# Anlage 1: Technisch-organisatorische Maßnahmen

Inklusion Digital setzt die folgenden Auftragsverarbeiter ein:

| Unterauftragnehmer | Anschrift/Land | Leistung |
|---|---|---|
| Planetary Networks GmbH | Naumannstraße 64, 10829 Berlin | Rechenzentrumsbetrieb, inkl. Hosting, Infrastruktur und (Cloud-) Speicherleistungen |
| Planetary Quantum GmbH | Naumannstraße 64, 10829 Berlin | Monitoring und Infrastrukturüberwachungsdiensleistungen |
| Hetzner Online GmbH | Industriestraße 25, 91710 Gunzenhausen | Sicherheitsbackups, ausschließlich auf Servern in der EU und des EWR. |

## 1.1 Allgemeine Maßnahmen

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| | • Es wurde ein Datenschutzbeauftragter benannt und dieser verfügt über angemessene Ressourcen zur Wahrnehmung seiner Aufgabe<br>• Der Schutzbedarf der Daten wurde festgelegt und die Daten entsprechenden Schutzklassen zugeordnet<br>• Es wurden Zugriffsrechte an die Mitarbeiter:innen vergeben, und einer Tabelle zugeordnet. Verpflichtungen auf Datengeheimnis |

- Schulungsmaßnahme

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Ermittlung, Benachrichtigung und Erfassung der Teilnahme von Datenschutz-Schulungen wird technisch gewährleistet | • Jede:r Mitarbeiter:in erhält jährlich eine Unterweisung im Datenschutzrecht<br>• Es werden jährlich Maßnahmen zur Steigerung der Awareness bzgl. IT-Sicherheit durchgeführt |

| | |
|---|---|
| | |

- Dokumentation

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| | • Es existiert ein Datenschutzkonzept<br>• Es existiert ein Berechtigungskonzept<br>• Es existiert ein IT-Sicherheitskonzept<br>• Es existiert ein Incident-Notfall-Plan<br>• Es existiert serverseitig ein Backupkonzept<br>• Es existiert ein Archivierungskonzept<br>• Es existiert ein Löschkonzept<br>• Es existiert ein Verzeichnis der Verarbeitungstätigkeiten |

## 1.2 Spezielle Technisch-Organisatorische Maßnahme

- Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zur Zuordenbarkeit erforderlichen zusätzlichen Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, so dass der Verantwortliche keinen Zugriff auf diese Informationen hat.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| | |

| | |
|---|---|
| • Bei einer Pseudonymisierung werden Zuordnungsdaten in einem getrennten und abgesicherten System aufbewahrt, auf welche die pseudonymen Daten verarbeitende Personen keinen Zugriff haben<br>• Selbst bei einem Vollzugriff auf die Datenbank kann der Angreifer keine personenbezogenen Daten auslesen.<br>• Die pseudonymisierten Daten verlassen das System nicht.<br>• Eine Prüfung auf Unplausibilitäten und Dopplungen im Vorfeld einer Pseudonymisierung erfolgt grundsätzlich automatisiert | • Es werden alle Daten pseudonymisiert verarbeitet oder es existiert eine Begründung, warum eine pseudonyme Verarbeitung nicht möglich ist<br>• Personenbezogene Daten werden pseudonymisiert abgelegt. |

- Verschlüsselung

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Automatische Verschlüsselung von Daten, die auf über USB angeschlossene externe Datenträger gespeichert werden<br>• Verschlüsselung von Notebooks | • Es ist gewährleistet, dass die Erzeugung des Schlüssels bzw. Schlüsselmaterials ein sicherer Prozess ist<br>• Dienstnotebooks werden von uns gesichert, im übrigen gibt es Mobile Device Management. Studiendaten werden nicht auf privaten Endgeräten verarbeitet.<br>• Es ist sichergestellt, dass der Salt und/oder der Schlüssel bzw. das Schlüsselmaterial derart erzeugt werden, dass diese weder vorhersagbar sind noch erraten werden können<br>• Es ist gewährleistet, dass die Vertraulichkeit des Schlüssels bzw. des Schlüsselmaterials während des vollständigen Lebenszyklus der verarbeiteten personenbezogenen Daten gewährleistet ist<br>• Es ist sichergestellt, dass der Zugriff auf den Salt und/oder den Schlüssel |

