TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Gültig ab: 01. Juli 2024

INHALTSVERZEICHNIS

1. Einleitung

1.1 Diese Beschreibung der technischen und organisatorischen Maßnahmen im Sinne des Art. 32 DSGVO erfolgt in Einklang mit Punkt 4.2 des Anhangs A (Vereinbarung zur Auftragsverarbeitung) zu den Allgemeinen Geschäftsbedingungen (AGB) der Rosenberger Telematics GmbH, FN 317674v, Atterseestraße 56, A-4850 Timelkam (im Folgenden „*Rosenberger Telematics*“).

1.2 Für die Zwecke dieser Beschreibung kommen die Begriffsbestimmungen des Anhangs A zu den AGB zur Anwendung.

1.3 Rosenberger Telematics wird diese Beschreibung von Zeit zu Zeit aktualisieren.

2. Vertraulichkeit

2.1 Zutrittskontrolle:

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie vertraulichen Akten und Datenträgern physisch verwehren:

- Siehe Datenschutzerklärung conova communications GmbH [https://www.conova.com/datenschutz/]
- Gesonderte Sicherheitsbereiche (z.B. Serverraum)
- Alarmanlage
- Zutritt zu Büroräumlichkeiten und Firmengelände mit RFID-Token oder Schlüssel
- Protokollierte Ausgabe von Schlüsseln (Büro)

2.2 Zugangskontrolle:

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können:

- personifizierte Nutzerkennungen
- Einrichtung eines Benutzerstammsatzes pro User
- Kennwortverfahren
- Authentifizierungsverfahren (z.B.: 2-Faktor Authentifizierung)
- Sperrung von Arbeitsplätzen bei Inaktivität (Time Out des Security Tokens)
- Verschlüsselung von Datenträgern
- Abkapselung von sensiblen Systemen durch getrennte Netzbereiche
- Protokollierung der Anmeldeversuche
- Regelmäßig aktualisierte Antiviren- und Spywarefilter

TECHNICAL AND ORGANIZATIONAL MEASURES

Valid from: 1st of July 2024

TABLE OF CONTENTS

1. Introduction

1.1 This description of the technical and organizational measures within the meaning of art. 32 GDPR is provided in accordance with section 4.2 of appendix A (Data Processing Agreement) to the General Terms and Conditions (GTC) of Rosenberger Telematics GmbH, Reg. No. 317674v, Atterseestraße 56, A-4850 Timelkam (hereinafter "*Rosenberger Telematics*").

1.2 For the purposes of this description, the definitions of appendix A to the GTC shall apply.

1.3 Rosenberger Telematics may amend this description from time to time.

2. Confidentiality

2.1 Entry Control:

Measures that physically prevent unauthorized persons from gaining access to IT systems and data processing equipment used to process personal data, as well as to confidential files and data carriers:

- See privacy policy conova communications GmbH [https://www.conova.com/datenschutz/]
- Separate security areas (e.g., server room)
- Alarm system
- Access to offices and company premises with RFID tokens or keys
- Logged issue of keys (office)

2.2 Access Control:

Measures that prevent unauthorized persons from processing or using data protected under data protection law:

- Personalized user IDs
- Creation of a user master record for each user
- Password procedures
- Authentication procedures (e.g., 2-factor authentication)
- Blocking of workstations in case of inactivity (time-out of the security token)
- Encryption of data carriers
- Encapsulation of sensitive systems through separate network areas
- Logging of login attempts
- Regularly updated antivirus and spyware filters
- Multiple hardware and software firewall shielding of

— Mehrfache Hardware- und Software Firewall-Abschirmung der Kundenserver

2.3 Zugriffskontrolle:

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, sodass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

— Siehe Datenschutzerklärung conova communications GmbH [https://www.conova.com/datenschutz/]

— Protokollierung von Zugriffen auf Positionsdaten (optional) und von Veränderungen von Stammdaten

— Benutzerverwaltung und Rechtekonzept (insbesondere Fileserver)

