

Datenschutzvorgaben in der Forschung

Februar 2022

Markus Lemke

Informationssicherheits- und Datenschutzbeauftragter

HafenCity Universität Hamburg

Inhalt

1.	Einleitung	3
2.	Datenschutzvorgaben planen	3
3.	Datenschutzvorgaben während des Projekts umsetzen.....	3
4.	Sonderfälle in der Forschung, die einer gesonderten Klärung bedürfen.....	4

1. Einleitung

Auch in der Forschung ist die Einhaltung datenschutzrechtlicher Vorgaben ein wichtiger Bestandteil der wissenschaftlichen Arbeit. Das Dokument soll dabei helfen eine datenschutzkonforme Verarbeitung der Daten zu gewährleisten.

2. Datenschutzvorgaben planen

Werden personenbezogene Daten verarbeitet und wenn ja, welche Art personenbezogener Daten werden für das Verfahren verarbeitet?

Es muss eine Risikoanalyse / der Schutzbedarf der Daten definiert und dokumentiert werden.

Bei Forschungsoperationen muss eine gemeinsame Verantwortlichkeit geprüft werden.

Es ist zu prüfen, ob Auftragsverarbeitungsverträge mit Dienstleistern (wie z.B. Transkriptionsbüros und SAAS-Anbietern) geschlossen werden müssen.

Für die Daten muss ein Speicher- und Zugriffskonzept mit den entsprechenden technischen und organisatorischen Maßnahmen entwickelt werden.

Entwicklung von Pseudonymisierungs-, Anonymisierungs- und Löschkonzepten mit Datum

Einwilligungen für alle Teilnehmenden, bei / von denen Daten erhoben werden. Zu welchen Zweck(en) werden die Daten erhoben und verarbeitet. Wenn Daten über Dritte in einem Fragebogen erhoben werden, müssen diese ebenfalls einwilligen, wenn dies zumutbar ist. Beispiel: Forschung mit Schüler:innen und Eltern, Lehrer:innen.

Erstellung des Verzeichnisses von Verarbeitungstätigkeiten (VVT) nach Art. 30 DSGVO durch die verantwortliche Stelle. Das VVT ist das zentrale Datenschutzdokument, in dem die Verarbeitung der Daten transparent und mit den Rechtsgrundlagen dargelegt wird.

Frühzeitige Einbindung des Datenschutzbeauftragten bei Projektbeginn.

3. Datenschutzvorgaben während des Projekts umsetzen

Sichere Aufbewahrung der Einwilligungen, Pseudonymisierungslisten, Dokumentationen, Risikoabwägungen müssen berücksichtigt werden.

Aufbewahrung / Speicherung der Daten / Zugriff auf Forschungsdaten einschränken und organisieren

Pseudonymisierung / Anonymisierung der Daten gemäß der Einwilligung sicherstellen, prüfen und dokumentieren.

Regelmäßige Prüfung der Umsetzung von Datenschutzvorgaben bei gemeinsamer Verantwortlichkeit oder Auftragsverarbeitung sowie der gewählten technischen und organisatorischen Maßnahmen.

Regelmäßige Aktualisierung der Dokumentation von Verarbeitungsvorgängen im Verzeichnis von Verarbeitungstätigkeiten.

Löschung von personenbezogenen Daten gemäß Einwilligungen berücksichtigen

Ggf. Archivierung der anonymisierten Forschungsdaten

4. Sonderfälle in der Forschung, die einer gesonderten Klärung bedürfen

Besteht eine gemeinsame Verantwortlichkeit zwischen Universitäten, muss dies vertraglich über einen Kooperationsvertrag geregelt werden.

Werden besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO verarbeitet, muss eine Prüfung für die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erfolgen.

Besondere Kategorien personenbezogener Daten sind:

Rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO muss gemeinsam mit dem IT-Betrieb, der projektführenden Stelle und dem Informationssicherheits- bzw. Datenschutzbeauftragten durchgeführt werden, um das hohe Risiko der Betroffenen in Bezug auf ihre Persönlichkeitsrechte durch technische und organisatorische Maßnahmen zu minimieren.

Erfolgen Datenübermittlung an ein Drittland? Liegt ein Angemessenheitsbeschluss vor? Die Europäische Union erkennt in einer Reihe von Ländern die Datenschutzbestimmungen als hinreichend an. Hinweis: Wenn personenbezogene Daten an ein Land außerhalb der EU gesendet werden sollen (Server im Ausland), muss sichergestellt sein, dass dieses Land die gleichen Sicherheitsstandards bezüglich des Datenschutzes anlegt. Mit einzelnen Staaten hat die EU entsprechende Abkommen (z.B. Schweiz, Japan). Sollte kein Abkommen vorliegen, ist zu prüfen, ob eine Übersendung erlaubt ist.

Verhältnismäßigkeit im Zusammenhang mit Archivierungsempfehlungen für Forschungsdaten (10 Jahre) prüfen.