

Überblick zum Sicherheits- und Datenschutzkonzept der PTC Telematik GmbH

Die PTC Telematik GmbH verfügt über ein umfangreiches und modernes Konzept, um den Datenschutz und die Datensicherheit innerhalb des Unternehmens zu gewährleisten.

Das Datenschutz- und Sicherheitskonzept der PTC Telematik GmbH umfasst umfangreiche Regelungen, die beispielsweise den Datenschutz für die Mitarbeiter in der PTC Telematik GmbH gewährleisten, die Rechte der betroffenen Personen wahren und eine Zugriffskontrolle sowie eine Weitergabekontrolle bezüglich personenbezogener Daten beinhalten. Zum Sicherheits- und Datenschutzkonzept der PTC Telematik GmbH gehört außerdem eine umfangreiche Zutrittskontrolle zum Unternehmen.

Regelungen betreffend die Löschung, der Archivierung, der Einschränkung und der Entsorgung von Daten sind ebenso Bestandteil des Sicherheits- und Datenschutzkonzeptes der PTC Telematik GmbH wie ein effektives Notfallkonzept in Form eines Disaster Recovery Konzepts für den Fall einer Verletzung des Schutzes personenbezogener Daten.

Die PTC Telematik GmbH führt außerdem regelmäßige Backups durch und sorgt auch damit für größtmöglichen Schutz personenbezogener Daten im Unternehmen.

Datenschutzrelevante Richtlinien wie beispielsweise:

- die Unternehmensrichtlinie der PTC Telematik GmbH zum Datenschutz
- die Richtlinie zur Nutzung von Internet- und E-Mail-Zugang
- die Richtlinie der PTC Telematik R GmbH zum Heimarbeitsplatz
- die Passwortrichtlinie
- sowie die Richtlinie bring your own device BYOD

sorgen zusammen mit dem ausformulierten Datenschutzkonzept der PTC Telematik GmbH sowie zahlreichen Datenschutzvereinbarung mit den Mitarbeitern für ein größtmögliches Maß an Datensicherheit und Datenschutz im Unternehmen.

Einen kompletten Überblick über das Datenschutz- und Sicherheitskonzept der PTC Telematik GmbH mit Stand vom 30.12.2019 bietet die folgende Tabelle.

Wahrung der Rechte betroffener Personen

Die PTC Telematik GmbH hat ein Konzept zur Wahrung der Rechte betroffener Personen, mit dem die Rechte der betroffenen Personen bezüglich

- Auskunft
- Berichtigung
- Löschung
- Datentransfer
- Widerruf
- Widerspruch
- Beschwerderecht

innerhalb der gesetzlichen Fristen gewährleistet werden.

Datenschutz bezüglich der Mitarbeiter der PTC Telematik GmbH

Die PTC Telematik GmbH hält folgende Konzepte bezüglich des Datenschutzes auf Mitarbeiterebene vor:

- Regelung Heimarbeitsplatz
- Regelung Bring Your Own Device BYOD
- Vertrauens-/Verschwiegenheitsverpflichtungen
- Regelung zur Nutzung betrieblicher Internet- und E-Mail-Zugänge
- Regelung zur Nutzung von Social Media

Speicherkontrolle und Eingabekontrolle

Folgende Konzepte sind Bestandteil der Speicher- und Eingabekontrolle:

- Aufbewahrung von Formularen, aus denen Daten in automatisierte Verarbeitungen übernommen wurden
- Verwaltung der Rechte durch einen Systemadministrator
- Beschränkung der Anzahl der Systemadministratoren auf das „Notwendigste“
- Genaue Festlegung der Berechtigungen in den IT-Systemen
- Protokollierungen von Dateneingaben sowie Löschungen und Änderungen
- Rechtevergabe bezüglich der Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.

