Checkliste für die Datenschutz- und Datensicherheitsstandards bei Anträgen auf Datenzugang nach Art. 40 Abs. 4 DSA

Ihr Forschungsvorhaben zu systemischen Risiken auf sehr großen Online-Plattformen erfordert die Analyse von Daten, die durch die Nutzung dieser Dienste entstehen. Bei diesen Daten kann es sich um personenbezogene Daten handeln, da sie direkte oder indirekte Rückschlüsse auf die Nutzerinnen und Nutzer zulassen – sei es durch deren Interaktionen, Profile oder veröffentlichte Inhalte. Werden nur anonymisierte Daten verlangt und verarbeitet, müssen Angaben zum Datenschutz nicht gemacht werden.

Hinweis: Personenbezogene Daten und Anonymisierung

> Die DS-GVO stellt hohe Hürden an die fehlende Möglichkeit der Herstellung eines Personenbezuges mit technischen Mitteln. Die unzutreffende Annahme einer Anonymisierung kann daher das weitere Verfahren in relevanter Weise verzögern. Pauschale Aussagen, ob im konkreten Fall von einer Anonymisierung oder Pseudonymisierung auszugehen ist, sind nicht möglich. Es handelt sich um eine Einzelfallfrage. Da soziale Medien mittlerweile alle Belange des menschlichen Zusammenlebens betreffen und sich Angebote für jedes Interessengebiet, Geschlecht, jede Religion, soziale Gruppe, sexuelle Orientierung etc. finden, dürften die Daten regelmäßig Rückschlüsse auf betroffene Personen zulassen und damit häufig nicht als anonymisiert gelten können.

Sofern Ihr Forschungsvorhaben den Zugang (auch) zu personenbezogenen Daten umfasst, müssen Sie nachweisen, dass Sie in der Lage sind, die besonderen Anforderungen an die Datensicherheit und die Vertraulichkeit einzuhalten und personenbezogene Daten zu schützen. In Ihrem Antrag sind die angemessenen technischen und organisatorischen Maßnahmen zu beschreiben, die Sie hierzu getroffen haben (Artikel 40 Absatz 8 lit. d DSA). Die zuständige Datenschutzaufsichtsbehörde wird anhand Ihrer Angaben die datenschutzrechtlichen Aspekte Ihres Forschungsvorhabens prüfen, insbesondere die Zwecke, die Verhältnismäßigkeit der Datenverarbeitung sowie die von Ihnen getroffenen technischen und organisatorischen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten.

Diese Checkliste nebst Erläuterungen soll als Hilfestellung für die Gewährleistung der Einhaltung der datenschutzrechtlich zu beachtenden Anforderungen dienen. Um Ihnen die Beantwortung dieser Fragen zu erleichtern, finden Sie bei datenschutzrechtlichen Fachbegriffen Verweise auf ein angehängtes Glossar (**G**). Darin wird auf weitere Materialien verwiesen, die diese Begrifflichkeiten aufschlüsseln.

1. Angaben zur Forschungseinrichtung bzw. einer vertretungs- und empfangsberechtigten Person für Rückfragen zum Datenschutz

Zu nennen sind neben Name, Anschrift und Kontakt der Forschungseinrichtung deren Vertretungspersonen (z.B. Geschäftsführer/Geschäftsführerin(nen)) sowie die Namen der beteiligten Forscher und Forscherinnen (samt Funktion und Kontakt), insbesondere Projektleitung und Ansprechperson für Rückfragen zum Datenschutz. Wenn Sie hierzu keine gesonderten Angaben machen, wird der principle researcher als Ansprechperson für Rückfragen zum Datenschutz angesehen.

2. Gegebenenfalls: Angaben zu den weiteren beteiligten Forschungseinrichtungen

Sofern weitere Forschungseinrichtungen bzw. Forschende an der Verarbeitung beteiligt sind, sind Angaben zu den beteiligten Einrichtungen und Forschenden (samt Funktion und Kontakt), sowie zu vertretungs- und empfangsberechtigten Personen für Rückfragen zum Datenschutz beizufügen. Wenn Sie hierzu keine gesonderten Angaben machen, werden

weitere Forschende anderer Forschungseinrichtungen als Ansprechperson für Rückfragen zum Datenschutz angesehen.

Wenn die beteiligten Forschenden und Forschungseinrichtungen gemeinsam personenbezogene Daten verarbeiten, kann eine gemeinsame Verantwortlichkeit vorliegen. In diesem Falle ist dem Antrag eine Erläuterung beizufügen, aus der sich ergibt, dass und wie die vom Antrag umfassten Daten durch die Forschungseinrichtungen verarbeitet werden und welche Einrichtung welchen Beitrag leistet bzw. welche Rolle die einzelnen Einrichtungen einnehmen. Erforderlich ist insoweit der Abschluss einer Vereinbarung gemäß Artikel 26 der Verordnung (EU) 2016/679 (DS-GVO), die dann beigelegt wird. **[G1]**

Wenn Daten nicht gemeinsam mit Dritten, sondern im Auftrag der Forschungseinrichtung durch Dritte verarbeitet werden, kann eine Auftragsverarbeitung vorliegen. In diesem Falle sind Angaben zum geschlossenen Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO beizufügen. **[G2]**

Diese Angaben können Sie in das Textfeld zu den Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten eintragen und ergänzende Dokumente im dafür vorgesehenen Upload-Feld hochladen.

