idem telematics

A member of the BPW Group

Technische und organisatorische Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO

(Stand November 2022)

1. Zutrittskontrolle

- Einsatz von Alarmanlagen inkl. Bewegungsmelder (Standort Ulm)
- Dokumentierte Schlüsselverwaltung (Schlüssel werden ausschließlich an Mitarbeiter ausgehändigt)
- Besucher
  - Besuch nur während der Besucherzeiten (reguläre Geschäftszeiten); Ausnahmen nur mit vorheriger Genehmigung
  - Beaufsichtigung des Besuchs (d.h. nur in Begleitung)
- Protokollierungskonzept
  - Zutritt zum Server- und Fernwartungsraum ausschließlich mit Dongle oder Schlüssel (Personenkreis stark eingeschränkt)
  - Zutrittskontrollsystem zum Fernwartungsraum
  - Dokumentation über Zugang des Fernwartungsraum
  - Auswertungen des Zutrittskontrollsystems
- IT-Serveradministration
  - Ausschließlich durch die IT-Abteilung

2. Zugangskontrolle

- Bestehendes Berechtigungskonzept zur Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten (durch Active Directory geregelt)
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerrechten
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das Team Operations reduziert
- Zugangsberechtigungskonzept
  - Einweisung aller Mitarbeiter in dem Umgang mit Authentifizierungsverfahren und – mechanismen (Einverständiserklärung zur IT-Richtlinie)
  - Geregelter Prozess zur zentralen Verwaltung von Benutzeridentitäten, insbesondere zur Anlage (z.B. neue Mitarbeiter), Änderungen (z.B. Namenswechsel nach Heirat) und Löschung (z.B. Weggang Mitarbeiter)
  - Vergabe von eindeutigen Kennungen für jeden Nutzer
  - Möglichst automatische Umsetzung der Passwortrichtlinie für starke Passwörter im Rahmen der IT-Richtlinie für die Active Directory in den Systemen mit Nutzererkennungen
  - Passwörter werden auch nach einem Sicherheitsvorfall auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden
  - Bei erstmaligem Login eines neuen Nutzers oder Zurücksetzung des Passworts durch IT (z.B. bei Vergessen des Passworts) muss eine Passwortänderung durch den Nutzer erfolgen
  - Passwörter dürfen nicht weitergegeben werden (auch nicht an Kollegen, Vorgesetzten oder die IT-Abteilung) – im Ausnahmefall (z.B. längere Erkrankungen) wird das Passwort durch die IT zurückgesetzt und dieser Vorgang dokumentiert

idem telematics GmbH · info@idemtelematics.com · www.idemtelematics.com

Geschäftsführer: Jens Zeller, Thomas Piller · Amtsgericht München · HRB 154698 · USt-Id: DE239143054 · Steuernr.: 143148/40454
Sitz der Gesellschaft München · Lazarettstraße 4 · D-80636 München · T +49 89 720 13 67-0 · F +49 89 720 13 67-29
Standort Ulm · Riedweg 5 · D-89081 Ulm · T +49 731 936 97-0 · F +49 731 936 97-79

- Unterrichtung an Mitarbeiter, dass Passwörter nicht auf Zettel oder Pinnwände aufgezeichnet werden dürfen (IT-Richtlinie)
- Keine Passwörter per E-Mail übermitteln
- Automatische Sperrung über 60 Minuten von Zugängen bei fünf Fehlversuchen durch falsches Passwort
- Darstellung der Anzahl der fehlgeschlagenen Logins für einen Nutzer, der sich erfolgreich angemeldet
- Passwörter in den relevanten Datenbanken werden nicht im Klartext gespeichert, sondern es werden geeignete kryptographische Verfahren eingesetzt
- Uhren, der verwendeten Informationsverarbeitungssysteme (PCs, Notebooks, etc.) sind mit geeigneten Zeitquellen synchronisiert, um eine gezielte Analyse bei Sicherheitsereignissen zu ermöglichen