— Abschließbare Container an den Arbeitsplätzen

— Berechtigungsvergabe auf Ebene von Rollen, Profilen, Gruppen und Feldern

— Sicherung der referenziellen Integrität; Zugriffsschutz und Sperrung

— LDAP-Anbindung

— 2-Faktor-Authentifizierung (optional)

— Single-Sign-On (SSO) Integrationen (optional)

2.4 Trennungsgebot:

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist:

— Berechtigungskonzepte

— System aus Lese-/Schreibberechtigungen für Installations-Ordner

— Abgetrenntes Gäste-WLAN

— Trennung von Test- und Produktivsystemen

— Getrennte Definition von Datenobjekten und Präsentationsobjekten

2.5 Pseudonymisierung:

— Maßnahmen, entsprechend Art. 4 Ziffer 5 DSGVO

3. Integrität

3.1 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, sowie Maßnahmen, mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist:

— Übermittlung von Daten über verschlüsselte Container oder Tunnelverbindungen

— Firewallsysteme

— HTTPS-Verschlüsselung

— Optional VPN-Zugriff in geschütztem Unternehmensnetzwerk möglich

— Aufbereitung von Datenbankabfragen im Server und Rückgabe von Anfrage-/Suchergebnissen in aufbereiteter Form mit definiertem Datenumfang zur Verhinderung von SQL-Injections

3.2 Eingabekontrolle:

customer servers

2.3 Data access control:

Measures that ensure that those authorized to use the data processing procedures can only access the personal data subject to their access authorization, so that data cannot be read, copied, modified, or removed without authorization during processing, use and storage:

— See data protection declaration conova communications GmbH [https://www.conova.com/datenschutz/]

— Logging of access to position data (optional) and changes to master data

— User administration and rights concept (especially file server)

— Lockable containers at the workstations

— Authorization assignment at the level of roles, profiles, groups and fields

— Securing referential integrity; access protection and locking

— LDAP connection

— 2-factor authentication (optional)

— Single sign-on (SSO) integrations (optional)

2.4 Requirement of Separation:

Measures that ensure that data collected for different purposes is processed separately and is separated from other data and systems in such a way that unplanned use of this data for other purposes is excluded:

— Authorization concepts

— System of read/write permissions for installation folders

— Separate guest WIFI

— Separation of test and production systems

— Separate definition of data objects and presentation objects

2.5 Pseudonymization:

— Measures in accordance with Article 4 (5) GDPR

3. Integrity

3.1 Transfer control:

Measures to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or during transport or storage on data carriers, and measures to verify and establish to which bodies personal data is intended to be transmitted:

— Transmission of data via encrypted containers or tunnel connections

— Firewall systems

— HTTPS encryption

— Optional VPN access in protected company network possible

— Preparation of database queries on the server and return of queries/search results in prepared form with defined data scope to prevent SQL injections

3.2 Input control:

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

- Protokollierung wesentlicher Systemaktivitäten und Aufbewahrung dieser Protokolle

3.3 Authentizität:

Maßnahmen, die Echtheit, Zuverlässigkeit und Glaubwürdigkeit einer Mitteilung sicherstellen. Ein Angriff wäre die unbefugte Erzeugung von Nachrichten z.B. unter falscher Identität. Auch die Authentizität von IT-Systemen muss gewährleistet sein.

- Identifikation des Senders über eindeutige IDs
- Datenübermittlung weitestgehend in proprietären Formaten
- DTLS- bzw. TLS-Verschlüsselung bei diversen Produkten

4. Verfügbarkeit und Belastbarkeit

4.1 Verfügbarkeitskontrolle:

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Siehe Datenschutzerklärung conova communications GmbH [https://www.conova.com/datenschutz/]

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Auftragskontrolle:

Maßnahmen, die gewährleisten, dass in einem Auftragsdatenverarbeitungsverhältnis gemäß Art 28 DSGVO jede Verarbeitung von personenbezogenen Daten nur im Rahmen der ergangenen Weisungen und Vorgaben des Verantwortlichen erfolgt:

- Festlegung von Weisungsbefugnissen
- Kontrollrechte bei Auftragsdatenverarbeitern
- Vergabe von Aufträgen ausschließlich über Ticketing-System

5.2 Datenschutzmanagement:

Das Datenschutzmanagement beschreibt eine Methode, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren.

