# Datensicherheits- und Datenschutzinformation über Datennutzungsprojekte

Bitte lesen Sie das Formular durch und füllen Punkte 1 bis 5 aus. Auf der letzten Seite findet sich ein Unterschriftenfeld, mit der Sie die Kenntnisnahme des Datensicherheits- und Datenschutzkonzept für Datennutzungsprojekte bestätigen. Weitere offene Punkte im Dokument werden zusammen mit dem Datenintegrationszentrum ausgefüllt.

## Vorhaben

      *(Titel des Vorhabens)*

## Zielsetzung des Vorhabens / Zweckbestimmung der genutzten personenbezogenen Daten

      (*Projektbeschreibung aus dem Antrag)* oder siehe Datennutzungsantrag

## Betroffener Personenkreis

      *(Von welchen Personen werden personenbezogene Daten erhoben, verarbeitet und genutzt – bspw. Patienten; Mitarbeiter, …?)* oder siehe Datennutzungsantrag

## Beteiligte Stellen

Durchführende Einrichtung (Klinik/Institut):       (oder siehe Datennutzungsantrag)

Zutreffendes bitte ankreuzen:

[ ]  Mitbetreuung des Projekts in medizinischen und labormedizinischen Fragestellungen: Frau Prof. Ceglarek/ Stellvertretung Herr Dr. Baber (Data Access Committee ILM: MB-ZLab-study@medizin.uni-leipzig.de)

[ ]  Mitbetreuung des Projekts in medizininformatischen und statistischen Fragestellungen: Prof. Dr. Markus Löffler und Dr. Frank Meineke (IMISE)

[ ]  Mitbetreuung des Projekts in medizininformatischen und statistischen Fragestellungen: Prof. Dr. Toralf Kirsten (Medizininformatik/Medical Data Science)

Unterstützende Einrichtung: Datenintegrationszentrum, mit

* organisatorische Betreuung des Nutzungsprojektes
* Einholung von Zustimmungen der Fachabteilungen des UKL zur Datenverwendung
* Datenausleitung
* Pseudonymisierung

## Zugriffsberechtigte Personen der beteiligten Stellen (Funktionsbezeichnungen)

Durchführende Einrichtung (Antragsteller:in):

1. (verantwortliche Wissenschaftler:in)
	1. (Stellvertreter:in)
2. (ausführende Wissenschaftler:in)
	1. (Stellvertreter:in)
3. (. . . . . . . . . . . . . . . . . . . . . . . . . . . . .)
	1. (Stellvertreter:in)

Unterstützende Einrichtung:

Datenintegrationszentrum (Team Datenextraktion, Team Datenmanagement, Team Ablauforganisation)

## Beschreibung der erhobenen, genutzten, verarbeiteten Daten sowie deren Erforderlichkeit

Eine genaue Übersicht ist in Anlage 1 zum Datennutzungsantrag enthalten. Es werden nur Datenelemente, die für die Fragestellung des Projektes erforderlich sind, aufgeführt und verarbeitet.

## Rechtsgrundlage zur Datenverarbeitung

Rechtsgrundlage: §29 Sächsisches Krankenhausgesetz (Sächs. KHG). Patientendaten werden innerhalb des UKL für eigene wissenschaftliche und qualitätssichernde Zwecke genutzt.

Bei Nutzung von an anderen Fachabteilungen (bspw. Kliniken) des UKL erhobenen Daten:

[ ]  Informationsschreiben an Kliniks-/Institutsdirektor:innen

## Datenflüsse / Schnittstellen zwischen den beteiligten Stellen und deren Absicherung

Die Daten werden im Rahmen der Behandlung in den Fachabteilungen des UKL erhoben und in verschiedenen Krankenhausinformationssystemen gespeichert. Das Datenintegrationszentrum leitet die gewünschten Parameter aus den entsprechenden Systemen aus.

Das DIZ betreibt einen zentralen Datenspeicher in der klinischen Domäne und transferiert die Daten zur Forschungsdomäne (s. Architekturskizze).

Das DIZ stellt diese Daten über einen gesicherten Ordner im Laufwerk W dem Antragssteller zur Verfügung. Dieser Ordner ist nur für die beteiligten Personen (durchführende Einrichtung und unterstützende Einrichtung) freigeben.

[ ]  Abweichend zur obigen Darstellung wurde gemeinsam mit dem DIZ vereinbart:      .

