Datenschutzkonzept für das Projekt

xxx

Projektleitung:

Hinweis

Zusätzlich sind die forschende Stelle (beispielsweise Universität oder Rehabilitationseinrichtung), ihre Rechtsform und gegebenenfalls Förderer des Projektes zu benennen.

Stand xx.xx.xxxx

Achtung!

Alle Hinweise sind vor Übersendung an die DRV zu entfernen.

Inhalt

[**1.** **Einleitung** 4](#_Toc96336659)

[**2.** **Grundsätze des Datenschutzes** 4](#_Toc96336665)

[**2.1.** **Rechtmäßigkeit der Verarbeitung** 4](#_Toc96336666)

[**2.1.1.** **Einwilligung** 4](#_Toc96336667)

[**2.1.2.** **Gesetzliche Grundlagen** 5](#_Toc96336668)

[**2.2.** **Zweckbindung** 5](#_Toc96336669)

[**2.3.** **Datenminimierung** 5](#_Toc96336670)

[**2.4.** **Speicherbegrenzung** 5](#_Toc96336671)

[**2.5.** **Integrität und Vertraulichkeit** 5](#_Toc96336672)

[**3.** **Arten personenbezogener Daten im Forschungsprojekt** 6](#_Toc96336673)

[**4.** **Beteiligte Einrichtungen und ihre Aufgaben im Prozess** 6](#_Toc96336674)

[**4.1.** **Stelle A (beispielsweise Universität xy)** 6](#_Toc96336675)

[**4.2.** **Stelle B (beispielsweise Reha-Zentrum xy/Klinik xy)** 6](#_Toc96336676)

[**4.3.** **Stelle C (beispielsweise Deutsche Rentenversicherung xy)** 6](#_Toc96336677)

[**5.** **Prozesse der Datenverarbeitung** 7](#_Toc96336678)

[**5.1.** **Rekrutierung der Teilnehmenden** 7](#_Toc96336679)

[**5.1.1.** **Stichprobenziehung** 7](#_Toc96336680)

[**5.1.2.** **Kontaktierung und Einladung** 7](#_Toc96336681)

[**5.1.3.** **Aufklärung und Einwilligung** 7](#_Toc96336682)

[**5.1.4.** **Widerruf der Einwilligung** 7](#_Toc96336683)

[**5.2.** **Datenerhebung bei den Teilnehmenden** 7](#_Toc96336684)

[**5.2.1.** **Untersuchung im Reha-Zentrum** 7](#_Toc96336685)

[**5.2.2.** **Befragungen** 7](#_Toc96336686)

[**5.2.3.** **Interviews** 8](#_Toc96336687)

[**5.2.4.** **Untersuchungen mit Datenübertragung von diagnostischen Geräten** 8](#_Toc96336688)

[**5.3.** **Datenerhebung bei Dritten** 8](#_Toc96336689)

[**5.3.1.** **Entbindung von der ärztlichen Schweigepflicht** 8](#_Toc96336690)

[**5.3.2.** **Behandelnde Ärzte** 8](#_Toc96336691)

[**5.3.3.** **Deutsche Rentenversicherung** 8](#_Toc96336692)

[**5.3.4.** **Arbeitgeber** 8](#_Toc96336693)

[**5.3.5.** **Rehabilitationseinrichtungen** 8](#_Toc96336694)

[**5.3.6.** **Krankenhäuser** 8](#_Toc96336695)

[**5.4.** **Aufbewahrung der Unterlagen** 8](#_Toc96336696)

[**5.5.** **Löschung / Speicherdauer der Daten** 8](#_Toc96336697)

[**5.6.** **Regelungen bei Datenschutzverletzungen** 9](#_Toc96336698)

[**6.** **Umsetzung der Rechte der Teilnehmenden** 9](#_Toc96336699)

[**7.** **Technische und organisatorische Maßnahmen** 9](#_Toc96336700)

[**7.1.** **Pseudonymisierung** 10](#_Toc96336701)

[**7.2.** **Verschlüsselung** 10](#_Toc96336702)

[**7.2.1.** **Verschlüsselung bei der Datenübertragung** 10](#_Toc96336703)

[**7.2.2.** **Verschlüsselung der Dateien** 10](#_Toc96336704)

[**7.2.3.** **Verschlüsselung der Datenträger** 10](#_Toc96336705)

[**7.3.** **Zutrittskontrolle** 10](#_Toc96336706)

[**7.4.** **Zugangskontrolle** 10](#_Toc96336707)

[**7.5.** **Zugriffskontrolle** 10](#_Toc96336708)

