# Technisch- organisatorische Maßnahmen i.S.d. ART. 32 DSGVO

| | |
|---|---|
| **Unternehmen:** | **Arbeitsmedizin Dr. Lisa Schenk**<br>Joachim-Friedrich-Straße 16<br>10711 Berlin<br><br>Tel.: +49 30 9395 0030<br>Fax: +49 30 9395 0031 |
| **Verantwortlich nach DSGVO:** | **Dr. Lisa Schenk**<br>lisa.schenk@arbeitsmedizin-schenk.de |
| **Datenschutzbeauftragter:** | **Sven Stude**<br>datenschutz@arbeitsmedizin-schenk.de |

## 1. Vertraulichkeit

### 1.1. Zutrittskontrolle

Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten und Daten von juristischen Personen verarbeitet werden, zu verwehren.

Die in unserem Hause umgesetzten Maßnahmen:

- Besucher melden sich am Empfang und werden durch Mitarbeiter begleitet.
- Die Datenverarbeitungsanlagen befinden sich in einem separaten, durch ein Sicherheitsschloss gesicherten Raum.
- Der Zutritt zu den Datenverarbeitungsanlagen ist unbefugten vollständig verwehrt.

### 1.2. Zugangskontrolle

Es ist zu verhindern, dass die Datenverarbeitungssysteme durch Unbefugte genutzt werden können.

Die in unserem Hause umgesetzten Maßnahmen:

- Zugang zu den Datenverarbeitungsanlagen erhält ausschließlich autorisiertes und fachlich qualifiziertes Personal.
- Der Zugang erfolgt über eine Benutzerkennung und die Eingabe eines Passwortes.
- Die Passwörter entsprechen einem technisch sicheren Niveau und sind durch interne Richtlinien geregelt.
- Die Anmeldungen werden protokolliert.
- Die Festplatten aller mobilen Clients sind verschlüsselt.

### 1.3. Zugriffskontrolle

Es ist sicherzustellen, 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 oder verändert werden können.

Die in unserem Hause umgesetzten Maßnahmen:

- Der Zugriff auf die Datenverarbeitungssysteme ist durch eine Nutzer- und Rechteverwaltung abgesichert. Es ist dem einzelnen Mitarbeiter nur möglich die für seine Aufgaben erforderlichen Daten einzusehen, zu nutzen, zu verarbeiten oder zu löschen.

- Die Zugriffe auf die Datenverarbeitungssysteme werden protokolliert.
- Die Mitarbeiter sind verpflichtet, ihren Computer bei Verlassen des Arbeitsplatzes zu sperren.
- Jeder Mitarbeiter wird zur Vertraulichkeit und der Einhaltung des Datenschutzes bei Aufnahme seiner Tätigkeit verpflichtet. Ein Verstoß hätte disziplinarische Maßnahmen (Abmahnung, Kündigung) und ggf. eine Strafanzeige zur Folge. Betroffene Auftraggeber und zuständige Aufsichtsbehörden werden über einen solchen Vorfall informiert.

## 1.4. Weitergabekontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können, und dass überprüft werden kann, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist.

Die in unserem Hause umgesetzten Maßnahmen:

- Personenbezogene Daten werden ausschließlich über verschlüsselte Datenverbindungen, die dem Stand der Technik entsprechen, übertragen.
- Alle zum Transport personenbezogener Daten eingesetzten Datenträger werden erfasst und sind verschlüsselt. Der Einsatz privater oder nicht verschlüsselter Datenträger ist untersagt.
- Nicht mehr benötigte oder defekte Datenträger werden durch ein zertifiziertes Unternehmen vernichtet.
- Sollte die Weitergabe von personenbezogenen Daten an Dritte notwendig werden (z.B. Labor) erfolgt dies ausschließlich nach Genehmigung durch die betroffene Person.

## 1.5. Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Die in unserem Hause umgesetzten Maßnahmen:

- Die Daten der einzelnen Auftraggeber und Probanden werden logisch voneinander getrennt gespeichert (Mandantenfähige Software).

## 1.6. Pseudonymisierung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer betroffenen Person zugeordnet werden können, sofern diese zusätzliche Information gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

- Die Pseudonymisierung personenbezogener Daten obliegt dem Auftraggeber.

