Anlage zum Vertrag zur Auftragsverarbeitung
Technische und organisatorische Maßnahmen (TOM)
der P&S GmbH & Co. KG

Stand: 8.03.2022

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1 Zugangskontrolle

- Besucher Begleitung durch P&S-Personal.
- Haupteingangstür mit Knauf auf der Außenseite
- Eingangsbereiche und Fenster sind außerhalb der Geschäftszeiten verschlossen.
- Elektronisches Zutrittssystem mit automatischem Verschließen an der Büro Eingangstür.
- Außerhalb der Bürozeiten ist der Eingangsbereich der Geschäftsräume videoüberwacht.
- Außerhalb der Bürozeiten sind die Gebäudeeingangstüren verschlossen.
- Bei Reinigungsdiensten setzen wir auf Kontinuität und langfristige Partnerschaft

2 Zugriffskontrolle

- Rechner- Login mit Benutzername und Passwort mit Protokoll
- Verwendung von Anti-Virus Software auf Servern und Clients
- Computersysteme werden ständig auf dem aktuellen Stand gehalten
- Verwendung von Firewall und Intrusion Detection System als Schutz für das P&S Netzwerk
- Einsatz von VPN bei Zugriffen von außen auf das P&S Netzwerk
- . Aktenvernichtung über zertifizierten Dienstleister

3 Organisatorische Maßnahmen:

- Nutzerrechte und Zugänge werden durch Administratoren verwaltet
- Berechtigung auf Netzwerkverzeichnisse nutzerbezogen rollenbasierend.
- Zertifizierter zentraler Passwortmanager zum Speichern der System- und Kundenpasswörter
- Einsatz von Passwortregelungen nach aktuell empfohlenem Standard.
- Zugänge werden nach einer entsprechenden Anzahl von Fehlversuchen gesperrt.
- Protokollierung von Zugriffen auf Anwendungen bei der Eingabe, Änderung und Löschung von Daten.
- Mindestens jährlich Schulungen und Unterweisungen zum Datenschutz und zur Datensicherheit.

4 Trennungskontrolle

- Trennung von Produktiv- und Testumgebung.
- Physikalische Trennung von System und Datenbank
- Für unterschiedliche Anwendungen werden getrennte Verzeichnisse/Datenbanken mit verschiedenen Rechten eingesetzt.

5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Die Übertragung zwischen den Systemkomponenten der P&S-Produkte erfolgt

  a Pseudonymisiert

b Verschlüsselt in der P&S-Cloud

c Bei Installation auf einem Kundensystem, obliegt die Verschlüsselung der Übertragung dem Auftraggeber

- Die verwendete Datenbank ist generell verschlüsselt.

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

1 Weitergabekontrolle

- Einsatz von VPN zur Online-Datenübertragung
- Daten, die über Datenträger weitergegeben werden, werden komprimiert und verschlüsselt gespeichert
- Nutzung von 2FA (Zwei-Faktor-Authentisierung) bei allen Subunternehmern, sofern die Möglichkeit dazu besteht.
- Daten, die aufgrund von gesetzlichen Vorgaben an die entsprechenden Stellen zu übertragen sind, wie zum Beispiel Steuer- und Sozialversicherungsdaten werden auf den durch den Gesetzgeber vorgeschrieben Wegen und mit den dort vorgegeben Verschlüsselungen übertragen.
- Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind schriftlich zur Verschwiegenheit verpflichtet.

2 Eingabekontrolle

- In dem von der P&S eingesetzten Programme ist implementiert, dass jederzeit, insbesondere auch nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in dem System eingegeben, verändert oder gelöscht wurden.
- Es gibt neben Berechtigungseinstellungen auch zusätzliche Sperrmechanismen, die eine Veränderung oder Löschung verhindern können.

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1 Für Kunden der P&S-Cloud wird durch das Rechenzentrum gewährleistet:

- Die Sicherheit der Daten und deren Verfügbarkeit wird durch ein mehrstufiges Backup- und Recovery-Konzept gewährleistet, sowie die redundante Auslegung zentraler Systeme und ihrer Komponenten.
- Systeme und Datenbanken werden online gesichert, um eine größtmögliche Verfügbarkeit im Rahmen der vereinbarten Leistungserbringung zu gewährleisten.
- Im gesamten Gebäude existiert eine Brandmeldeanlage. Der Serverraum ist durch eine automatische Feuerlöschanlage gesichert.
- Im gesamten Gebäude besteht Rauchverbot.
- Das gesamte Gebäude ist durch eine Alarmanlage mit automatischer Benachrichtigung des Sicherheitsunternehmens geschützt.
- Es erfolgen regelmäßige Datensicherungen sowie permanente Datenspiegelung.
- Der Zugang zu den Servern ist durch mehrstufige Sicherheitskomponenten abgesichert.
- Die Zugriffe auf die zentrale Anwendung im Rechenzentrumsbetrieb erfolgen über redundante Leitungen.

2 Für die Installation auf dem Kundensystem, obliegen die Maßnahmen für die Verfügbarkeit dem Auftraggeber.

4 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

1 Für Kunden der P&S-Cloud wird durch das Rechenzentrum gewährleistet:

- Systeme und Datenbanken werden gesichert, um eine größtmögliche Verfügbarkeit zu gewährleisten.
- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

2 Für die Installation auf dem Kundensystem:

- Die Datenbank wird für den Fall einer nötigen Wiederherstellung täglich in einen Ordner gesichert.
- Für die weitere Sicherung und Wiederherstellung der Kundensysteme, ist der Auftraggeber verantwortlich.

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

1 Quartalsweise Überprüfung durch das Datenschutzteam:

- Dokumentation der Verfahrensweisen und Regelungen auf notwendige Änderungen
- Wirksamkeit der Verfahrensweisen und Regelungen
- Aktuell zusätzlicher Schulungsbedarf der Mitarbeiter

2 Automatische Überprüfung der Systeme über Monitoring-Tools für:

- Auffälligkeiten im Netzwerk
- Auffälligkeiten auf den Serversystemen