MEDIZINISCHE UNIVERSITÄT WIEN

Leitfaden für die Übermittlung von personenbezogenen Daten der MedUni Wien an Externe[1]

Die Daten-Clearingstelle (DC) wurde vom Rektorat eingerichtet, um ForscherInnen bei der Einhaltung der hohen datenschutzrechtlichen Standards zu unterstützen. Vor einer Übermittlung der Daten an Dritte ist zu prüfen, ob diese ausreichend pseudonymisiert oder anonymisiert sind.

Die folgenden Fragen sollten Ihnen helfen einzuschätzen, ob Sie für die Weitergabe Ihrer Daten an Externe einen Beschluss der DC benötigen. Dies betrifft sowohl personenbezogene Daten im Rahmen Ihres Forschungsprojektes, als auch eine etwaige Nachnutzung (Sekundärnutzung) der Daten nach Projektabschluss.

Bei personenbezogenen Daten handelt es sich um alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann) z.B. Daten von PatientInnen, ProbandInnen, Angehörigen, MitarbeiterInnen der MedUni Wien. Dazu zählen auch bereits pseudonymisierte Daten von Personen.

Unabhängig von der datenschutzrechtlichen Beurteilung ist zu klären, ob andere rechtliche Gründe einer Weitergabe entgegenstehen. Bitte prüfen Sie die vertragliche Situation Ihres Projektes (Auftragsforschung, akademische Studien, klinische Prüfungen, etc.) und ob Bedingungen (Nutzungsrechte, Verwertungsrecht, etc.) an die Weitergabe geknüpft sind.

Bitte beachten Sie, dass ein Votum der DC nicht die Bewertung durch die jeweils zuständige Ethik-Kommission ersetzt.

Für die datenschutzrechtliche Prüfung bitte folgende Fragen beantworten:

1. **Werden die Daten im Zuge des Projekts nur intern (dazu zählt auch der Vienna Scientific Cluster[2] unter Einhaltung der vertraglichen Vorgaben, siehe Anhang D) verarbeitet, gespeichert und NIE und in keiner Form an Externe[1] übermittelt, auch nicht nach Abschluss des Projekts?**

   falls JA: Dann besteht keine Notwendigkeit der Antragstellung an die DC. Bitte beachten Sie jedenfalls die internen Richtlinien zum Umgang mit Forschungsdaten der MedUni Wien.

   falls VSC: Es besteht keine Notwendigkeit der Antragstellung an die DC, wenn die Bedingungen aus der Nutzungsvereinbarung (Anhang D) erfüllt werden. Bitte beachten Sie jedenfalls die internen Richtlinien zum Umgang mit Forschungsdaten der MedUni Wien.

   falls NEIN: → Bitte zu Punkt 2.

[1] Das sind alle Personen oder Einrichtungen, die nicht zur Medizinischen Universität Wien gehören

[2] Die Systeme des Vienna Scientific Cluster (VSC) werden an der Technischen Universität Wien betrieben

2. Um welche Datenarten handelt es sich?

- Bei Bilddaten, Ton- oder Filmaufnahmen, Gendaten, biometrischen Daten:
  → Antrag bei der DC einbringen!
- Bei anderen Datenarten (z.B. textuelle Daten)
  → Bitte zu Punkt 3.

3. Handelt es sich beim Empfänger der Daten um wissenschaftliche Einrichtungen nach dem FOG im Inland bzw. innerhalb der EU (§ 2b Z12 bzw. gelistet in § 2c Abs 1, siehe Anhang A)?

falls JA: Dann besteht keine Notwendigkeit der Antragstellung, sofern die Daten der Vorrausetzung einer ausreichend guten Pseudonymisierung entsprechen.
→ siehe Kriterien zur Qualität der Pseudonymisierung (Anhang C)
Bitte beachten Sie, dass jedenfalls ein Vertrag abzuschließen ist, der die datenschutzrechtliche Verpflichtungen inkl. der Datensicherheitsmaßnahmen eindeutig regelt. Bei Übermittlung der Daten ist zudem eine entsprechende kryptographische Verschlüsselung vorzusehen (siehe Anhang B).

