte GmbH
- Kundendaten (Firma, Anschrift, Telefon, E-Mail):
- Kontaktdaten (Name, Vorname, Telefon, E-Mail)
- Vertragsdaten und bezogene Produkte und Dienstleistungen, Status Support-Abo
- Supportdaten (Beteiligte Personen Name, Datum, Uhrzeit, Supportfallbeschreibung)
- Passwortdaten (gespeicherte Passwörter und kundenspezifische Zugänge)

Mit Ausnahme der Vertraulichkeit der Passwortdaten (Risiko 2 Hoch) sind alle CRM mit dem Risiko 1 (Normal) zu bewerten.

Bewertung Passwortdaten

Die gespeicherten Passwortdaten erlauben den Zugriff auf Systeme der Kunden mit zum Teil sensiblen Daten.

Maßnahmen

M. V 1 Schutz der Passwortdaten

Gespeicherte Passwortdaten werden in einer gesonderten Tabelle des CRM anonymisiert gespeichert. Die Tabelle (wie das ganze CRM-System) sind mit AES-256 verschlüsselt. Die Kommunikation zwischen Arbeitsplatz des Standpunkte-Mitarbeiters und dem CRM-Server ist mit SSL/TLS verschlüsselt. Durch diese Maßnahme wird das Risiko auf die Stufe "Normal" gesenkt

Weitere kundenspezifische Daten und Dateien die der Standpunkte anvertraut werden

- OPTIpin (OPTIpin Datenbanklösung, sowie OPTIflex)
- OPTItouch Dateien
- Schnittstellendateien (z.B. Export aus OPTIback, TurboBack)
- Produktspezifikationen (Lebensmitteldaten von Lieferanten (LMIV))
- Lieferanten-Artikelstammdaten (z.B. Pistor)

Mit Ausnahme der Vertraulichkeit bei OPTIpin und den Schnittstellendateien (Risiko 2 Hoch) sind die Risiken mit 1 (Normal) zu bewerten.

Bewertung OPTIpin und Schnittstellendateien

Die in OPTIpin, sowie den Schnittstellendateien gespeicherten Daten erlauben Einblick in die Rezepturen der Produkte der Kunden

Maßnahmen

M. V 2 Schutz von OPTIpin

OPTIpin Dateien sind durch Passwörter geschützt. OPTIpin verwendet ein Standardpasswort sowie eine Autolog-Möglichkeit, die vom Kunden geändert, respektive deaktiviert werden kann. Dateien werden von der Standpunkte GmbH ausschließlich über eine TSL/SSL verschlüsselte Verbindung übermittelt und bei der Standpunkte GmbH Cloud zur Bearbeitung gespeichert. Nach der Bearbeitung und Freigabe der Arbeit durch den Kunden werden die Dateien sofort gelöscht.

M. V 1 Schutz von Schnittstellendateien

Werden die Schnittstellendateien von Kunden mittels E-Mail übermittelt, obliegt es den Kunden diese gegebenenfalls in ein passwortgeschütztes Zip-Archiv zu packen. Von der Standpunkte GmbH werden die Dateien ausschließlich über eine TSL/SSL verschlüsselte Verbindung übermittelt. Nach der Bearbeitung und Freigabe der Arbeit durch den Kunden werden die Dateien sofort gelöscht.
Durch diese Maßnahmen wird das Risiko auf die Stufe "Normal" gesenkt.

Ruggell, 20.01.2023

STANDPUNKTE GMBH
Industriering 20
9491 RUGGELL
LIECHTENSTEIN

TELEFON 00423 340 42 42

INFO@STANDPUNKTE.LI
WWW.STANDPUNKTE.LI