Anlage 1

Technisch-organisatorische Maßnahmen der

Tech-Prax GmbH

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Das Ziel einer Zutrittskontrolle ist es, Unbefugten den Zutritt (z.B. zu den Räumen der Datenverarbeitung, den Büroräumen oder den Serverräumen) zu verwehren. Der Begriff des Zutritts ist dabei räumlich zu verstehen.
Sollten Mitarbeiter der Tech-Prax GmbH in der mobilen Arbeit tätig sein, sind hierzu gesondert Vereinbarungen mit dem Mitarbeiter abgeschlossen worden.

Der Zutritt wird einheitlich mit folgenden Maßnahmen sichergestellt:

- ☑ Geschäftsräume sind durch zwei Türen gesichert
- ☑ Manuelles Schließsystem
- ☑ Schlüsselregelung / Liste
- ☑ Besucher nur in Begleitung durch Mitarbeiter
- ☑ Sorgfalt bei Auswahl der Reinigungsdienste
- ☑ Geschäftsräume werden nur zu Geschäftszeiten betreten
- ☑ Besucher Listen mit Unterschrift
- ☑ Türen mit Knauf auf Außenseite
- ☑ Klingelanlage mit Kamera
- ☑ Chipkarten / Transpondersysteme
- ☑ Zum Dienstende werden die Büroräume gemäß Clean Desk Prinzip verlassen

Zugangskontrolle

Durch die Zugangskontrolle soll ein unbefugter Zugriff auf die Datenverarbeitungsanlagen und Datenverarbeitungssysteme, die personenbezogene Daten verarbeiten, verhindert werden.

Folgende Maßnahmen werden angewendet:

- ☑ Login mit Benutzername und Passwort
- ☑ Anti-Viren-Software Server
- ☑ Anti-Viren-Software Clients
- ☑ Richtlinie „Sicheres Passwort“
- ☑ Richtlinie „Löschen / Vernichten“
- ☑ zwei unabhängige Firewalls
- ☑ Server sind nur per VPN-Verbindung von außen erreichbar, nur von autorisierten Mitarbeitern
- ☑ Allgemeine Richtlinie Datenschutz und / oder Datensicherheit
- ☑ Verschlüsselung von Festplatten (Server und Clients)

- ☑ Wartungs- und Reparaturarbeiten werden nur durch ausgewählte Fachfirmen durchgeführt
- ☑ Verfahrensanweisungen zur manuellen Desktopsperre, sicheres Passwort, Löschen und Vernichten von Daten, Clean Desk Prinzip im Einsatz und allgemeine Informationen zum Datenschutz und Datensicherheit

Zugriffskontrolle

Das Ziel der Zugriffskontrolle ist es zu gewährleisten, dass ausschließlich die zur Benutzung der Datenverarbeitungssystem Berechtigten auf die ihnen zugriffsberechtigten personenbezogenen Daten zugreifen können. Ebenso dürfen personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden.

Um unerlaubt Tätigkeiten innerhalb der Systeme der Tech-Prax GmbH außerhalb der eingeräumten Berechtigungen zu verhindert, werden folgende Maßnahmen angewendet:

- ☑ Rechte- und Rollenkonzept
- ☑ Zentrale Aktenvernichtung (DIN 32757)
- ☑ Protokollierung der Datenlöschung
- ☑ Protokollierung von Zugriffen auf Anwendungen (insbesondere bei der Eingabe, Änderung und Löschung von Daten)
- ☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☑ Arbeiten erfolgen nur im Rahmen des Auftrags sowie weitergehende Arbeiten nur in Abstimmung mit dem Auftraggeber erfolgen
- ☑ Reduzierung auf eine notwendige Mindestanzahl an Administratoren
- ☑ Sperrung von Zugängen von ausscheidenden Mitarbeitern

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Mit der Weitergabekontrolle soll gewährleistet werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, vervielfältigt oder entfernt werden können. Es muss ebenso überprüft werden, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Eine Weitergabe an Dritte Einrichtungen findet nicht statt, sodass hierzu keine Maßnahmen erforderlich sind. Die Übertragung der pb-Daten zum und vom Kunden findet per verschlüsselter Verbindung statt.

Eingabekontrolle

Die Eingabekontrolle verfolgt das Ziel, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in welche Systeme und Anlage zur Datenverarbeitung eingegeben, verändert oder entfernt worden sind.

Die Nachvollziehbarkeit innerhalb der Datenverwaltung stellt die Tech-Prax GmbH wie folgt sicher:

- ☑ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☑ Die Speicherdauer der Protokolldaten orientiert sich an die allgemeine Frist zur Speicherung von den verarbeiteten Daten
- ☑ Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt auf Basis des implementierten Berechtigungskonzeptes
- ☑ Die Eingabe, Änderung und Löschung finden nur in einem Programm statt, dem Kundensupport-Programm

Auftragskontrolle

Das Ziel der Auftragskontrolle gemäß von Art. 28 DSGVO ist es zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend des Auftrags und den Weisungen des Auftraggebers verarbeitet werden könne.