Ist keine Pseudonymisierung entsprechend Anhang C möglich:
→ Antrag bei der DC einbringen!

falls NEIN: → Bitte zu Punkt 4.

4. Wird die PatientInneninformation und Einwilligungserklärung (informed consent) der MedUni Wien Ethik-Kommission[3] für dieses Projekt verwendet?

Achten Sie bitte darauf, dass jedenfalls folgende Angaben enthalten sind:

- Bekanntgabe des/r Empfänger/s inkl. des Empfängerlandes.
- Klare konsistente Formulierung, in welcher Form die Daten weitergegeben werden (direkt personenbezogen, pseudonymisiert, anonymisiert).
- Wenn Sie biometrische oder genetische Daten weitergeben, muss dies explizit angegeben werden.
- Die verwendeten Begriffe (Pseudonymisierung, Anonymisierung, biometrische Daten, genetische Daten) müssen definiert sein.
- Bei Weitergabe der Daten in Länder außerhalb der EU bzw. EWR, muss ein entsprechender Hinweis angegeben sein, dass unter Umständen nicht das gleiche Datenschutzniveau wie innerhalb der EU bzw. EWR vorliegt.

falls JA: Dann besteht keine Notwendigkeit der Antragstellung, sofern die Daten der Vorrausetzung einer ausreichend guten Pseudonymisierung entsprechen.
→ siehe Kriterien zur Qualität der Pseudonymisierung (Anhang C)
Bitte beachten Sie, dass jedenfalls ein Vertrag abzuschließen ist, der die datenschutzrechtliche Verpflichtungen inkl. der Datensicherheitsmaßnahmen eindeutig regelt. Bei Übermittlung der Daten ist zudem eine entsprechende kryptographische Verschlüsselung vorzusehen (siehe Anhang B).

falls NEIN: → Antrag bei der DC einbringen!

[3] http://ethikkommission.meduniwien.ac.at/service/patienteninformation/

Anhang A: wissenschaftliche Einrichtung nach dem FOG

Definition wissenschaftliche Einrichtung (FOG § 2b Z 12): „wissenschaftliche Einrichtungen“: natürliche Personen, Personengemeinschaften sowie juristische Personen, die Zwecke gemäß Art. 89 Abs. 1 DSGVO verfolgen, d.h. insbesondere Tätigkeiten der Forschung und experimentellen Entwicklung (Z 10) vornehmen, ungeachtet dessen, ob dies

a) zu gemeinnützigen Zwecken (§§ 34 ff der Bundesabgabenordnung, BGBl. Nr. 194/1961) oder nicht oder
b) im universitären, betrieblichen oder außeruniversitären Rahmen

erfolgt.

Die folgenden wissenschaftlichen Einrichtungen sind im FOG genannt:

