Anhang 3 – Technische und organisatorische Maßnahmen zur Datensicherheit

gemäß Art. 32 DSGVO (als Auftragsverarbeiter)

1. Gegenstand

Dieses Dokument beschreibt die durch die PTC Telematik GmbH (nachfolgend „**Unternehmen**“) getroffenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten, soweit das Unternehmen als Auftragsverarbeiter handelt.

Die Maßnahmen beziehen sich auf folgende Verarbeitungen:

- Bereitstellung eines Online-Portals zur Darstellung satellitengestützter Ortungsdaten von Fahrzeugen.
- Speicherung satellitengestützter Telemetriedaten und deren Verarbeitung gemäß Servicevertrag.
- Auswertung fahrzeugbezogener Ortungsdaten.
- Erfassung der Daten eines RFID-Lesegerätes, sofern im Fahrzeug vorhanden.
- Verarbeitung von Kassendaten, sofern vereinbarungsgemäß vom Kassensystem übertragen.
- Versand von Emails und Newsletter, ggf. durch Unter-Auftragsverarbeiter mit denen
- eine separate Datenverarbeitungsvereinbarung getroffen wird.

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

Die personenbezogenen Daten werden im Rechenzentrum Telehouse Deutschland GmbH, Kleyerstrasse 75-87, 60326 Frankfurt in Colocation auf eigenen Servern gespeichert.

2.1 Zutrittskontrolle

Das Rechenzentrum Telehouse Deutschland GmbH garantiert die folgenden Sicherheitsmaßnahmen:

- Sicherheitssysteme
- Videoüberwachung von Außenbereichen mit Aufzeichnung über einen Zeitraum von drei Monaten
- Die Anlage ist mit einem Zaun mit Erkennungssystem umgeben
- 24/7 besetztes Kontrollzentrum auf dem Rechenzentrumsgelände – Fehlermeldungen werden über ein zentralisiertes Kontrollsystem gemeldet
- 24/7 Sicherheitspersonal vor Ort
- Es wird ein strenges Verfahren für die Zugangsberechtigungen verfolgt

Der Zugang der eigenen Mitarbeiter erfolgt über besondere Ausweisdokumente.

- Die Ausweisdokumente werden namentlich erfasst.
- Soweit kein namentlich bestimmtes Ausweisdokument ausgegeben wurde, erfolgt die schriftliche Anmeldung online.
- Dabei werden die Namen der Mitarbeiter oder beauftragter Techniker namentlich festgehalten und die genauen Zutrittszeiten bestimmt.

2.2 Zugangskontrolle

- Für die Kennwörter zur Anmeldung an der internen Windows-Domäne ist eine automatische Kennwortrichtlinie aktiviert, die Kennwortlänge und Komplexität erzwingt.
- Die Kennwörter zur Infrastruktur werden mit einer Mindestlänge von einem Kennwortgenerator (KeePass2) erzeugt und in regelmäßigen Abständen geändert.
- Auf den Windows-Arbeitsplätzen der Mitarbeiter ist Windows Defender oder Bit Defender als Virenschutz installiert.
- Für den Zugriff von Mitarbeitern an externen Standorten werden ausschließlich sichere VPN-Verbindungen (OpenVPN) genutzt.
- Die Mitarbeiter werden darauf hingewiesen, dass sie bei jedem Verlassen des Arbeitsplatzes ihren Bildschirm gleich sperren müssen.