Folgende Maßnahmen ergreift die Tech-Prax GmbH, um der Auftragskontrolle gerecht zu werden:

- ☑ Vertragliche Regelung gemäß Art. 28 DSGVO (Auftragsverarbeitung)
- ☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☑ Unterauftragnehmer werden sorgfältig geprüft nach den Vorgaben der DSGVO eingesetzt
- ☑ Vereinbarung wirksamer Kontrollrechte
- ☑ Sicherstellung und Vernichtung von Daten nach Beendigung des Auftrags

Verfügbarkeitskontrolle

Das Ziel in der Verfügbarkeitskontrolle liegt im Schutz gegen Zerstörung und Verlust von personenbezogenen Daten.

Folgenden Maßnahmen ergreift die Tech-Prax GmbH:

- ☑ Backup und Recovery Konzept
- ☑ Server Datensicherungen werden extern aufbewahrt
- ☑ RAID-System
- ☑ Existenz eines Notfallkonzepts
- ☑ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- ☑ Virenschutz Clients und Server, darüber hinaus weitere Add-Ons und Schutz durch Firewall
- ☑ Getrennte Partitionen für Betriebssysteme und Daten
- ☑ Feuerlöschgerät vor dem Serverraum
- ☑ Feuer- und Rauchmeldeanlage
- ☑ Serverraumüberwachung der Temperatur und Feuchtigkeit
- ☑ Serverraumklimatisierung
- ☑ Unterbrechungsfreie Stromversorgung (USV)
- ☑ Kein unbefugter Zutritt

Trennungskontrolle

Mit dem Trennungsgebot soll gewährleistet werden, dass die zu unterschiedlichen Zwecken erhobenen Daten ebenfalls getrennt voneinander verarbeitet werden.

Um sicherzustellen, dass die zu unterschiedlichen Zwecken erhobenen Daten getrennt voneinander verarbeitet werden, hat die Tech-Prax GmbH folgende Maßnahmen getroffen:

- ☑ Die Daten des Auftraggebers sind physikalisch und logisch von anderen Daten getrennt
- ☑ Steuerung über das Berechtigungskonzept
- ☑ Datentrennung durch separate Benutzerkonten
- ☑ Funktionstrennung durch mandantenfähige Systeme

Pseudonymisierung (Art. 32 Abs. 1. lit. a DSGVO; Art. 25. Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt, wenn möglich, in einer Art und Weise, dass ohne Hinzuziehen zusätzlicher Informationen diese Daten nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Allgemeine Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

- ☑ Die datenschutzrechtliche Dokumentation aller Prozesse und Verfahren ist zentral dokumentiert
    - Mitarbeiter haben im Intranet Zugriff auf notwendige Unterlagen
- ☑ Neue Verarbeitungsverfahren werden frühzeitig vom DSB überprüft. Alle Prozesse unterlaufen einer Vorabkontrolle. Somit sind die Grundsätze privacy by design und privacy by default gewährleistet
- ☑ Eine Überprüfung der Wirksamkeit aller technischer Schutzmaßnahmen wird einmal im Jahr durchgeführt
- ☑ Die Mitarbeiter sind mit einer digitalen Datenschutzschulung auf die Vertraulichkeit und dem Datengeheimnis geschult und verpflichtet
- ☑ Regelmäßige Sensibilisierungen der Mitarbeiter findet mindestens einmal im Jahr statt
- ☑ Es existiert eine definierte Vertretungsregelung innerhalb der Funktionsgruppen
- ☑ Datenschutzfolgenabschätzungen finden je nach Bedarf statt
- ☑ Die Tech-Prax GmbH kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- ☑ Den Auskunftsanfragen seitens der Betroffenen werden anhand eines Prozesse Folge geleistet
- ☑ Datenschutzverletzungen werden binnen 72 Stunden an die Aufsichtsbehörde gemeldet
    - Formaler Prozess und Verantwortlichkeiten sind definiert
    - Nachbearbeitung von Sicherheitsvorfällen und Datenpannen ist gewährleistet
- ☑ Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich
- ☑ Das Widerrufsrecht von Patienten oder Betroffenen wird anhand eines etalierten Prozesses gewährleistet

- ☑ Es existiert ein Prüfschema für die Auswahl von Auftragsverarbeitern
    - TOMs werden anhand MUSS- und KANN-Kriterien geprüft

Weitere Maßnahmen

Sämtliche Beschäftigten der Tech-Prax GmbH sind in Schriftform zur Wahrung der Vertraulichkeit verpflichtet. Die Beschäftigten werden durch den Datenschutzbeauftragten regelmäßig im Umgang mit personenbezogenen Daten geschult.

Die Mitarbeiter sind informiert, dass bei z.B. Verlust des Notebooks oder sonstigen personenbezogenen Daten, der Datenschutzbeauftragte unverzüglich informiert werden muss. Dieser ergreift daraufhin die entsprechenden Maßnahmen. Für diesen Fall greift der Notfallplan und die entsprechenden Maßnahmen werden eingeleitet.

Anfragen von Betroffenen können durch das Datenschutz-Management fristgemäß bearbeitet werden. Im Verzeichnis von Verarbeitungstätigkeiten sind alle Verarbeitungsprozesse dokumentiert.

Schlussbestimmung

Der Datenschutz unterliegt bei der Tech-Prax GmbH einem kontinuierlichen Verbesserungsprozess und wird an die jeweiligen aktuellen und gültigen Datenschutzbestimmungen angepasst. Ebenso findet eine enge Zusammenarbeit zwischen dem Bereich Datenschutz und der IT-Sicherheit statt. Eine Aktualisierung des Dokuments findet fortlaufend statt.