PTV LOGISTICS

Allgemeine und technische organisatorische Maßnahmen

PTV Logistics GmbH, Sitz der Gesellschaft / Registered Office: Karlsruhe, Geschäftsführung / Management Board: Steven De Schrijver (Vors./CEO), An De Wispelaere (CPO), Dr. Marco Di Matteo, Claudia Wenzel, Handelsregister (HRB Nr.) / Commercial Register (HRB No.): 745512, USt-ID-Nr. / VAT ID No.: 35007/25076, Registergericht / Court of Registration: Mannheim.

Inhalt

Kurztitel	TOMs
Vorlagenhistorie	V1.0.0 vom 22.08.2023

Technische und organisatorische Maßnahmen (TOMs)

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutz-gesetze zu gewährleisten (Art. 32 DSGVO). Die Maßnahmen müssen geeignet sein, die personenbezogenen Daten entsprechend ihrer Art und ihrer Kategorie an-gemessen zu schützen. Erforderlich sind die Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Um den Anforderungen an die Sicherheit der Datenverarbeitung gerecht zu werden, ergreift die PTV Logistics GmbH folgende Maßnahmen:

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

1.1. Zutrittskontrolle

Kein unbefugter Zutritt zu Gebäude und Rechenzentrum

- Sorgfältig ausgewählter Wachdienst
- Videoüberwachung der Eingangsbereiche des Gebäudes und des Rechenzentrums
- Gebäudezutritt nur mittels Chip-Key (Transpondersystem)
- Vergabe der Chip-Keys erfolgt unter Berücksichtigung des Zutrittsberechtigungs-konzepts der Zutrittsmanagementsoftware. Über die Vergabe wird eine Liste geführt. Erteilung und Änderungen der Berechtigung nur unter Wahrung des 4-Augen-Prinzips
- Innerhalb des Gebäudes gewährt Chip-Key nur unter Berücksichtigung der Geschäftszeiten und der Berechtigungsgruppe Zutritt zu spezifischen Bereichen
- Besetzter Empfang während der Öffnungszeiten. Einlass von Besuchern nur nach Klingeln, öffnen der Zugangstür durch Empfangsmitarbeiter
- Führung eines Besucherbuches mit Besucherprotokoll
- Aufenthalt von Besuchern im Gebäude nur mit Besucherausweis und in Begleitung eines PTV Mitarbeiters.
- Sicherung sensibler Bereiche durch Sicherheitsschlösser, Schließsysteme nur mit entsprechender Berechtigung mittels Chip-Key (Bspw. Serverraum)
- Sorgfältige Auswahl externer Dienstleister, bspw. des Reinigungspersonals. Verpflichtung zur Einhaltung von Datenschutz und Verschwiegenheit
- Aufenthalt von Handwerkern nur in Begleitung von Mitarbeitern des Facilitymanagements.
- Absicherung der Gebäudeschächte

1.2. Zugangskontrolle

Keine unbefugte Systembenutzung

- Login mit Benutzername und entweder Passwort oder Pin
- Richtlinien zu: „Sicheres Passwort“, Passwort ist nur einstellbar, wenn die Sicherheitsanforderungen eingehalten sind
- Anti-Viren-Software für Server, Clients, mobile Geräte
- Firewall
- Mobile Device Systeme, Richtlinie zu Nutzung und Passwortvergabe
- Zeitliche Begrenzung der Passwortgültigkeit und Passworthistorie
- Verschlüsselung von Datenträgern, Notebookfestplatten und Smartphones
- Verwalten der Benutzerberechtigungen
- Richtlinie und Voreinstellung “Desktopsperre“, Reaktivierung Passwortgeschützt

1.3. Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen

- Berechtigungs- und Administrationskonzept vorhanden, minimale Anzahl an Administratoren
- Konzept für Beantragung und Genehmigung von Berechtigungen
- Benutzerrollen- / Gruppenkonzept
- Verwaltung der Benutzerrechte durch Administratoren
- Zugriffsprüfung per Protokoll bei Eingabe, Änderung und Löschung
- Externer Aktenvernichter (DIN 32757) und gesicherte Verwahrung der zur Vernichtung bereitgestellten Dokumente