## 1.7. Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

- Der Fernzugriffe (Homeoffice) auf unsere Systeme ist nur mit openVPN möglich.
- Die Zugriffe auf das Verwaltungsprogramm werden mit TLS verschlüsselt.

- Mobile Clients und die Server sind mit Bitlocker verschlüsselt.
- Die Backup-Dateien und mobile Datenträger werden mit AES-265 verschlüsselt.
- Bei der Übertragung personenbezogener Daten per Email (angehängte Dateien) kommt ebenfalls eine AES-256 Verschlüsselung zum Einsatz.

# 2. Integrität

## 2.1. Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht worden sind.

Die in unserem Hause umgesetzten Maßnahmen:

- Die von uns eingesetzte Verwaltungssoftware protokolliert alle Zugriffe auf Mandanten (Auftraggeber) und Probanden.
- Unsere Server-Logs sind so eingestellt, dass Zugriffe protokolliert werden.

## 2.2. Weitergabekontrolle

Die unter Punkt 1.4 beschriebenen Maßnahmen dienen auch der Sicherstellung der Integrität.

# 3. Verfügbarkeit und Belastbarkeit

## 3.1. Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die in unserem Hause umgesetzten Maßnahmen:

- Soweit es technisch möglich ist, sind unsere Datenverarbeitungssysteme gegen zufällige Zerstörung durch folgende technische Maßnahmen geschützt:
    - RAID-Systeme,
    - USV-Anlagen mit Überspannungsschutz
    - Virenscanner (Clients, Server, Emailsystem)
    - IP-Tables Firewall
    - GFS-Backupsystem für Daten (60 Tage)
    - Bare-Metal-Backup für Serversysteme
- Unsere Datenverarbeitungs- und Schutzsysteme werden regelmäßig auf den neuesten Stand gebracht, Sicherheitsupdates werden zeitnah installiert.

## 3.2. Schnelle Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall schnell wiederherzustellen.

Die in unserem Hause umgesetzten Maßnahmen:

- IT- Notfall- und Wiederherstellungspläne sind vorhanden.
- Wir führen regelmäßige Wiederherstellungstests der Backups durch und dokumentieren diese.

# 4. Regelmäßige Überprüfung, Bewertung und Evaluierung

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

ist

## 4.1. Datenschutzmanagement

Die in unserem Hause umgesetzten Maßnahmen:

- Wir haben einen Datenschutzbeauftragten bestellt (Kontaktdaten siehe Seite 1).
- Es finden zudem regelmäßige Auditierung durch einen externen Datenschutzberater statt.
- Die Mitarbeiter werden bei Ihrer Einstellung und wiederkehrend - mindestens einmal pro Jahr - zu den Themen Informationssicherheit und Datenschutz geschult.
- Es ist eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter (Intranet) vorhanden.
- Wir kommen den Informationspflichten nach Art. 13 und 14 DSGVO nach.
- Es existiert ein Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener.

## 4.2. Incident-Response-Management

Die in unserem Hause umgesetzten Maßnahmen:

- Wir haben Prozesse zur Erkennung und Meldung von Data-Breaches eingeführt und diese dokumentiert.
- Alle Data-Breaches und die damit verbundenen Maßnahmen werden durch den Datenschutzbeauftragten dokumentiert und ggf. durch einen externen Datenschutzberater überprüft.

## 4.3. Datenschutzfreundliche Voreinstellung

Privacy by Design / privacy by Default

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- Wir haben Prozesse implementiert, die den Betroffenen eine einfache Ausübung Ihres Widerrufsrechtes ermöglichen.

## 4.4. Auftragskontrolle (Outsourcing)

Es sind Maßnahmen zu treffen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Die in unserem Hause umgesetzten Maßnahmen:

- Wir kontrollieren vorab, ob ein Auftragnehmer die notwendigen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen und dokumentiert hat. Bei längerer Zusammenarbeit werden die Kontrollen in regelmäßigen Abständen wiederholt.
- Mit jedem Auftragsverarbeiter werden die notwendigen Verträge (AVV / Standardvertragsklauseln) abgeschlossen.