

9 Technisch-organisatorische Vorkehrungen

Das Datenschutzrecht sieht eine Vielzahl von **Vorkehrungen** vor, die im Rahmen von Forschungsprojekten zum Einsatz kommen können. Nur bei einem am Risiko der Verarbeitung orientierten Einsatz der genannten Maßnahmen kann die datenschutzrechtliche Privilegierung für Forschungszwecke zur Anwendung kommen (Art. 89 Abs. 1 DSGVO, vgl. § 27 Abs. 1 S. 3 BDSG). Normativ genannt werden folgende Maßnahmen:⁵⁸⁰

- Datenverschlüsselung (Art. 32 Abs. 1 lit. a DSGVO, § 22 Abs. 2 Nr. 6 BDSG),
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitung sicherzustellen (Art. 32 Abs. 1 lit. b DSGVO, § 22 Abs. 2 Nr. 8 BDSG),
- Fähigkeit, die Verfügbarkeit und den Zugang zu Daten herzustellen (Art. 32 Abs. 1 lit. c DSGVO, § 22 Abs. 2 Nr. 8 BDSG),
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technisch-organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO, § 22 Abs. 2 Nr. 9 BDSG),
- Protokollierung (§ 22 Abs. 2 Nr. 2 BDSG),
- Sensibilisierung der an der Verarbeitung Beteiligten (§ 22 Abs. 2 Nr. 3 BDSG),

⁵⁸⁰ Roßnagel ZD 2019, 161; Dierks 2020, 8f.; kritisch zum Verweis auf § 22 Abs. 1 in § 27 Abs. 1 S. 2 BDSG wegen des fehlenden Bezugs zur Forschung Golla in Specht/Mantz, § 23 Rn. 32.

Benennung bzw. Einbeziehung eines Datenschutzbeauftragten (§ 22 Abs. 2 Nr. 4 BDSG)⁵⁸¹,

- Zugangsbeschränkungen (§ 22 Abs. 2 Nr. 5 BDSG),

spezifische Verfahrensregelungen bei Übermittlung oder Zweckänderung (§ 22 Abs. 2 Nr. 10 BDSG)⁵⁸²,

- Genehmigungsvorbehalte (§ 75 Abs. 4, 4a SGB X),
- Anzeigepflichten (§ 80 Abs. 1 SGB X),

Einbeziehung einer Ethikkommission (§ 15 MBOÄ),⁵⁸³

- weitere technisch-organisatorische Maßnahmen zur Wahrung der Datenschutzkonformität (§ 22 Abs. 2 Nr. 1 BDSG).

Hinsichtlich dieser Anforderungen besteht durch die Aufsichtsbehörden, deren Zusammenschlüsse und insbesondere den Europäischen Datenschutzausschuss die Möglichkeit der Konkretisierung.⁵⁸⁴ Insbesondere **bei einer wenig bestimmten Zweckbindung** von für Forschungszwecke verarbeiteten Daten verlangt die Konferenz der deutschen Datenschutzaufsichtsbehörden kompensatorische Maßnahmen im Interesse von Transparenz (A.), Vertrauensbildung (B.) und Datensicherheit (C.):⁵⁸⁵

A. Transparenz

- „Verwendung einer für den Einwilligenden zugänglichen Nutzungsordnung oder eines einsehbaren Forschungsplanes, der die geplanten Arbeitsmethoden und die Fragen, die Gegenstand der Forschung sein sollen, beleuchtet
- Ausarbeitung und Dokumentation im Hinblick auf das konkrete Forschungsprojekt, wieso in diesem Fall eine nähere Konkretisierung der Forschungszwecke nicht möglich ist
- Einrichten einer Internetpräsenz, durch die die Studienteilnehmer über laufende und künftige Studien informiert werden“

B. Vertrauensbildung

- „Positives Votum eines Ethikgremiums vor der Nutzung für weitere Forschungszwecke
- Prüfung, ob das Arbeiten mit einem dynamic consent möglich ist, bzw. Einräumung einer Widerspruchsmöglichkeit vor der Verwendung der Daten für neue Forschungsfragen“

C. Datensicherheit

- „Keine Datenweitergabe in Drittländer mit geringerem Datenschutzniveau
- Gesonderte Zusagen zur Datenminimierung, Verschlüsselung, Anonymisierung oder Pseudonymisierung
- Spezifische Vorschriften für die Begrenzung des Zugriffs auf die erhobenen Daten“

581 Roßnagel ZD 2019, 162.

582 Nachweise zum Landesrecht bei Bernhardt/Ruhmann/Weichert, 8.

583 Zur Geschichte ethischer Standards, zu „informed consent“ und Kontrolle EDPS 2020, 13.

584 Martini/Hohmann NJW 2020, 3577.

585 DSK, Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ in Erwägungsgrund 33 der DS-GVO v. 03.04.2019; ähnlich zu Rahmenbedingungen des Broad Consent TME, 98ff.

Bei der Verarbeitung von Sozialdaten gilt § 22 BDSG entsprechend (§ 67b Abs. 1 S. 4 SGB X). Bei den genannten Maßnahmen fällt auf, dass diese zumeist nicht nur im Forschungsbereich bzw. bei sensitiven Daten, sondern generell zur Pflicht gemacht werden.⁵⁸⁶ Die spezifische Erwähnung verpflichtet zu einer **erhöhten Prüftiefe** und zu spezifischen, dem Risiko angemessenen Maßnahmen.

Die Feststellung, welche der genannten Maßnahmen zu ergreifen sind, erfolgt unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen (**Risikoorientierung** – vgl. § 22 Abs. 2 S. 2 i.V.m. § 27 Abs. 1 S. 2 BDSG).⁵⁸⁷ Die Art und der Umfang der Garantien hängen also im Forschungsbereich vom jeweiligen Projekt und den damit verbundenen Risiken ab.⁵⁸⁸

Aus dem oben Ausgeführten kann abgeleitet werden, dass bei jedem privilegierten Forschungsprojekt, bei dem in erheblichem Umfang mit personenbezogenen Daten gearbeitet wird, ein **Datenschutzkonzept** erstellt werden muss, in dem die angemessenen Garantiemaßnahmen aufgeführt werden (ausdrücklich z.B. § 24 Abs. 1 S. 2 HDSIG).⁵⁸⁹ Diese Pflicht ergibt sich zudem indirekt aus der nach Art. 35 Abs. 3 lit. b DSGVO bestehenden Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (s.u. Kap. 11.4).⁵⁹⁰

586 Johannes/Richter, DuD 2017, 302f.

587 Zum risikobasierten Ansatz Schröder ZD 2019, 503ff.

588 Johannes/Richter, DuD 2017, 302.

589 Roßnagel ZD 2019, 161.

590 DWWS-Wedde, § 22 Rn. 21; Roßnagel ZD 2019, 163.