| | |
|---|---|
| | bzw. das Schlüsselmaterial auf ein absolutes Minimum vertrauenswürdiger Anwender beschränkt ist<br>• Es werden ausschließlich Standard-Verschlüsselungsalgorithmen entsprechend den Empfehlungen anerkannter Organisationen verwendet<br>• Es ist sichergestellt, dass das verwendete Verfahren eine hinreichende Stärke sowie keinerlei bekannte Schwächen aufweist<br>• Es ist gewährleistet, dass der Schlüssel geheim gehalten wird<br>• Es ist sichergestellt, dass ausschließlich Standard-Hash-Funktionen verwendet werden, für die es keine bekannten Schwachstellen gibt<br>• Es ist sichergestellt, dass bei Verwendung von Hash-Funktionen ein Salt benutzt wird<br>• Es ist sichergestellt, dass der Salt von ausreichender (Mindestentropie von 100 Bit) Qualität ist |

## Vertraulichkeit

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren, schützen personenbezogene Daten vor unbefugtem physischem Zugriff. D.h. unbefugte Personen erhalten keinen physischen Zugriff auf Datenträgern, auf denen personenbezogene Daten gespeichert sind.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| Der Zutritt zu den Geschäftsräumen ist durch ein manuelles Schließsystem gesichert. | • Es existiert ein Zutrittskontrollsystem, in welchem die zutrittsberechtigten Mitarbeiter festgelegt sind<br>• Es erfolgen folgende Zutrittskontrollen für den Zutritt zum Betriebsgelände/Gebäude<br>1. Empfang<br>2. Verschließen von Türen und Fenstern, sobald Personal nicht im Raum<br>• Es bestehen Regelungen für den Zutritt von Fremdpersonal, Reinigungspersonal, Besucher |

| | |
|---|---|
| | • Differenzierte Sicherheitsbereiche/-zonen (z. B. für Server, Großrechner, Archiv) sind festgelegt<br>• Die Datenträger sind Bestandteil des Zutrittsschutzkonzepts<br>• Es liegt eine Anweisung zur Ausgabe von Schlüsseln vor |

Zugangskontrolle

Maßnahmen zur Zugangskontrolle dienen der Verhinderung der unbefugten Nutzung von Anlagen/Systemen, mit welchen (personenbezogene) Daten verarbeitet werden.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| Die unbefugte Nutzung von IT-Systemen wird wie folgt verhindert:<br><br>Mitarbeiter:innen:<br><br>• User-ID<br>• Benutzername/Passwort<br>• Zwei-Faktor-Authentifizierung<br><br>Nutzer:innen:<br><br>• User-ID<br>• Benutzername/Passwort<br>• Zwei-Faktor-Authentifizierung<br>• Sperrung des Kontos nach 3-maligen Fehlversuchen, erneute Anmeldung erst nach 1, 2, 5, 10, 60 Minuten (Staffelung) möglich<br><br>• Zwei-Faktor-Authentifizierung, die zwei Faktoren sind<br>1. Zwei-Faktor-Authentifizierung Benutzername/Passwort (statisch)<br>2. Einmal Passwort / Mobiltelefon | Mitarbeiter:innen:<br><br>• Es existiert eine Benutzerverwaltung, in welcher Benutzern Authentifizierungsmöglichkeiten zugewiesen werden<br>• Für Zugriff auf interne Daten wird ein Passwort-Management-System eingesetzt über das Zugriffsrechte geregelt werden.<br>• Es gibt eine Richtlinie zur Vergabe und Nutzung von Passwörtern<br>• Jeder Berechtigte verfügt über ein eigenes nur ihm bekanntes Passwort<br>• Neue Schwachstellen in den IT-Systemen werden nach Bekanntwerden gemeldet, analysiert und ggf. behoben, um das Eindringen seitens unbefugter Dritter in die IT-Systeme zu verhindern |

| | |
|---|---|
| • Passwörter werden ausschließlich verschlüsselt gespeichert<br>• Über alle Aktivitäten in den IT-Systemen werden automatisch Protokolle erstellt | |