1. Bundesmuseen nach dem Bundesmuseen-Gesetz 2002, BGBl. I Nr. 14/2002,
2. Fachhochschulen nach dem Fachhochschul-Studiengesetz,
3. die Geologische Bundesanstalt (GBA) gemäß § 18,
4. das Institute of Science and Technology – Austria gemäß § 1 ISTAG,
5. natürliche Personen, Personengemeinschaften sowie juristische Personen, die Art-89-Mittel
   a) seitens des Wissenschaftsfonds (§ 2 FTFG) oder
   b) im Rahmen europäischer Rahmenprogramme für Forschung und Entwicklung erhalten haben, für die vereinbarte Dauer, mindestens jedoch fünf Jahre ab Zuerkennung der Art-89-Mittel,
6. die Österreichische Akademie der Wissenschaften,
7. die Österreichische Bibliothekenverbund und Service Gesellschaft mit beschränkter Haftung (§ 1 des Bundesgesetzes über die Österreichische Bibliothekenverbund und Service Gesellschaft mit beschränkter Haftung, BGBl. I Nr. 15/2002),
8. als Partner von der Österreichischen Forschungsförderungsgesellschaft mbH (§ 1 Abs. 1 FFGG) für die Einlösung des Innovationsschecks ausgewiesene Einrichtungen,
9. als Partner in der Forschungsinfrastrukturdatenbank des Bundesministeriums für Bildung, Wissenschaft und Forschung ausgewiesene Forschungseinrichtungen und Unternehmen, die ihre Forschungsinfrastruktur öffentlich anbieten,
10. Privatuniversitäten nach dem Privatuniversitätengesetz,
11. gemäß § 4a Abs. 3 oder Abs. 4 lit. a oder b des Einkommensteuergesetzes 1988, BGBl. Nr. 400/1988, spendenbegünstigte Einrichtungen,
12. die Universität für Weiterbildung Krems gemäß § 1 UWKG,
13. Universitäten nach dem Universitätsgesetz 2002,
14. wissenschaftliche Bibliotheken sowie
15. die Zentralanstalt für Meteorologie und Geodynamik (ZAMG) gemäß § 22.

Anhang B: Kryptographische Verschlüsselung

Bei elektronischer Übermittlung von Gesundheitsdaten (besondere Kategorien von Daten, Art. 9 DSGVO) ist nach § 6 GTelG 2012 die Vertraulichkeit der Daten durch kryptografische Verschlüsselung sicherzustellen. Für die Verschlüsselung muss ein sicheres, kryptografisches Verfahren gewählt werden, beispielsweise „Advanced Encryption Standard“ mit der Schlüssellänge von mindestens 256 Bit (AES-256). Diese Verschlüsselung ist z.B. in den Programmen 7-ZIP (https://www.7-zip.org/) oder Cryptomator (https://cryptomator.org/) verfügbar.

Für die Verschlüsselung wird zudem ein Passwort benötigt, das dem Empfänger auf einem anderen, technischen Kommunikationskanal wie die Daten zu übermitteln ist (z.B. verschlüsselte Daten per Mail -> Passwort per SMS oder Telefon, nicht aber per Mail).

Anhang C: Kriterien zur Qualität der Pseudonymisierung

Definition Pseudonymisierung (Art 4 Z 5 DSGVO): „Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Zu beachten ist, dass eine Person als identifizierbar angesehen wird, wenn sich diese direkt oder indirekt mittels Zuordnung zu einem Merkmal identifizieren lässt.

Daher dürfen folgende textuelle Daten von betroffenen Personen[4] jedenfalls NICHT enthalten sein:

- Namensangaben (auch Initialen)
- Geburtsdatum (Alter oder Geburtsjahr ist zulässig)
- Adressdaten
- Kontaktdaten (E-Mail, Telefonnummer,etc.)
- Beruf
- Daten, die eine unmittelbare Identifikation der Person ermöglichen
  Beispiele: SVNR, Patienten-ID, LIC, MAC, Fallnummer, Aufnahmezahl, Study Instance UID etc.
- Selektive Datumsangaben wie Aufnahme- bzw. Entlassungsdatum, Ambulanzbesuche, Datumsangaben zu spezifischen Interventionen oder Ereignisse (z.B. Operationsdatum) etc.
- Seltene, selektive medizinische Daten
- Freitexte z.B. Patientenbrief, Befundtext, Dekurse

Hinweise: Wesentlich ist, dass aus der Kombination textueller Daten keine Re-Identifikation einer betroffenen Person möglich ist. Aus diesem Grund empfiehlt die DC bei der Pseudonymisierung textueller Daten IDs zu verwenden, die keine Rückschlüsse auf die betroffene Person zulassen.

Auch bei bereits pseudonymisierten Daten kann, je nach Fallkonstellation, auf eine konkrete Person rückgeschlossen werden, wenn die Bezugsgruppe nicht groß genug ist. Daher ist bei Auswertungen darauf zu achten, dass die Merkmale bei mindestens 5 Personen identisch sind.