5.3 Incident-Response-Management:

Entwicklung und Darstellung des Prozesses im Fall erkannter oder vermuteter Sicherheitsvorfälle/Störungen im IT-Bereich.

- Incident-Response-Management wurde eingerichtet.

5.4 Datenschutzfreundliche Voreinstellungen (Privacy by Default):

Ein Produkt oder ein Dienst weist ohne weiteres Zutun beim ersten Einschalten bzw. Aufruf die datenschutzfreundlichsten Einstellungen und Komponenten auf. Beispiel: Verzicht auf vorangekreuzte Einwilligungserklärungen oder ähnliche vorausgewählte Einstellungen. Es soll nicht ausreichen, dass ein Nutzer Wahl- und Gestaltungsmöglichkeiten hat.

- Beachtung datenschutzfreundlicher Voreinstellungen

5.5 Datenschutz durch Technik (Privacy by Design):

Technische und organisatorische Maßnahmen zur Datenvermeidung, z.B. Pseudonymisierung, Verschlüsselung, Zugangs- und Zutrittskontrollen, Anonymisierung.

Datenschutzbeauftragter:

Klaus Floth
klaus.floth@rosenberger.com
+43 7672 94429 0

- Beachtung des Datenschutzes durch Technik. Siehe dazu

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, changed or removed from IT systems:

- Logging of significant system activities and storage of these logs

3.3 Authenticity:

Measures that ensure the authenticity, reliability, and credibility of a message. An attack would be the unauthorized generation of messages, e.g., under a false identity. The authenticity of IT systems must also be guaranteed.

- Sender identification through unique IDs
- Data transfer mainly in proprietary formats
- DTLS- /TLS-encryption on various products

4. Availability and resilience

4.1 Availability control:

Measures to ensure that personal data is protected against accidental destruction or loss:

- See privacy policy conova communications GmbH [https://www.conova.com/datenschutz/]

5. Procedures for regular review, assessment, and evaluation

5.1 Order control:

Measures to ensure that, in a data processing relationship pursuant to Article 28 GDPR, any processing of personal data only takes place within the framework of the instructions and specifications by the controller:

- Definition of authority to issue instructions
- Control rights for commissioned data processors
- Order placement only via ticketing-system

5.2 Data protection management:

Data protection management describes a method for systematically planning, organizing, controlling, and monitoring the legal and operational requirements of data protection.

5.3 Incident response management:

Development and presentation of the process in the event of recognized or suspected security incidents/malfunctions in the IT area.

- Incident response management has been set up.

5.4 Privacy by Default:

A product or service has the most privacy-friendly settings and components when it is first switched on or accessed without any further action. Example: No pre-ticked consent forms or similar pre-selected settings. It should not be sufficient for a user to have choices and configuration options.

- Compliance with Privacy by Default

5.5 Privacy by Design:

Technical and organizational measures for data avoidance, e.g., pseudonymization, encryption and access controls, anonymization.

Data privacy officer:

Klaus Floth
klaus.floth@rosenberger.com
+43 7672 94429 0

- Compliance with Privacy by Design. See also the

schon die oben dargestellten Maßnahmen.

6. Maßgebliche Sprache

6.1 Die englische Fassung dieser Beschreibung dient lediglich Informationszwecken. Im Falle eines Widerspruchs zwischen der deutschen und der englischen Fassung geht die deutsche Fassung vor.

measures described above.

6. Relevant Language

6.1 The English Version of this description is for information purposes only. In the event of a conflict between the German and the English version, the German version shall prevail.