Zugriffskontrolle

Hierunter fallen Maßnahmen, welche dafür Sorge tragen sollen, dass die zur Benutzung eines Informationssystems Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und eine unberechtigte Verarbeitung verhindert wird.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Mitarbeiter:innen müssen alle relevanten Passwörter in einem firmeninternen Passwortmanager verwalten. | • Es besteht ein dokumentiertes Berechtigungsmanagement (Berechtigungskonzept), in dem verbindlich geregelt ist, wie Berechtigungen beantragt, freigegeben, umgesetzt und wieder entzogen werden<br>• Gewährte Zugriffsrechte werden dokumentiert<br>• Im Rahmen dieses Berechtigungsmanagements ist nachweisbar, wer wann welche Berechtigungen innehatte<br>• Es bestehen differenzierte Berechtigungen, diese werden im Passwortmanager über die Gruppenzuweisungen geregelt.<br>• Bei der Programmentwicklung erfolgt eine Funktionstrennung zwischen Test- und Produktionsumgebung |

Weitergabekontrolle

Hierbei handelt es sich um Maßnahmen, die verhindern, dass Daten unbefugt weitergegeben werden. Insbesondere soll verhindert werden, dass Daten bei einer elektronischen Übertragung bzw. Transport nicht unbefugt verarbeitet werden können.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| | |

| | |
|---|---|
| • Bei der Übertragung der Daten zwischen unserem System auf dem Gerät des Nutzers sind die Daten verschlüsselt.<br>• Nicht angemeldete Nutzer:innen erhalten bei Ansicht der Anwendung bzw. beim Erhalt von Emails keine personenbezogenen Daten.<br>• Angemeldete und authentifizierte Nutzer:innen erhalten innerhalb der Anwendung nur Zugriff auf die von ihnen eingegebenen oder explizit für sie freigegebenen Daten. | Insbesondere bezüglich Nutzer:innen:<br>• Nutzer:innen der Anwendung können nur auf solche Daten zugreifen, die sie selber eingegeben haben oder die gezielt an sie weitergegeben wurden.<br>• Nutzer:innen der Anwendung können nur Daten auf die sie Zugriff haben gezielt an andere Nutzer:innen weitergeben.<br>• Die Anwendung unterstützt den Export von personenbezogenen Daten nicht, mit Ausnahme des Ausdruckens von Förderplänen. |

Trennungskontrolle

Hierbei handelt es sich um Maßnahmen, welche gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann beispielsweise durch logische oder physikalische Trennung der Daten erreicht werden.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Nutzer:innen der Anwendung können nur auf solche Daten zugreifen, die sie selber eingegeben haben oder die gezielt an sie weitergegeben wurden.<br>• Durch systemweit eindeutige Identifikationsbezeichnungen können die Daten immer genau den berechtigten Nutzer:innen zugeordnet werden.<br>• Es existiert eine Trennung zwischen Test- und Produktivdaten | • Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung der Daten anderer Mandanten Rechnung trägt |

Zweckbindung

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| | |

| | |
|---|---|
| | • Es werden nur solche Daten verarbeitet, die unmittelbar dem eigentlichen Zweck dienen und die zur Erfüllung der Aufgabe oder Durchführung des Prozesses notwendig sind |

## ▪ Integrität

Eingabekontrolle

Diese Maßnahmen sollen dafür sorgen, dass man nachträglich feststellen kann, ob und wenn ja von wem personenbezogene Daten in informationstechnischen Systemen eingegeben, verändert oder entfernt worden sind.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Von einer Protokollierung jeglicher Änderungen der gespeicherten Daten wird abgesehen, da das Protokoll an sich wieder personenbezogene Daten enthalten würde. | • Es ist sichergestellt, dass die personenbezogenen Daten nicht außerhalb der App (z.B. von Mitarbeiter:innen) verändert werden können (Ausnahme: Administrator:in)<br>• Mitarbeiter:innen können nur die von ihnen angelegten Daten ändern und einsehen. |

Auftragskontrolle

Hierunter fallen Maßnahmen, welche gewährleisten, dass im Auftrag verarbeitete personenbezogene Daten nur entsprechend der Weisungen des Auftraggebers verarbeitet werden.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Es existiert eine Dokumentation, welche die lückenlose Nachvollziehbarkeit der einzelnen im Rahmen der Auftragsausführung erforderlichen Arbeitsschritte gewährleistet | • Auftragsverarbeiter werden ausschließlich nach einer Überprüfung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt<br>• Es werden nur Auftragsverarbeiter ausgewählt, die eine Einhaltung aller datenschutzrechtlichen Anforderungen sicherstellen und einen externen Datenschutzbeauftragten bestellen. |

| | |
|---|---|
| | • Es existiert ein Vertrag zur Auftragsverarbeitung, der den Anforderungen der DSGVO genügt.<br>• Die weisungsbefugten Personen auf Seite des Auftraggebers sind benannt und beim Auftragnehmer bekannt<br>• Subunternehmer von Auftragsverarbeitern sind vertraglich an dieselben Pflichten gebunden wie Auftragsverarbeiter.<br>• Mitarbeiter:innen des Auftragsverarbeiters sind auf das Datengeheimnis verpflichtet.<br>• Auftragsverarbeiter verarbeiten keine Daten außerhalb der EU, ein Datentransfer ist untersagt. |

### ▪ Verfügbarkeit

Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten gegen zufällige Zerstörung oder zufälligen Verlust geschützt sind.

