**Muster: Datenschutzkonzept für Forschungsvorhaben
(auch im Rahmen von akademischen Abschlussarbeiten oder Promotionsvorhaben)**

(basierend auf einer Vorlage des Hessischen Beauftragte für Datenschutz und Informationsfreiheit – Stand 0.1 - 7.3.2022)

1. **Beschreibung des Forschungsvorhabens**
* Darstellung Forschungsfrage/ Beschreibung des Forschungsvorhabens

Durch eine Begrenzung des Forschungsvorhabens auf bestimmte Bereiche (Patientengruppen, Krankheitsbilder) und Daten können Eingriffe in die Rechte der Betroffenen möglichst geringgehalten werden. Dadurch kann z. B. die Interessenabwägung im Kontext des § 17 DSG NRW (vgl. VI. 2. unten) eher zugunsten der Forschenden ausfallen.

* Studiendesign

An dieser Stelle ist darzulegen, auf welche Weise die Daten gewonnen werden sollen (Befragung, Auswertung vorhandener Daten etc.). Entscheidend ist, ob mit anonymen Daten gearbeitet wird, oder ob auf Daten mit oder ohne Einwilligung zurückgegriffen werden soll (im letzteren Fall eröffnet dies den unter VI. dargestellten Anwendungsbereich).

* (IT-) Infrastruktur
* Geplante Laufzeit und mögliche Anschlussforschung (Weitergabe personenbezogener Daten an andere Forschungsvorhaben)
1. **Organisatorische Rahmenbedingungen**
* Verantwortlichkeiten: Wer ist datenschutzrechtlich verantwortlich nach Art. 4 Nr. 7 DS-GVO?

Verantwortlich im Sinn des Art. 4 Nr. 7 DS-GVO dürfte in der Regel die Person sein, die die Forschungsarbeit erstellt. Bei der Einbindung in Forschungsprojekte kann dies aber auch die Person sein, die das Projekt leitet.

* Gemeinsame Verantwortlichkeiten oder Auftragsverarbeitungsverhältnisse identifizieren
* Andere Beteiligte (Sponsoren, Kooperationspartner)
* Internationale Bezüge (Übermittlung von Daten ins Ausland)
* Einbeziehung Ethikkommission
1. **Beschreibung der Datenverarbeitungen**
	1. **Betroffene Personen**
* Patienten, Probanden, Minderjährige, Beschäftigte, Kunden etc.
	1. **Kategorien von Daten**
* Adressdaten, Gesundheitsdaten, Bioproben etc.

Die benötigten Datensätze sind im Vorfeld klar zu benennen. Diese haben sich am Grundsatz der Erforderlichkeit und der Datensparsamkeit zu orientieren. Die zu bestimmenden Datensätze dürfen aber natürlich all das umfassen, was zum Erreichen des Forschungszieles als erforderlich angesehen wird.

* 1. **Erhebung der Daten**
* Beschreibung der beabsichtigen (elektronischen) Datenerhebung
* Woher kommen die Daten, von wem werden sie bereitgestellt (interne Datenbank oder Übermittlung von externen Stellen)?

Bei einer Direkterhebung der Daten bei den betroffenen Personen (Fragebögen etc.) ist deren Einwilligung abzufragen, die dann als Rechtsgrundlage der Verarbeitung dienen kann.

Die Nutzung der Daten auf Basis des § 17 Abs. 1. DSG NRW erfolgt daher vorwiegend bei retrospektiven Forschungsvorhaben mit bereits vorhandenen Daten.

* Automatisierter Abruf oder bestimmte Verfahren zur Übertragung der Daten
	1. **Zweckbestimmung und Zweckbindung**
* Klare Definition der Zwecke der Verarbeitung der jeweiligen Daten im Forschungsvorhaben
1. **Garantien für die Rechte und Freiheiten der betroffenen Person**
	1. **Schutzbedarf und Risikoanalyse**
* Welche Risiken sind für die betroffenen Personen mit der Verarbeitung verbunden?
* Risikobewertung auf Basis von Schadenshöhe und Eintrittswahrscheinlichkeit
* Definierung einer Schutzbedarfskategorie[[1]](#footnote-1) (normal, hoch)
	1. **Pseudonymisierung**
* Prüfung der Pseudonymisierung aller Daten

Pseudonymisierung bedeutet, dass personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können (Art 4 Nr. 5 DS-GVO). Die zusätzlichen Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Die personenbezogenen Daten sind frühestmöglich zu pseudonymisieren.

* Beschreibung Pseudonymisierungsverfahren

Sobald der Forschungs- oder Statistikzweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungs- oder Statistikzweck dies zulässt (siehe auch § 17 Abs. 2 DSG NRW)

* Ggfs. Festlegung der Bedingungen für eine Re-Identifikation
	1. **Anonymisierung**
* Prüfung frühestmöglicher Anonymisierung

Gemäß § 17 Abs. 3 DSG NRW sind personenbezogener Daten zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen.

* Beschreibung des Anonymisierungsverfahrens
	1. **Aufbewahrung und Speicherdauer**
* Wo werden die Daten gespeichert?
* Darstellung des Lebenszyklus der Daten (ggfs. Flussdiagramm)
* Definierung der Speicherdauer mit Begründung der Erforderlichkeit (s. auch Anonymisierung)
* Darstellung von Regellöschpflicht und ggfs. Löschkonzept (Einschränkung der Löschpflicht nach Art. 17 Absatz 3 lit. d DS-GVO; siehe Ziffer VII.2)
1. **Technische und organisatorische Maßnahmen**
* Die im Einzelnen zu treffenden technischen und organisatorischen Maßnahmen müssen individuell ermittelt werden
* Berücksichtigung der gesetzlichen Regelbeispiele:

Der Verantwortliche sieht nach § 17 DSG NRW angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vor. Dazu gehören insbesondere:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung nach der Verordnung (EU) Nr. 2016/679 erfolgt,

2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,

3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

4. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,

(5. Pseudonymisierung personenbezogener Daten, (s.o.))