Das Datenschutzrecht betrifft nur den Zeitraum von Geburt bis Tod. Mit dem Tod erlischt das Recht auf Datenschutz. Die Daten bereits verstorbener Personen können daher ohne datenschutzrechliche Vorgaben verarbeitet werden[5].

Wenn Sie Unterstützung bei der Einhaltung der datenschutzrechtlichen Anforderungen im Zuge der Datenweitergabe an Externe benötigen, zögern Sie bitte nicht Kontakt mit uns aufzunehmen: datenclearing@meduniwien.ac.at

[4] PatientInnen, ProbandInnen, Angehörige, MitarbeiterInnen etc.

[5] Postmortaler Schutz kann jedoch aufgrund von anderen Gesetzen bestehen (Bildnisschutz und andere Urheberrechte sowie Persönlichkeitsrechte).

Anhang D: Auszug aus der Vereinbarung über die Nutzung des Vienna Scientific Cluster (VSC) zur Speicherung und Verarbeitung personenbezogener Daten

Die Verarbeitung von personenbezogenen Daten im Rahmen von Projekten auf Systemen des VSC, der an der Technischen Universität Wien (TU Wien) betrieben wird, müssen der Daten-Clearingstelle nicht vorgelegt werden, wenn die Vereinbarung über die Nutzung des Vienna Scientific Cluster zur Speicherung und Verarbeitung personenbezogener Daten erfüllt wird.

Folgende Bedingungen sind laut Vereinbarung einzuhalten (Auszug):

- Die Eingabe von personenbezogenen Daten erfolgt ausschließlich durch MitarbeiterInnen der MedUni Wien. MitarbeiterInnen des jeweiligen Projekts der MedUni Wien erhalten Zugang zum VSC.
- Projekte, bei denen personenbezogene Daten verwendet werden, werden von der MedUni Wien entsprechend gekennzeichnet.
  - Das Speichern personenbezogener Daten im Speicherplatz anderer Projekte ist nicht gestattet.
  - Der eigene Speicherplatz darf nicht für MitarbeiterInnen anderer Projekte freigegeben oder geteilt werden.
- Vor Übertragung zum VSC müssen die ProjektleiterInnen sicherstellen, dass die Daten anonymisiert oder pseudonymisiert sind. Im Falle der Pseudonymisierung darf der Schlüssel zur Aufhebung der Pseudonymisierung zu keiner Zeit am VSC gespeichert sein.
- Die TU Wien und alle mit der Administration der Systeme des VSC betrauten Personen sind zur Geheimhaltung verpflichtet.
- Die Verarbeitungen von Verwaltungsdaten und und öffentliche Daten auf der VSC-Webseite sind im Verzeichnis der Verarbeitungen der TU Wien eingetragen und unterliegen den Regelungen der TU Wien.
- Nach Projektabschluss sind folgende nicht mehr benötigten Daten umgehend zu löschen:
  - Arbeitsdaten. Für die Löschung ist der/die Projektleiter/in verantwortlich.
  - Personenbezogene Verwaltungsdaten. Die Löschung wird von der TU Wien durchgeführt. Eine Ausnahmen bildet eine gesetzlichen Verpflichtung diese Daten auch nach Vertragsende zu verarbeiten. Nicht betroffen sind der Benutzername und die eindeutige Nummer des Benutzers, welche systembedingt nicht neu vergeben werden.
- Die TU Wien erstellt keine Logfiles welche den Output von Berechnungen enthalten. Der vom VSC geloggte „Jobname“ und der Pfad des Jobscripts dürfen diese keine personenbezogenen Daten enthalten.
- Besondere technische Maßnahmen (sofern erforderlich, z.B. der Verzicht auf Backups), sind vom Projektleiter mit dem VSC-Team im Vorhinein abklaren.