[**7.6.** **Weitergabekontrolle** 11](#_Toc96336709)

[**7.7.** **Sensibilisierung der am Projekt Beteiligten** 11](#_Toc96336710)

[**7.8.** **Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme** 11](#_Toc96336711)

[**7.8.1.** **Vertraulichkeit** 11](#_Toc96336712)

[**7.8.2.** **Integrität** 11](#_Toc96336713)

[**7.8.3.** **Verfügbarkeit** 11](#_Toc96336714)

[**7.8.4.** **Belastbarkeit** 12](#_Toc96336715)

[**8.** **Auftragsverarbeitung** 12](#_Toc96336716)

[**9.** **Datenschutz-Folgenabschätzung (DSFA)** 12](#_Toc96336717)

[**10.** **Anlagen** 12](#_Toc96336718)

# **Einleitung**

Das vorliegende Konzept beschreibt alle Maßnahmen zum Datenschutz und zur
IT-Sicherheit für das Projekt „xxx“. Inhalt und Ablauf des Projekts sind der Anlage „Projektskizze“ zu entnehmen.

Jede am Projekt beteiligte Institution stellt sicher, dass die Datenverarbeitung in Übereinstimmung mit diesem Datenschutzkonzept erfolgt.

Bei Änderungen im Projektablauf wird das Datenschutzkonzept überprüft und gegebenenfalls angepasst.

# **Grundsätze des Datenschutzes**

Bei der Verarbeitung personenbezogener Daten müssen bestimmte Grundsätze eingehalten werden, die im Artikel 5 Datenschutzgrundverordnung (DSGVO) definiert sind.

## **Rechtmäßigkeit der Verarbeitung**

Hinweis

Rechtmäßigkeit bedeutet, dass Daten nur verarbeitet werden dürfen, wenn es dafür eine Rechtsgrundlage gibt. Dies kann die Einwilligung der Projektteilnehmer sein oder eine gesetzliche Vorschrift, die die Verarbeitung zum Forschungszweck ausdrücklich erlaubt. Es sind nur Ausführungen zu den Gesetzen festzuhalten, die bei der Durchführung des Projektes zu berücksichtigen sind.

### **Einwilligung**

Die Teilnahme am Forschungsprojekt basiert auf der freiwilligen, informierten Einwilligung entsprechend der Anforderungen des Artikel 6 Absatz 1 Buchstabe a DSGVO in Verbindung mit Artikel 7 DSGVO. Zur Projektteilnahme eingeladene Personen erhalten vorab eine schriftliche Teilnahmeinformation, in der sie über den geplanten Ablauf des Projektes, Vor- und Nachteile ihrer Projektteilnahme und Fragen zum Datenschutz informiert werden.

Hinweis

Die Teilnahmeinformation und gegebenenfalls die Einwilligung sind als Anlage beizufügen.

### **Gesetzliche Grundlagen**

Hinweis

Bei den im Folgenden aufgeführten gesetzlichen Grundlagen handelt es sich lediglich um eine mögliche Auswahl. Die Auswahl ist an das aktuelle Projekt anzupassen.

####  **Datenschutzgrundverordnung (DSGVO)**

####  **Bundesdatenschutzgesetz (BDSG)/Landesdatenschutzgesetz (LDSG)**

####  **Sozialgesetzbuch (SGB)**

####  **Telemediengesetz (TMG)**

####  **Medizinproduktegesetz (MPG)**

####  **Arzneimittelgesetz (AMG)**

##  **Zweckbindung**

Die im Forschungsprojekt erhobenen personenbezogenen Daten werden nur für das Erreichen der Ziele dieses Projektes verarbeitet. Eine weitere Verarbeitung der Daten ist nur zulässig, wenn die unter Punkt 2.1 genannten Voraussetzungen erfüllt sind.

##  **Datenminimierung**

Die Verarbeitung der personenbezogenen Daten im Forschungsprojekt ist auf das für das Ziel des Projekts notwendige Maß beschränkt. Es werden nur Daten erhoben, die für das Erreichen des Forschungsziels unbedingt erforderlich sind.

##  **Speicherbegrenzung**

Personenbezogene Daten werden nur so lange aufbewahrt, wie es für das Erreichen des Ziels des Projekts erforderlich ist. Die genauen Aufbewahrungsfristen sind unter Punkt 5.5 definiert.