2.3 Zugriffskontrolle

- Die verwendeten internen Systeme (Windows-Domäne, GitLab, Atlassian Confluence, Atlassian Jira, Atlassian Stride, United Planet Intrexx) erlauben eine Zugriffskontrolle auf Benutzer- und Gruppenebene.
- Die Herausgabe von Zugangsdaten erfolgt nach dem Need-to-Know-Prinzip. Mitarbeiter erhalten nur Zugangsdaten, die für ihre Arbeit relevant sind.
- Beim Ausscheiden von Mitarbeitern werden alle Zugänge entsprechend der internen Richtlinie gelöscht/gesperrt.
- Die Anzahl der administrativen Zugänge zu allen Systemen ist auf das notwendige Maß (Geschäftsleitung, Prokura, Entwicklungsleiter, Datensicherheits-Manager) begrenzt.
- Geschäftskritische Kennwörter werden ausschließlich in verschlüsselten Datenbanken (KeePass2) gespeichert.
- Papierakten mit personenbezogenen Daten werden mit einem geeignetem Aktenvernichter zerstört.
- Die Herausgabe von Zugangsdaten erfolgt nach dem Need-to-Know Prinzip.
    - Neue Mitarbeiter erhalten nur die Zugangsdaten, die für ihre Arbeit relevant sind.
    - Beim Ausscheiden von Mitarbeitern werden alle Zugänge und damit die Zugriffsrechte gelöscht / gesperrt.
    - Beim Wechsel der Aufgabenverteilung wird entsprechend verfahren. Soweit erforderlich, werden Zugriffsrechte über Zugangsdaten eingeräumt oder nicht mehr benötigte Zugriffsrechte eingeschränkt und die Zugangsdaten gelöscht / gesperrt.

2.4 Trennung

- Es besteht eine klare Trennung zwischen Produktiv- und Testsystemen, die auf jeweils unterschiedlichen Servern betrieben werden.
- Die Daten einzelner Kunden werden durch die Mandantenfähigkeit des Online-Portals logisch separiert. Die Speicherdauer kann je Mandant getrennt eingestellt werden.

2.5 Verschlüsselung (Art 32 Abs. 1 lit. a) DSGVO)

- Daten zwischen allen Websites, inklusive des Online-Portals, und den Benutzern, werden SSL-verschlüsselt übertragen.

2.6 Pseudonymisierung (Art 32 Abs. 1 lit. a) DSGVO)

- Die IP-Adresse von Besuchern öffentlicher Websites wird vom verwendeten Tracking-System Matoma pseudonymisiert (letzte 2 von 4 Stellen) gespeichert.
- Die GPS-Daten werden pseudonymisiert gesammelt und erst einem Fahrer und damit einer Person zugeordnet, wenn der Kunde dies aktiviert.

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

3.1 Eingabekontrolle

- Bei der Fahrtenbuch-Anwendung werden entsprechen den gesetzlichen Vorgaben alle Eingaben, Änderungen und Löschungen protokolliert.

3.2 Weitergabekontrolle

- Mitarbeiter wählen sich auf die Server-Systeme ausschließlich per verschlüsselter SSHVerbindung ein oder bei der Verwendung von RDP durch ein VPN-Netzwerk.

4. Verfügbarkeit (Art 32 Abs. 1 lit. b) DSGVO)

- Die Auslastung der Server-Systeme wird ständig überwacht (Icinga2 und pnp4nagios), so dass zuständige Mitarbeiter rasch auf Ausnahmesituationen reagieren können.
- Alle Daten werden auf redundanten RAID-Systemen gespeichert, die mit Hot-Spare-Festplatten ausgestattet sind, welche bei Ausfall sofort einspringen.
- Von den personenbezogenen Daten und den zur Verarbeitung notwendigen Systemen werden regelmäßig Backups nach dem festgelegten Backup-Konzept erstellt.

Das Rechenzentrum Telehouse Deutschland GmbH garantiert die folgenden Spezifikationen:

4.1.1 Stromversorgung

- Stromversorgung der Racks bis zu 8kW mit höher skalierbaren Optionen
- N+1 redundante mit USV unterstützte Stromversorgung mit Batterie Backup
- Bis zu 21MVA unterbrechungsfreie Energieversorgung
- Sub-Verteilung nach Angaben des Kunden mit separater Strommessung
- Das Data Center kann im Falle eines Stromausfalls vollkommen autonom mit Dieselgeneratoren betrieben werden

4.1.2 Umgebung und Klimaanlage

- Redundante Klimaanlage und Kühlsysteme bei N 1
- Raumtemperatur wird bei 24°C 2/- 4°C gehalten
- Die Temperaturen in den Datenzentren werden von Sensoren überwacht
- Relative Luftfeuchtigkeit zwischen 50% bis 15%
- Tragfähigkeit des Bodens liegt zwischen 5 bis 15 kN / m2
- Doppelboden zwischen 300-700 mm