Backup- und Recoverykonzept

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Backups werden regelmäßig auf Datenvollständigkeit kontrolliert | • Es existiert ein angemessenes Backup- und Recoverykonzept mit täglicher Sicherung aller relevanten Daten und Konfigurationen<br>• Es ist festgelegt, welche Daten für welchen Zeitraum gesichert werden und die anschließende Löschung der Daten ist gewährleistet (automatische tägliche Sicherung, sieben Tage Aufbewahrung)<br>• Backups werden (auch) geografisch an von den Servern unterschiedliche Speicherorte aufbewahrt |

### ▪ Belastbarkeit/ Ausfallsicherheit/Wiederherstellbarkeit

Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten bei Verlust oder Zerstörung schnell wiederhergestellt werden können.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| | |

| | |
|---|---|
| • Es existiert ein Netzwerk-Monitoring, welches alle relevanten Server, Dienste und Prozesse überwacht und Abweichungen zuverlässig meldet | • Es wurde festgelegt, welche Person bei welcher Störung oder welchem Ausfall zu benachrichtigen ist<br>• Es existiert ein Notfallplan mit Regelungen wie beispielsweise |

Server- und Client-Absicherung

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Es existiert für jeden Server ein passendes Image, so dass bei Bedarf der Server jederzeit wiederhergestellt werden kann.<br>• Die vom Auftragnehmer installierten auftragsrelevanten Dienste werden 24/7 überwacht und gemäß des vereinbarten Service Level Agreements im Falle einer Störung entsprechend entstört.<br>• Sachgerechter Einsatz dem technischen Standard entsprechende Sicherheitssoftware (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter). | |

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
- Datenschutz-Management

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Beschäftigte nach Bedarf / Berechtigung<br>• Sicherheitskonzept | • Verantwortlichkeiten sind eindeutig zugewiesen<br>• Benannter Externer Datenschutzbeauftragter |

| | |
|---|---|
| • FAQ<br>• Datenschutzerklärung<br>• DSFA<br>• Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig durchgeführt<br>+ Alle zwei Jahre | • Beschäftigte geschult und auf Vertraulichkeit/Geheimhaltung verpflichtet<br>• Regelmäßige Sensibilisierung der Mitarbeiter:innen<br>• Datenschutz durch Technikgestaltung („Privacy by Design) wird bei allen Verarbeitungsprozessen umgesetzt<br>• Datenschutz durch datenschutzfreundliche Voreinstellungen („Privacy by Default) wird bei allen Verarbeitungsprozessen umgesetzt. (z.B. werden nach dem Login alle personenbezogenen Daten der Teilnehmenden unleserlich dargestellt, um den "Blick über die Schulter" zu verhindern)<br>• Datenschutz-Folgenabschätzung ist durchgeführt<br>• Betroffenenrechte werden gewährleistet<br>• Verzeichnis von Verarbeitungstätigkeiten existiert und ist auf dem jeweils aktuellen Stand<br>• Dokumentation aller Verletzungen des Schutzes personenbezogener Daten |

- Incident-Response-Management (IT-Störungsmanagement)

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| • Es existiert ein Netzwerk-Monitoring, welches alle relevanten Server, Dienste und Prozesse überwacht und Abweichungen zuverlässig meldet<br>• Intrusion-Prevention-System | • Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)<br>• Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen<br>• Team zum Umgang mit Sicherheitsvorfällen gebildet und Team beinhaltet<br>+ Mitglied der Geschäftsführung<br>+ IT-Leiter<br>+ Datenschutzbeauftragter<br>• Dokumentation von Sicherheitsvorfällen und Datenpannen |

- Ergänzende Maßnahmen
  - Rechenzentrum Zertifizierung nach ISO 27001
  - Unterauftragsverarbeiter zertifiziert nach ISO 9001