Konzept zur Archivierung, Löschung, Entsorgung und Einschränkung der Verarbeitung personen- bezogener Daten

Die PTC Telematik GmbH verfügt über ein Archivierungs-, Lösch- und Entsorgungskonzept, das feste und geregelte Zuständigkeiten enthält. Die Mitarbeiter der PTC Telematik GmbH wurden bezüglich der Löschfristen, der gesetzlichen Voraussetzungen und der Vorgaben für Geräteentsorgung sowie über Entsorgungsdienstleister informiert.

Kontrolle über die Weitergabe

- Wo immer möglich, findet eine Pseudonymisierung statt
- Empfänger von Daten sind festgelegt und werden dokumentiert
- Dedizierte Weitergabeberechtigungen

Kontrolle über Aufträge

- Schriftliche Festlegung aller Weisungen in Form von Auftragsverarbeitungsverträgen
- sorgfältige Auswahl von Auftragnehmern
- Kontrolle der Auftragnehmer bezüglich der Datensicherheit und des Datenschutzes
- Vernichtung der Daten nach Auftragende wird sichergestellt
- Systeme und Serverfunktionieren unabhängig voneinander

Einhaltung des Trennungsgebotes und Gewährleistung des Zweckbindungsgebotes

- Softwareseitig erfolgt eine logische Mandantentrennung
- Hardwareseitig erfolgt eine physische Mandantentrennung
- Bei der Pseudonymisierung von Daten werden die Zuordnungsdateien getrennt und auf einem getrennten, abgesicherten System aufbewahrt
- Produktivsystem und Testsystem werden getrennt

Zutrittskontrolle

Folgende Sicherheitskonzepte zur Zutrittskontrolle werden durchgeführt:

- Videoüberwachung
- Professionelle Alarmanlage
- Sicherheitseingangstür
- Sicherheitsschlösser mit Code-System
- Hilfskräfte und betriebsfremde Personen werden beaufsichtigt
- Für betriebsfremde Personen bestehen Zutrittsregelungen
- Minimierung des Einbruchsriskos durch Lage des Büros

Zugriffskontrollen und Zugangskontrollen

Durch folgende Maßnahmen werden Zugriffe und Zugänge kontrolliert:

- Nutzung aktueller Softwareversionen
- Nutzung aktueller Virenschutzprogramme
- Nutzung von Firewalls für Hardware und Software
- Mindestpasswortlängen und Passwortmanager gemäß der Passwortrichtlinie
- Einsatz von Intrusion-Prevention-Systemen (IPS)
- Datenzugriffe werden protokolliert
- Einsatz von automatisch passwortgeschützten Sperrbildschirmen

Integrität und Verfügbarkeitskontrolle

- Für private mobile Devices und Gäste wird Gäste-WLAN bereitgestellt
- Mobilen Datenträger und Geräte werden verschlüsselt
- Datenträger werden ordnungsgemäß nach DIN 32757 vernichtet
- Umsetzung von Berechtigungs- und Authentifizierungskonzepten mit Zugriffsregulierungen, die auf das Nötigste beschränkt werden
- Abschließbarer Serverschrank
- Server im gesicherten Rechenzentrum
- Für Personalsachen und Verträge stehen abschließbare Aktenschränke zur Verfügung
- Daten auf Papier werden mit einem Sicherheitsstufe P-5 Aktenvernichter inhouse vernichtet
- Reinigungspersonal wird sorgfältig ausgewählt

- Die PTC Telematik GmbH hat ein ständig kontrolliertes Backup- und Recoverykonzept.
- Es existiert ein Notfallkonzept
- Sicherungskopien werden an besonders geschützten Orten gelagert
- Es werden Belastbarkeitstests bzw. Tests der Auslastung durchgeführt
- Im Unternehmen stehen Feuerlöschgeräte zur Verfügung

Notfallkonzept/Desaster Recovery Konzept

Es besteht ein Notfallkonzept, mit dem unverzüglich und den gesetzlichen Anforderungen entsprechend auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) reagiert werden kann.