## Darstellung Speicherorte und deren Absicherung

[ ]  Laufwerk W. Der Ordner wird noch angelegt. Zugriffskontrolle und –erteilung erfolgen durch DIZ-Mitarbeiter.

[ ]  Datenbereitstellung über: . . . . . . . . . . . . . . . . . . . . . .

Alle Daten, die im Projekt verarbeitet werden, werden auf einem klinikinternen Netzlaufwerk mit Zugriffsbeschränkung abgelegt.

## Verfahren zur Pseudonymisierung / Anonymisierung

Es erfolgt ein Pseudonymisierungsverfahren über direkt angewandte Skripte des Datenintegrationszentrums. Es werden keine Klarnamen, Adressen oder Geburtsdaten ausgeleitet. Im Sinne der Datensparsamkeit können Fallnummern verwendet werden.

Hinweis:

Nach §29 Abs.4 SächsKHG sind nach Erreichen des Forschungszwecks alle Daten zu anonymisieren. Dies bedeutet, dass alle personenidentifizierenden Daten entfernt werden müssen.

## Art der Archivierung / Speicherfristen

Ein Archivordner wird vom Bereich 1 des UKL bereitgestellt.

[ ]  Die Löschung der Daten erfolgt 5 Jahre nach Projektende.

[ ]  Die Löschung der Daten erfolgt 10 Jahre nach Publikation der Ergebnisse (nach den Regeln der Guten Wissenschaftlichen Praxis, DFG)

[ ]  Die Löschung der Daten erfolgt nach       Jahren, gemäß      .

## Art des Löschens / Vernichtens von Daten und Datenträgern

Verwaltung der physischen Datenträger erfolgt durch den Bereich 1 des UKL.

Löschung und Löschaufträge werden durch das Datenintegrationszentrum ausgelöst.

## Geltendmachung von Rechten Betroffener

Betroffene können ihre Rechte jederzeit durch das Datenintegrationszentrum (Teams Consentmanagement und Ablaufmanagement) wahrnehmen. Die Bearbeitung der Anfragen erfolgt in Kooperation mit Datenschutzbeauftragten des UKL.

## Gibt es eine Art Qualitätssicherung, Monitoring?

Auf Seiten der Antragsteller

Wenn zutreffend

[ ]  Ja,       (Wer führt das Monitoring durch (konkrete Benennung der Person) und hat damit ebenfalls Zugriff auf die Daten? Welche Sicherheitsmaßnahmen werden ggf. ergriffen, um unbefugten Zugriff zu verhindern?)

[ ]  Nein

Am DIZ erfolgen regelmäßige Datenkontrollen und –prüfungen entsprechend den geltenden Verfahrensanweisungen.

## Technische Ausgestaltung

Durchführende Einrichtung (Antragsteller:in):

* Office-Anwendungen, Fileserver,

Unterstützende Einrichtung:

* DIZ: Office-Anwendungen, Fileserver, FHIR-Server in der klinischen Domäne

Weitere Ausführungen sind im VVT der Klinik (Durchführende Einrichtung) und des DIZ (unterstützende Einrichtung) verzeichnet. Zur Auswertung wird nur auf UKL-Rechnern und von der UKL-IT freigegebene Software genutzt. Zur Datenauswertung werden das explizit sein: Excel, SPSS, R Statistics. Mobile Datenträger werden nicht genutzt.

## Technisch-organisatorische Sicherheitsmaßnahmen

Die TOMs sind in der Datenschutzpflichtdokumentation der durchführenden und der unterstützenden Einrichtungen festgehalten. Sie werden regelmäßig aktualisiert. Darüber hinaus werden keine weiteren Verfahren angewandt, die einer besonderen, projektbezogenen Dokumentation bedürfen.

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),

Alle Räume sind durch Schließsysteme des UKL gesichert und sind nach Beendigung der Tätigkeit abzuschließen.

1. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

Rechner und Einzelprogramme sind jeweils durch Passwörter geschützt.

1. dafür Sorge zu tragen, 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 (Zugriffskontrolle),

Rechner, Ordner (Laufwerk W) und Einzelprogramme sind jeweils durch Passwörter geschützt.

1. dafür Sorge zu tragen, 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 (Übermittlungs- und Weitergabekontrolle),

Rechner, Ordner (Laufwerk W) und Einzelprogramme sind jeweils durch Passwörter geschützt.

1. dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

Die Eingabekontrolle wird vom Bereich 1 des UKL bewerkstelligt.

1. dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle), z.B. Brandschutzmaßnahmen,

Alle Daten sind auf Servern des UKL abgelegt.

Brandschutzmaßnahmen werden durch Bereich 5 des UKL wahrgenommen.

1. dafür Sorge zu tragen, dass IT-Systeme widerstandsfähig aufgestellt sind, um starke Beanspruchung überstehen zu können (Belastbarkeit),

Die Belastbarkeit wird vom Bereich 1 des UKL bewerkstelligt.

1. dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können = Daten dürfen nur zu dem Zweck verarbeitet werden, für den sie erhoben wurden – für nichts Anderes (Trennungskontrolle; Anonymitäts- und Trennungsgebot)

Ausgeleitete Daten werden nur für oben genannten Forschungszweck verwendet. Für eine Verwendung für weitere Fragestellungen sind separate Datennutzungsanträge zu stellen.

1. dafür Sorge zu tragen, dass nach einer Systemstörung oder –ausfall, die Systeme und Daten schnellstmöglich wieder zur Verfügung stehen (Wiederherstellung der Verfügbarkeit bei Zwischenfall),

Backups werden durch Bereich 1 des UKL sichergestellt.

1. Regelmäßige Überprüfung der Maßnahmen auf Zweckerfüllung, Wirksamkeit und dem Stand der Technik (Überprüfung, Bewertung und Evaluierung der Wirksamkeit).

Regelmäßige Überprüfungen werden durch den Bereich 1 des UKL wahrgenommen

## Einbindung von Dienstleistern / Sub-Unternehmen

Nicht geplant

## automatisierte Entscheidungen im Einzelfall

Handelt es sich um ein Verfahren, welches automatisierte Entscheidungen im Einzelfall einschließlich Profiling ermöglicht? (Art. 22 EU DS-GVO) [ ]  Ja [x]  Nein

## Ist eine Übermittlung an ein Drittland außerhalb der EU oder an eine internationale Organisation vorgesehen?

|  |
| --- |
| [x]  Eine Übermittlung personenbezogener Daten an Empfänger in einem Drittland oder an eine internationale Organisation findet nicht statt und ist nicht geplant. |
| [ ]  Eine Übermittlung personenbezogener Daten an Empfänger in ein Drittland oder an eine internationale Organisation findet statt bzw. ist geplant. |
| Wohin? |       |
| Benannter Vertreter in der EU (Art. 27 EU DS- GVO) |       |
| Vereinbarte geeignete Garantien für die Rechtmäßigkeit der Übertragung  | [ ]  Anerkannter Drittstaat[ ]  EU-Standardvertrag C/C (Controller/Controller)[ ]  EU-Standardvertrag C/P (Controller/Processor)[ ]  Aufsichtsbehördlich genehmigter Vertrag[ ]  BCR Binding Corporate Rules[ ]  Andere:      |

## Datenschutz durch Technikgestaltung und Voreinstellungen

Sind bei der Verarbeitung die Grundsätze des Datenschutzes durch Technikgestaltung und der datenschutzfreundlichen Voreinstellungen eingehalten? [x]  Ja[ ]  Nein

## **Darstellung - Datenschutzorganisation im Unternehmen; Verantwortung für das Thema Datenschutz**

Die Verantwortung für den Datenschutz am UKL trägt der Vorstand. Es ist ein Datenschutzbeauftragter bestellt. Am DIZ sind Datenschutzkoordinatoren benannt.

Ab Datenübergabe liegt die Verantwortung beim Verwaltungsdirektor der Medizinische Fakultät der Universität Leipzig.

## Verpflichtungen der Beschäftigten auf den Datenschutz / Sensibilisierung / Unterweisung zum Datenschutz

Alle Beschäftigten sind auf den Datenschutz verpflichtet. Eine erste Datenschutzunterweisung am UKL erfolgt durch den DSB auf der Einführungsveranstaltung. Regelmäßige, jährliche Schulungen werde durch benannte DSKs durchgeführt.

## Allgemeine Angaben

keine

**Der obige Inhalt wurde durch den Antragsteller erstellt. Daraus entstehende Verpflichtungen werden zur Kenntnis genommen und eingehalten.**

Leipzig, den Klicken oder tippen Sie, um ein Datum einzugeben.

………………..……………………………………

(Unterschrift, Stempel)

………………..……………………………………

(Name des Unterschriftsberechtigten in Druckbuchstaben)