Technisch-Organisatorische Maßnahmen

Technische und organisatorische Maßnahmen der p.AI GmbH

p.AI GmbH
Pappelallee 78/79
10437 Berlin
Deutschland

Inhaltsverzeichnis

1. Einleitung und Rahmenbedingungen	3
1.1 Einleitung	3
1.2 Unternehmen / Behörde	3
1.3 Mit dem Datenschutz beauftragte Person des Unternehmens / der Behörde	3
2. Technisch-Organisatorische Maßnahmen	4
2.1 Gewährleistung der Vertraulichkeit	4
2.1.1 Zutrittskontrolle	4
2.1.2 Zugangskontrolle	4
2.1.3 Zugriffskontrolle	5
2.1.4 Trennungskontrolle	5
2.2 Gewährleistung der Integrität	6
2.2.1 Weitergabekontrolle	6
2.2.2 Eingabekontrolle	6
2.3 Pseudonymisierung und Verschlüsselung	7
2.3.1 Pseudonymisierung	7
2.3.2 Verschlüsselung	7
2.4 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit	8
2.4.1 Verfügbarkeit (der Daten)	8
2.4.2 Belastbarkeit (der Systeme)	8
2.4.3 Wiederherstellbarkeit (der Daten / der Systeme)	9
2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	10
2.5.1 Auftragskontrolle	10
2.5.2 Datenschutz-Management	10
2.5.3 Incident-Response-Management	11
2.5.4 Datenschutzfreundliche Voreinstellungen	11

1. Einleitung und Rahmenbedingungen

1.1 Einleitung

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1.2 Unternehmen / Behörde

Die folgenden Festlegungen repräsentieren das Datenschutzkonzept der

p.AI GmbH
Pappelallee 78/79
10437 Berlin
Deutschland

1.3 Mit dem Datenschutz beauftragte Person des Unternehmens / der Behörde

Mit dem Datenschutz beauftragte Person des Unternehmens / der Behörde
Datenschutzberatung Mundanjohl
Andreas Mundanjohl
Zeller Strasse 30
73101 Aichelberg
Deutschland
Telefon: 082190782120
E-Mail: datenschutz@mundanjohl.de

2. Technisch-Organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen Folgendes ein:

2.1 Gewährleistung der Vertraulichkeit

2.1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

- 2FA-Login zu allen Projekten
- Schlüsselregelung mit einer Liste
- Sorgfalt bei der Auswahl des Reinigungspersonals
- Besucher nur in Begleitung durch Mitarbeiter

2.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Maßnahmen:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Anti-Viren-Software
- Einsatz einer Software-Firewall

- Verwaltung der Rechte durch einen Systemadministrator
- Login mit Benutzername und Passwort
- Verwalten von Benutzerberechtigungen
- Authentifikation mit SSH Keys

2.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen:

- Einsatz der minimalen Anzahl an Administratoren
- Verwaltung der Benutzerrechte durch Administratoren
- Sichere Aufbewahrung von Datenträgern und Unterlagen
- Einsatz von Aktenvernichtern bzw. Diensleistern

2.1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Maßnahmen:

- Trennung von Produktiv- und Testumgebung
- Steuerung über ein Berechtigungskonzept
- Festlegung von Datenbankrechten

2.2 Gewährleistung der Integrität

2.2.1 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen:

- Funktionelle Verantwortlichkeiten
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Protokollierung der Zugriffe und Abrufe

2.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- Verwendung von Zugriffsrechten
- Nachvollziehbarkeit der Bearbeitung von Daten durch individuelle Benutzernamen
- Technische Protokollierung der Änderung von Daten
- Technische Protokollierung der Löschung von Daten
- Klare Zuständigkeiten für die Löschung von Daten

2.3 Pseudonymisierung und Verschlüsselung

2.3.1 Pseudonymisierung

Maßnahmen, die eine Pseudonymisierung von Daten gewährleisten.

Maßnahmen:

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe zu pseudonymisieren
- Interne Anweisung, personenbezogene Daten nach Ablauf der Löschfrist zu pseudonymisieren

2.3.2 Verschlüsselung

Maßnahmen, die eine Verschlüsselung von Daten gewährleisten.

Maßnahmen:

- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Verschlüsselung von Systemen

2.4 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

2.4.1 Verfügbarkeit (der Daten)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Verfügbarkeit von Daten.

Maßnahmen:

- Tägliche Backups
- Betrieb von Hochverfügbarkeits-Webservern
- SLA mit Hosting Dienstleister
- Wöchentliche Backups
- Backup & Recovery-Konzept
- RAID System / Festplattenspiegelung
- Datensicherungskonzept vorhanden
- Unterbrechungsfreie Stromversorgung (USV)
- Monatliche Backups

2.4.2 Belastbarkeit (der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme.

Maßnahmen:

- Einspielen von aktuellen Sicherheitsupdates auf allen Applikationsservern
- Einsatz von Software Firewalls

2.4.3 Wiederherstellbarkeit (der Daten / der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen.

Maßnahmen:

- Restore von Datenbanken und Dateisystemen aus dem Backup der Webserver
- Serverraum ist getrennt von Arbeitsplätzen

2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

2.5.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen / Dokumentation
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Abschluss der notwendigen Auftragsdatenvereinbarungen
- Abschluss der notwendigen Standard-Vertragsklauseln
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Regelung zum Einsatz von Subunternehmern
- Überprüfung des Schutzniveaus des Auftragnehmers (initial)
- Überprüfung des Schutzniveaus des Auftragnehmers (kontinuierlich)
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer

2.5.2 Datenschutz-Management

Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren.

Maßnahmen:

- Einsatz von Softwarelösungen für Datenschutz-Management
- Implementierung von Verbesserungsvorschlägen
- Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- Zugriffsmöglichkeiten für Mitarbeiter zu den Regelungen zum Datenschutz (Wiki / Intranet)
- Überprüfung der Wirksamkeit der TOMs (mind. jährlich durchgeführt)

- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz
- Einhaltung der Informationspflichten gemäß Art. 13 DSGVO
- Einhaltung der Informationspflichten gemäß Art. 14 DSGVO

2.5.3 Incident-Response-Management

Maßnahmen, die gewährleisten, dass Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systeme geschützt werden können und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann.

Maßnahmen:

- Einsatz von Firewall und deren regelmäßige Aktualisierung
- Einsatz von Spamfilter und deren regelmäßige Aktualisierung
- Einsatz eines Intrusion Prevention Systems (IDS)
- Einsatz von Virenscanner und deren regelmäßige Aktualisierung

2.5.4 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass bereits durch die entsprechende Technikgestaltung (privacy by design) und Werkseinstellungen (privacy by default) einer Software vorab ein gewisses Datenschutzniveau herrscht.

Maßnahmen:

- Personenbezogene Daten werden nur zweckerforderlich erhoben
- Gewährleistung einer einfachen Ausübung des Widerrufsrechts eines Betroffenen