3. Zugriffskontrolle

- Ausschließlicher Zugriff von Berechtigten, auf entsprechenden/unterliegenden Daten. Die Anlagen 1 und 2 der Mitarbeitervereinbarung regelt, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden
- Aktenschredder, Externer Aktenvernichter, Physische Löschung von Datenträgern vor der Entsorgung
- Regelungen zur Verwaltung der Rollen (Zuweisungen, Entzug) über Active Directory
- Keine administrative Kennung für Nutzer, die keine administrative Tätigkeit ausführen
- Nur kompetente und eingewiesene Personen dürfen Administrationstätigkeiten auf den Servern durchführen
- Dort wo möglich und notwendig, Einsatz von Verfahren zur Zwei-Faktoren-Authentifizierung bei Anwendung, die dies insbesondere für Administrationen unterstützen;
- Vereinbarung einer Verschwiegenheitsverpflichtung im externen Dienstleistungsvertrag

4. Weitergabekontrolle

- Keine Weitergabe an Dritte außer den genannten Sub-Unternehmen
- Verschlüsselungskonzept für Dokumente die personenbezogene Daten beinhalten
- Fernwartung für Clients IT-Administrationszwecken ausschließlich über verschlüsselte Verbindungen nach Authentifizierung durch den Administrator und Freigabe durch den Nutzer
- Prozess zur wirksamen Datenlöschung vor Vergabe eines Endgeräts an einen anderen Mitarbeiter
- Ein Sicherheitskonzept für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten ist vorhanden (z.B. keine unerlaubte Einsicht in ausgedruckte Dokumente, ausreichender Schutz gespeicherter Informationen, ordnungsgemäße Entsorgung)
- Bei Einsatz von Fernwartungssoftware: Regelmäßiges Einspielen von Sicherheitsupdates und auf Informationen über bekannte Schwachstellen oder Fehlkonfiguration achten
- Protokollierung Fernwartung externer Dienstleister und den Zugang nur auf das zu wartende System begrenzen
- Archivierungskonzept
- Regelung zur Aufbewahrungspflicht der Daten
- Keine Archivierung auf Datenträgern, die für eine lange Speicherdauer ungeeignet sind

idem telematics GmbH · info@idemtelematics.com · www.idemtelematics.com

Geschäftsführer: Jens Zeller, Thomas Piller · Amtsgericht München · HRB 154698 · USt-Id: DE239143054 · Steuernr.: 143148/40454
Sitz der Gesellschaft München · Lazarettstraße 4 · D-80636 München · T +49 89 720 13 67-0 · F +49 89 720 13 67-29
Standort Ulm · Riedweg 5 · D-89081 Ulm · T +49 731 936 97-0 · F +49 731 936 97-79

5. Trennungskontrolle

- Trennung von Produktiv- und Testumgebung
- Logische Mandantentrennung (CargoFleet 3)
- Steuerung über Berechtigungskonzept
- Einsatz qualifizierte Datenträgerverwaltung
- Löschfrist

6. Auftragskontrolle

- Personenbezogene Daten werden nur entsprechend den Weisungen des Kunden verarbeitet
- Uhren, der verwendeten Informationsverarbeitungssysteme (PCs, Notebooks, etc.) sind mit geeigneten Zeitquellen synchronisiert, um eine gezielte Analyse bei Sicherheitsereignissen zu ermöglichen
- Systeme werden über geeignete Monitoring-Tools überwacht
- Monitoring-Prozesse werden laufend an das System angepasst
- Wartungsarbeiten werden dem Kunden vorher angekündigt

7. Verfügbarkeitskontrolle

- Bei Störungen wird Betrieb über 24/7 Support informiert
- 24/7 Support des Hosters bei Hardware-Ausfällen
- Notfallplan zur Business Continuity: Regelungen, welche Systeme in welcher Reihenfolge wieder instandgesetzt werden, welche (externen) Personen/Dienstleister im Notfall zu Rate gezogen werden können sowie Meldepflichten
- Regelmäßige Überprüfung des Notfallplanes
- Schriftlich fixiertes Backup-Konzept
- Durchführung von Backups
- Geeignete physische Aufbewahrung von Backupmedien (Tresor)
- Es besteht ein Brandschutzkonzept
    - Verwendung von Feuer-/Rauchmeldeanlagen (im Rahmen des Brandschutzkonzeptes)
    - Feuerhemmende Schränke/Tresore zur Lagerung essenzieller Komponenten
    - Regelmäßige Überprüfung, insbesondere Infrastruktur
    - Feuerlöscher
- Einsatz von Anlagen zur Sicherstellung der Stromversorgung von Serversystemen (unterbrechungsfreie Stromversorgung USV), insbesondere bei kurzfristigen Stromausfällen oder Schwankungen
- Einsatz von Backup- und Synchronisierungsmechanismen zur Verhinderung eines größeren Datenverlusts bei Verlust, Beschädigung oder Diebstahl
- Sicherheitsvorkehrungen durch Angriffe bei der Verwendung Website und Webanwendungen
    - Verwendung des HTTPS-Protokolls nach Stand der Technik (TLS1.2 oder TLS1.3) (Art. 25 Abs. 2 DSGVO)
    - Fernzugang zu Webservern nur mit verschlüsselten Verbindungen
    - Nur geschultes bzw. kompetente Personen dürfen Administrationstätigkeiten auf den Servern durchführen
    - Geregelter Prozess zur Information über Sicherheitsupdates und zeitnahes Einspielen derselben, insbesondere bei gängigen Content-Management-Systemen (CMS)
- Sicherheitsvorkehrungen durch Angriffe auf das Netzwerk
    - Einsatz einer Firewall am zentralen Internetübergang
    - Blockierung aller nicht benötigten Dienste

