Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG

der

PHCOM GmbH
Badstr. 38
70372 Stuttgart

---

1. Zutrittskontrolle

siehe TOM von Hetzner bei dem die Hardware gehostet ist.

2. Zugangskontrolle

siehe TOM von Hetzner bei dem die Hardware gehostet ist.

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.

X	Erstellen eines Berechtigungskonzepts	X	Verwaltung der Rechte durch Systemadministrator
X	Anzahl der Administratoren auf das „Notwendigste“ reduziert	X	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
X	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	X	Sichere Aufbewahrung von Datenträgern
X	physische Löschung von Datenträgern vor Wiederverwendung	X	ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
X	Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)	X	Protokollierung der Vernichtung
X	Verschlüsselung von Datenträgern		

4. 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.

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- X E-Mail-Verschlüsselung
- X Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- X Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- X Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- X Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- X Beim physischen Transport: sichere Transportbehälter/-verpackungen

5. 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.

X Protokollierung der Eingabe, Änderung und Löschung von Daten

X Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

X Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

X Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

X Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

6. Auftragskontrolle

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

X Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

X schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG

☐ Auftragnehmer hat Datenschutzbeauftragten bestellt

X Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

X Vertragsstrafen bei Verstößen

X vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

X Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)

X Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

X laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. Verfügbarkeitskontrolle

Siehe Tom von Hetzner

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

X	physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	X	Logische Mandantentrennung (softwareseitig)
X	Erstellung eines Berechtigungskonzepts	☐	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
X	Versehen der Datensätze mit Zweckattributen/Datenfeldern	☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
X	Festlegung von Datenbankrechten	X	Trennung von Produktiv- und Testsystem

26.05.2020
Datum

Philipp Stäbler
Verantwortlicher für die Erstellung (in Druckbuchstaben)

Unterschrift des Verantwortlichen