1.4. Trennungskontrolle:

Getrennte Verarbeitung von Daten, die unterschiedlichen Zwecken dienen

- Verarbeitung der Unternehmensdaten getrennt von den jeweiligen Kundendaten
- Trennung von relevanten Produktiv- und Testumgebung
- Mandantenfähigkeit relevanter Anwendungen

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a; 25 Abs. 1 DSGVO)

Vorrang der Verarbeitung pseudonymisierter Daten, soweit dies möglich ist

- Interne Anweisung personenbezogene Daten im Falle einer Weitergabe möglichst zu anonymisieren/pseudonymisieren
- Getrennte Aufbewahrung von pseudonymisierten Daten und Zuordnungsdaten in getrenntem und abgesichertem System

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

2.1. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

- VPN-Verwendung
- Verschlüsselung der Notebook-Festplatten
- Protokollierung von unerlaubten externen Zugriffsversuchen
- Bereitstellung über verschlüsselte Verbindungen (sftp, https)

2.2. Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Systeme eingegeben, verändert oder entfernt worden sind

- Protokollierung aller Eingaben in relevanten Programmen
- Übersicht über Programme, mittels derer Daten eingegeben, geändert oder gelöscht werden können
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Klare Zuständigkeiten für Löschungen

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

3.1. Verfügbarkeitskontrolle

- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
- Feuer- und Rauchmeldeanlagen
- Klimatisierung und Überwachung des Serverraums (Temperatur und Feuchtigkeit); Videoüberwachung, CO2-Feuerlöscher
- USV
- Schutzsteckdosenleisten im Serverraum
- RAID-Festplattenspeicher
- Backup- und Recoverykonzept (ausformuliert)
- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Tägliche bis jährliche Sicherung, Zusatzsicherungen und getestete Rücksicherungen,
- Getestetes Notfallkonzept
- Virenscanner und mehrstufige Firewalls
- Regelmäßige Software-Updates
- Aufbewahrung der Sicherungen in speziell geeigneten Datentresoren

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d; 25 Abs. 1 DSG-VO)

4.1. Auftragskontrolle (Outsourcing an Dritte)

- Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsvereinbarung bzw. Standardvertragsklauseln der EU
- Schriftliche Weisungen an Auftragsnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen einer Verpflichtung
- Vereinbarung wirksamer Kontrollrechte
- Regelungen zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

4.2. Datenschutz-Management

Gemeinsam mit dem externen Datenschutzbeauftragten wird ein Datenschutzmanagementsystem (DSMS) geführt, in dem alle Maßnahmen, Verfahren, Tätigkeiten etc. abgebildet werden. Das DSMS beinhaltet die wichtigsten

datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaß-nahmen. Das DSMS wird laufend gepflegt und aktualisiert. Unterstützung des Datenschutzbeauftragten durch interne Datenschutzkoordinatoren.

- Unsere Mitarbeiter werden auf die Einhaltung des Datenschutzes und Vertraulichkeit verpflichtet, Schulungen
- Durchführung von Datenschutz-Folgeabschätzungen (DSFA) bei Bedarf
- Beachtung der Informationspflichten nach Art. 13, 14 DSGVO bei Organisation

4.3. Incident-Response-Management

Ein organisatorischer und technischer Prozess zum Umgang mit Sicherheitsvorfällen (incidents) ist definiert und implementiert. Hierüber wird auch eine einheitliche Reaktion sowie ein prozessualisierter Umgang mit erkannten und vermuteten Sicherheitsvorfällen/Störungen sichergestellt. Ebenfalls erfolgt im Rahmen dessen eine einheitliche Nachbereitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.

- Einsatz von Firewall, Spamfiltern und Virenscannern. Regelmäßige Aktualisierung
- IT-Ticket-System bei Incident
- Einbindung von Datenschutzbeauftragten und Informationssicherheitsbeauftragtem

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

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden.

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maß-nahmen

5. Datenschutzbeauftragter

Die PTV Logistics GmbH hat einen externen Datenschutzbeauftragten bestellt (Art. 38 und 39 DSGVO). Dieser ist erreichbar unter:

E-Mail: datenschutz@ptvlogistics.com