4.1.3 Connectivity

- Eine Carrier- neutrale Anlage bietet Kunden die Freiheit der Wahl für die Konnektivität mit Zugang zu mehreren wichtigen lokalen und internationalen Netzbetreibern
- Optimale Verbindung zum deutschen Internet Exchange Hub (DE-CIX)
- Direkter Anschluss an den Frankfurter Glasfaser Ring

4.1.4 Branderkennungs- und Löschsysteme

- Optische / thermische Brandmelder auf zwei Ebenen (Decke und Doppelboden)
- Aktive inerte Feuerlöschanlagen
- Brandfrüherkennung (RAS -System)
- Wahl zwischen Räumen mit aktivem oder passivem Brandschutz

4.1.5 Weitere Spezifikationen

- 24/7 Überwachung und Remote Hands Dienstleistungen
- 24/7 Betrieb in einer sicheren und hochverfügbaren Umgebung, Inhouse- Verkabelung und Facility Management durch geschultes Personal
- Telehouse Frankfurt erfüllt die Tier 3 Klassifikation mit optionalen Multi-Tier Bereichen
- Vor Ort verfügbar Bereiche für den Bau von privaten Tier 4 Data Centers • Telehouse Frankfurt ist nach IDW PS951 (deutsches Zertifikat entspricht dem Statement on Auditing Standards (SAS) Nr. 70)
- Telehouse Frankfurt erhielt das Zertifikat ISO 27001:2005 (Information Security Management)

4.2 Insbesondere: Wiederherstellbarkeit nach Zwischenfall (Art 32 Abs. 1 lit. c) DSGVO)

- Zur raschen Wiederherstellbarkeit nach einem Serverausfall werden die Kundendaten auf einem dreifach redundanten Datenbankcluster (PostgreSQL) vorgehalten.
- Die Anwendungsserver werden in einer virtualisierten Serverumgebung (Proxmox) betrieben, die nach einem Serverausfall eine Wiederherstellung auf einen beliebigen anderen Node des Clusters ermöglicht.

4.3 Insbesondere: Belastbarkeit (Art 32 Abs. 1 lit. b) DSGVO)

- Die Produktivsysteme verfügen über eine redundante Netzwerkanbindung des Uplinks, Router, Switche, Verkabelung und Netzwerkkarten. Die Systeme sind für automatisches Failover konfiguriert.

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

- Vor der Inbetriebnahme größerer Änderungen an der Server-Infrastruktur wird ein Belastungstest auf einem redundanten System durchgeführt.

6. Weitere organisatorische Maßnahmen / Auftragskontrolle

Das Unternehmen hat eine für alle Mitarbeiter verbindliche Richtlinie zur Auftragsverarbeitung erlassen. Diese Richtlinie regelt unter anderem:

- Rollen und Verantwortlichkeiten (Datenschutzbeauftragter, Datenschutz-Manager, Datensicherheits-Manager)
- Verantwortlichkeiten und Prozesse zum Abschluss von Auftragsverarbeitungs-Verträgen mit Auftraggebern, einschließlich deren Prüfung
- Verantwortlichkeiten und Prozesse bei der Einschaltung von weiteren Auftragsverarbeitern (Unter-Auftragsverarbeitern), einschließlich der Kontrolle und
- Vertragsprüfung
- Verantwortlichkeiten und Prozesse zum Umgang mit Weisungen von Auftraggebern und zur Sicherstellung der Zweckbindung bei der Auftragsverarbeitung
- Regelungen für die Rückgabe und Löschung von Daten bei Ende der
- Auftragsverarbeitung
- Verantwortlichkeiten und Prozesse für den Umgang mit Anträgen von Betroffenen in Bezug auf Betroffenenrechte
- Verantwortlichkeiten und Prozesse für die Führung eines Verzeichnisses der

Verarbeitungstätigkeiten (als Auftragsverarbeiter)

- Regelungen zur Erkennung von Datenschutzvorfällen und Meldung an den Auftraggeber
- Sicherstellung der Verpflichtung der Beschäftigten zur Vertraulichkeit
- Verfahren zur Überprüfung und Anpassung der Richtlinie zur Auftragsverarbeitung

Das Unternehmen nutzt zudem einen standardisierten Vertrag für die Einschaltung von Unter-Auftragsverarbeitern sowie eine Checkliste zur Prüfung von Auftragsverarbeitungsverträgen.

Version: 1.3 / Stand: 18.02.2020