## **Integrität und Vertraulichkeit**

Integrität und Vertraulichkeit der personenbezogenen Daten werden durch geeignete technische und organisatorische Maßnahmen gewährleistet. Diese Maßnahmen sollen sicherstellen, dass der Zugriff und gegebenenfalls die Veränderung der personenbezogenen Daten nur durch berechtigte Personen erfolgt. Die einzelnen Maßnahmen werden unter Punkt 7 beschrieben.

# **Arten personenbezogener Daten im Forschungsprojekt**

Hinweis

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Identifizierbar ist eine Person, die direkt oder indirekt durch Zuordnung zu einer Kennung oder einem besonderen Merkmal identifiziert werden kann.

Die Daten sind präzise und umfassend zu benennen. Eine allgemeine Aufzählung ist nicht ausreichend.

Im Forschungsprojekt sollen folgende personenbezogene Daten verarbeitet werden:

* …
* …
* …

# **Beteiligte Einrichtungen und ihre Aufgaben im Prozess**

Hinweis

Hier sind alle Stellen einschließlich ihrer Rechtsformen zu benennen, die personenbezogene Daten im Forschungsprojekt verarbeiten. Des Weiteren sind deren Aufgaben und der Umgang mit den personenbezogenen Daten ausführlich zu beschreiben.

## **Stelle A (beispielsweise Universität xy)**

## **Stelle B (beispielsweise Reha-Zentrum xy/Klinik xy)**

## **Stelle C (beispielsweise Deutsche Rentenversicherung xy)**

# **Prozesse der Datenverarbeitung**

Hinweis

Hier sind die einzelnen Prozesse des Forschungsprojektes zu beschreiben, in denen ein Umgang mit personenbezogenen Daten erfolgt. Ab Punkt 5.1 bis 5.6 sind mögliche Teilprozesse eines Forschungsprojekts aufgeführt. Diese Aufzählung ist beispielhaft und an den Ablauf des aktuellen Projekts anzupassen.

## **Rekrutierung der Teilnehmenden**

### **Stichprobenziehung**

### **Kontaktierung und Einladung**

### **Aufklärung und Einwilligung**

### **Widerruf der Einwilligung**

####  **Möglichkeiten und Konsequenzen des Widerrufs**

####  **Form des Widerrufs**

####  **Umsetzung des Widerrufs**

## **Datenerhebung bei den Teilnehmenden**

### **Untersuchung im Reha-Zentrum**

### **Befragungen**

####  **Befragung zum Zeitpunkt t1**

####  **Befragung zum Zeitpunkt t2**

####  **Befragung zum Zeitpunkt t3**

### **Interviews**

####  **Interview mit den Teilnehmenden**

####  **Interview mit Beschäftigten der Reha-Zentren**

### **Untersuchungen mit Datenübertragung von diagnostischen Geräten**

####  **MRT**

####  **EKG**

## **Datenerhebung bei Dritten**

### **Entbindung von der ärztlichen Schweigepflicht**

#### **Gegenstand der Schweigepflichtentbindung**

#### **Adressaten der Schweigepflichtentbindung**

#### **Voraussetzung der Schweigepflichtentbindung**

#### **Gültigkeit und Dauer der Schweigepflichtentbindung**

### **Behandelnde Ärzte**

### **Deutsche Rentenversicherung**

### **Arbeitgeber**

### **Rehabilitationseinrichtungen**

### **Krankenhäuser**

## **Aufbewahrung der Unterlagen**

Personenbezogene Daten werden getrennt von den Forschungsdaten aufbewahrt. Hier ist beschrieben, wo die einzelnen Unterlagen aufbewahrt werden und wer Zugriff auf die Daten hat.

## **Löschung / Speicherdauer der Daten**

Hinweis

Anzugeben sind die konkreten Aufbewahrungs- und Löschfristen, bezogen auf die einzelnen Verarbeitungsschritte und die verschiedenen Datenkategorien. Ein allgemeiner Verweis auf einen möglichen Löschzeitpunkt genügt nicht. Es sind präzise Angaben erforderlich.

## **Regelungen bei Datenschutzverletzungen**

Gemäß Artikel 33 DSGVO sind Verletzungen des Schutzes personenbezogener Daten der zuständigen datenschutzrechtlichen Aufsichtsbehörde zu melden. Diese Meldung muss durch den Verantwortlichen unverzüglich möglichst innerhalb von 72 Stunden nach Bekanntwerden erfolgen.

Hinweis

Für das Forschungsprojekt ist der Umgang mit Datenschutzverletzungen zu beschreiben.

# **Umsetzung der Rechte der Teilnehmenden**

Die Teilnehmenden sind zum Zeitpunkt der Erhebung der personenbezogenen Daten über ihre Rechte gemäß der Datenschutzgrundverordnung zu informieren.