idem telematics GmbH · info@idemtelematics.com · www.idemtelematics.com

Geschäftsführer: Jens Zeller, Thomas Piller · Amtsgericht München · HRB 154698 · USt-Id: DE239143054 · Steuernr.: 143148/40454
Sitz der Gesellschaft München · Lazarettstraße 4 · D-80636 München · T +49 89 720 13 67-0 · F +49 89 720 13 67-29
Standort Ulm · Riedweg 5 · D-89081 Ulm · T +49 731 936 97-0 · F +49 731 936 97-79

- Einsatz eines Web-Proxies über den alle HTTP-Verbindungen gehen müssen (Art. 25 Abs. 2 DSGVO)
- Einsatz geeigneter Firewall-Architekturen zur Absicherung rein interner Systeme (z.B. Arbeitsplatz, Drucker) zu den über das Internet erreichbaren Servern (z.B. Mail-Server; Web-Server, VPN-Endpunkt)
- Nutzung des WLAN-Gastzugangs ohne Zugangsmöglichkeit zum internen Netzwerk
- Prüfung E-Mails mittels Anti-Malwareschutz
- Blockierung von gefährlichen E-Mail-Anhängen
- Anbindung von Niederlassungen oder Homeoffice über stark verschlüsselte VPN-Verbindungen mit Client-Zertifikatsauthentifizierung
- Einsatz von Anti-Viren-Software auf Clients

8. Privacy by Default and Privacy by Design

- Entwicklung und Auswahl von Software
  - Beschränkter Zugang zum Source-Code geregelt durch Atlassian-Software
  - Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen

9. Organisatorische Maßnahmen für alle Bereiche

- Verpflichtung zum Datengeheimnis der Beschäftigten
- Datenschutzschulung für Beschäftigte zeitnah nach Aufnahme der Beschäftigung
- Richtlinien z.B. zur E-Mail-/Internetnutzung, Umgang mit Schadensmeldungen
- Sensibilisierung der Beschäftigten, die mit Externen wie z.B. Lieferanten interagieren, in Bezug auf angemessene Einsatzregeln, Richtlinien, Prozesse und Verhalten (u.a. welche Daten dürfen in welche Form weitergegeben werden, was kann sicherheitskritisch sein)

10. Datenschutz- und Datensicherheitsmanagement

- Datenschutzkonzept mit entsprechenden Maßnahmen ist erstellt

Es liegen schriftlich vor

- Interne Verhaltensregeln: IT-Einwilligungserklärung
- Sondervereinbarung zum Arbeiten im Mobileoffice
- Risikoanalyse
- Umfassendes Datensicherheits- und Datenschutzkonzept
- Recoverykonzept
- Zertifikat: ISO 9001:2015
- Zertifizierungsstelle: EQZert
- Sonstiges: Maßnahmen Subunternehmer (InterNet X, Microsoft Deutschland GmbH, MECOMO Aktiengesellschaft)

idem telematics GmbH · info@idemtelematics.com · www.idemtelematics.com

Geschäftsführer: Jens Zeller, Thomas Piller · Amtsgericht München · HRB 154698 · USt-Id: DE239143054 · Steuernr.: 143148/40454
Sitz der Gesellschaft München · Lazarettstraße 4 · D-80636 München · T +49 89 720 13 67-0 · F +49 89 720 13 67-29
Standort Ulm · Riedweg 5 · D-89081 Ulm · T +49 731 936 97-0 · F +49 731 936 97-79