6. Verschlüsselung personenbezogener Daten,

7. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

8. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder

9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) Nr. 2016/679 sicherstellen.

* Ggfs. Rückgriff auf technische und organisatorische Maßnahmen der Hochschule
* Möglichkeit der Datentreuhänderschaft evaluieren
1. **Optional: Nachnutzung von Daten**
* Welche Nachnutzung von Daten ist geplant?
* Ist Anonymisierung/Pseudonymisierung dabei umgesetzt?
* Welche Hürden werden aufgebaut? (Antragsverfahren)
1. **Optional: Prüfung § 17 DSG NRW**

**(Nur wenn (personenbezogene Verarbeitung ohne Einwilligung erfolgt: z.B. Daten aus Datenbeständen)**

* 1. **Erforderlichkeit**

Wenn die Datenverarbeitung nicht auf die Einwilligung der betroffenen Personen gestützt wird, sind folgende Aspekte festzuhalten

* Darlegung der Erforderlichkeit der konkreten Datenverarbeitungen für die Zwecke der wissenschaftlichen Forschung

Die Verarbeitung ohne Einwilligung ist nicht erforderlich, wenn die Forschungsziele auch unter Nutzung anonymer oder anonymisierter Daten erreicht werden können oder mittels einer Einwilligung der Betroffenen.

* Warum ist das Forschungsvorhaben nur mit den gegenständlichen personen- bezogenen Daten realisierbar?
	1. **Interessenabwägung**
* Interessen der Forschenden an der Datenverarbeitung müssen die Interessen der betroffenen Personen an einem Ausschluss der Verarbeitung überwiegen
* Die Interessen sind gegenüberzustellen und zu vergleichen

Ein Überwiegen der Interessen des Forschenden liegt regelmäßig dann vor, wenn die Grundsätze der Erforderlichkeit, Zweckbindung und Verhältnismäßigkeit beachtet werden.

Bei der Prüfung der Verhältnismäßigkeit ist im Rahmen der „praktischen Konkordanz“ danach zu fragen, ob der Eingriff in die Rechte der betroffenen Personen infolge einer datenschutzgerechten Ausgestaltung des Forschungsvorhabens so gering wie möglich gehalten wird und nicht außer Verhältnis zu dem angestrebten Zweck steht.

* Berücksichtigung der „vernünftige Erwartungen“ der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen
1. **Betroffenenrechte und Datenschutzmanagement**
	1. **Kurzdarstellung der Prozesse und Bezeichnung eines Ansprechpartners für die Erfüllung folgender Betroffenenrechte:**
* Art. 13, 14 DS-GVO Informationspflichten
* Art. 15 DS-GVO Recht auf Auskunft
* Art. 16 DS-GVO Recht auf Berichtigung
* Art. 17 DS-GVO Recht auf Löschung incl. Art 7 – Widerruf einer Einwilligung
* Art. 18 DS-GVO Recht auf Einschränkung der Verarbeitung
* (Art. 21 DS-GVO Recht auf Widerspruch) – nur bei Verarbeitung ohne Einwilligung.
	1. **Dokumentation und Begründung bei Beschränkungen von Betroffenenrechte**
* Beschränkung der Informationspflicht nach Art. 14 DS-GVO?

Die Informationspflichten nach Art. 14 DS-GVO finden keine Anwendung, wenn und soweit die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für wissenschaftliche oder historische Forschungszwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien (Art. 14 Absatz 5 lit. b DS-GVO)

* Beschränkung der Rechte nach Art. 15, 16, 18 und 21 DS-GVO

Diese Rechte sind insoweit beschränkt, als diese voraussichtlich die Verwirklichung der Forschungszwecke unmöglich machen oder ernsthaft beeinträchtigen (§ 17 Absatz 5 DSG NRW).

Die Beschränkung muss für die Erfüllung der Forschungszwecke „notwendig“ sein und ist als Ausnahmefall ausgestaltet.

* Recht auf Löschung Art. 17 DS-GVO

Das Recht auf Löschung besteht nach Art. 17 Absatz 3 lit. d DS-GVO nicht, wenn die Datenverarbeitung für wissenschaftliche Forschungszwecke erforderlich ist und die Löschung Recht die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt.

* 1. **Darstellung der Prozesse und Bezeichnung verantwortlicher Personen / Stellen für**
* Meldung Datenpannen nach Art. 33 DS-GVO
* Verarbeitungsverzeichnis
* ggfs. Datenschutz-Folgenabschätzung
* Wurde mit Auftragsverarbeitern Vertrag mit dem Risiko angemessenen Maßnahmen abgeschlossen?
	+ z.B. für Umfragetool (nicht, wenn es durch die Hochschule betrieben wird), Transkription bei einem Transkriptionsbüro, Speicher(-cloud) zum Datentransfer etc.
* Soweit Datenübermittlungen in Länder außerhalb der Europäischen Union stattfinden, werden die Daten angemessen geschützt?
1. Standard-Datenschutzmodell der DSK

https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/20200417\_DSK\_SDM-Handbuch\_V20b.pdf [↑](#footnote-ref-1)