Sie haben das Recht auf Auskunft, das Recht auf Berichtigung, das Recht auf Löschung, das Recht auf Einschränkung der Verarbeitung, auf Datenübertragbarkeit und das Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 15-18, 20 und 77 DSGVO). Genauere Hinweise sind der Anlage „Teilnahmeinformation“ zu entnehmen.

Hinweis

Die Rechte der Teilnehmenden sind im Projekt umzusetzen. Es sollten Prozesse festgelegt und beschrieben werden, wie die Rechte umzusetzen sind.

# **Technische und organisatorische Maßnahmen**

Bei der Verarbeitung besonderer Kategorien personenbezogener Daten (beispielsweise Gesundheitsdaten) sind gemäß § 22 Bundesdatenschutzgesetz (BSDG) angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen vorzusehen.

Hinweis

Die technischen und organisatorischen Maßnahmen des Forschungsprojektes sind zu beschreiben. Ab Punkt 7.1 sind mögliche Maßnahmen aufgeführt. Diese Aufzählung ist nicht abschließend und an das aktuelle Projekt anzupassen.

## **Pseudonymisierung**

Hinweis

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne zusätzliche Informationen nicht mehr einer bestimmten Person zugeordnet werden können.

Hier ist darauf zu achten, dass die Zuordnungsliste immer getrennt von den Forschungsdaten aufbewahrt wird.

## **Verschlüsselung**

###  **Verschlüsselung bei der Datenübertragung**

####  **VPN-Tunnel**

####  **SSL-Verbindungen**

### **Verschlüsselung der Dateien**

### **Verschlüsselung der Datenträger**

##  **Zutrittskontrolle**

Hinweis

Es sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet werden, zu verwehren (beispielsweise Tür mit Knauf, Tür nur mit Schlüssel zu öffnen).

## **Zugangskontrolle**

Hinweis

Es sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (beispielsweise durch ein Passwort, Dienstausweis).

## **Zugriffskontrolle**

Hinweis

Es sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind, zu gewährleisten, dass die Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (beispielsweise durch ein Rechte- und Rollenkonzept).

## **Weitergabekontrolle**

Hinweis

Es sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt verarbeitet werden können. Weiterhin sind Maßnahmen zu treffen, dass überprüft und festgestellt werden kann, an welche Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (beispielsweise Sendung verschlüsselter E-Mails).

## **Sensibilisierung der am Projekt Beteiligten**

## **Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme**

### **Vertraulichkeit**

Hinweis

Die personenbezogenen Daten sind vor unbefugter Kenntnisnahme zu schützen.

### **Integrität**

Hinweis

Integrität ist die Verhinderung einer unautorisierten Veränderung der Daten. Es soll die Echtheit, Vollständigkeit, Zurechenbarkeit, Urheberschaft und Rechtsgültigkeit der Daten sichergestellt werden (Zugriffsprotokollierung).

### **Verfügbarkeit**

Hinweis

Es muss eine Bereitstellung der Daten und die Möglichkeit zur ordnungsgemäßen Verarbeitung gewährleistet werden (beispielsweise Sicherungskopie, geordnete Ablage).

### **Belastbarkeit**

Hinweis

Wenn es erforderlich ist, dass die Daten auch bei „Belastungsspitzen“, Ausfällen oder Angriffen verfügbar sind, sind hier geeignete Maßnahmen zu beschreiben.

# **Auftragsverarbeitung**

Hinweis

Werden personenbezogene Daten nicht ausschließlich durch die Verantwortlichen verarbeitet, ist zu prüfen, ob eine Auftragsverarbeitung vorliegt.

Ist eine Verarbeitung im Auftrag für das Projekt erforderlich, sind an dieser Stelle die Vertragspartner, die dort zu verarbeitenden Daten und die getroffenen Sicherheitsmaßnahmen zu beschreiben.

# **Datenschutz-Folgenabschätzung (DSFA)**

Hinweis

Weist eine Verarbeitung besondere Risiken (beispielsweise bei der Verarbeitung besonderer Kategorien personenbezogener Daten) für die Rechte der betroffenen Personen auf, ist vor Beginn der Verarbeitung eine DSFA durchzuführen.

An dieser Stelle ist anzugeben, ob und mit welchem Ergebnis geprüft wurde, ob eine DSFA durchzuführen ist. Fügen Sie bitte die entsprechenden Nachweise bei.

# **Anlagen**

Projektskizze

Teilnahmeinformation“

Einwilligung