3. Angaben zu den mit der Verarbeitung der personenbezogenen Daten jeweils verfolgten Zwecken

Grundsätzlich ist dem Antrag eine Auflistung und Erläuterung der konkreten Zwecke im Sinne des Art. 40 Abs. 4 EU VO 2022/2065 beizufügen (d.h. Forschungsarbeiten, die zur Aufspürung, zur Ermittlung und zum Verständnis systemischer Risiken in der Union gemäß Artikel 34 Abs. 1 beitragen, auch in Bezug auf die Bewertung der Angemessenheit, der Wirksamkeit und der Auswirkungen der Risikominderungsmaßnahmen gemäß Art. 35 DSA). Bitte beschreiben Sie in diesem Textfeld ausdrücklich auch die Zwecke der Verarbeitung der personenbezogenen Daten. Über das im Antrag vorgesehene Kontrollkästchen ist zu bestätigen, dass keine weiteren Zwecke mit der Verarbeitung der antragsgegenständlichen Daten verfolgt werden.

4. Angaben zur Erforderlichkeit der personenbezogenen Datenverarbeitung

Grundsätzlich ist dem Antrag ist ein Nachweis beizufügen, dass der Zugang zu den antragsgegenständlichen Daten und die beantragten Fristen für die Zwecke der Forschungsarbeiten notwendig und verhältnismäßig sind und dass die erwarteten Ergebnisse dieser Forschung zu den genannten Zwecken in Ziff. 4 beitragen werden. Bitte beschreiben Sie in diesem Textfeld ausdrücklich auch die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung der personenbezogenen Daten.

5. Angaben zur Anonymisierung [G3]

Aus dem Antrag hat hervorzugehen, ob der jeweilige konkrete Zweck des antragsgegenständlichen, dem Datenzugang nachgelagerten Forschungsvorhabens auch mit anonymisierten Daten erreicht werden kann.

- Wenn dies der Fall ist, ist eine Erläuterung des Anonymisierungsverfahrens dem Antrag als Anlage beizufügen.
- Wenn dies nicht der Fall ist, ist dem Antrag eine Anlage beizufügen, aus der konkret hervorgeht, warum die jeweilige Verarbeitung ggf. nicht mit anonymisierten Daten erfolgen kann und welche Rechtsgrundlage für die personenbezogene Datenverarbeitung einschlägig ist.

Hinweis:
Die Datenverarbeitungen zu den in Ziff. 7 genannten Zwecken können auf Grundlage des Art. 6 Abs. 1 lit. e DS-GVO (bei öffentlichen Forschungseinrichtungen für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt) oder lit. f (bei nichtöffentlichen Forschungseinrichtungen zur Wahrung berechtigter Interessen, wobei eine Abwägung mit den Interessen betroffener Personen vorzunehmen ist) und bei besonderen Kategorien personenbezogener Daten unter Anwendung von Art. 9 Abs. 2 lit. g DS-GVO (aus Gründen eines erheblichen öffentlichen Interesses) oder lit. j (für wissenschaftliche Zwecke) rechtmäßig sein.

6. Angaben zur Pseudonymisierung [G4]

Aus dem Antrag hat hervorzugehen, ob der jeweilige konkrete Zweck des antragsgegenständlichen dem Datenzugang nachgelagerten Forschungsvorhabens auch mit pseudonymisierten Daten erreicht werden kann.

- Wenn dies der Fall ist, ist eine Erläuterung des Pseudonymisierungsverfahrens dem Antrag als Anlage beizufügen.
- Wenn dies nicht der Fall ist, ist dem Antrag eine Anlage beizufügen, aus der konkret hervorgeht, warum die jeweilige Verarbeitung ausnahmsweise nicht mit pseudonymisierten Daten erfolgen kann.

7. Angaben zur personenbezogenen Datenverarbeitung

a. Dem Antrag ist eine Auflistung der vom Antrag umfassten Daten beizufügen, die auch darstellt, ob besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO (z.B. ethnischer Herkunft, sexuelle Orientierung, politische Meinung, Gesundheitsdaten) betroffen sind. Über das im Antrag vorgesehene Kontrollkästchen ist anzugeben, ob und ggf. mit welchen die vom Antrag umfassten Daten mit anderen, bereits vorliegenden Daten kombiniert werden.

b. Im Textfeld zur Rechtsgrundlage nach der DS-GVO ist anzugeben, ob bezüglich der geplanten Verarbeitung der beantragten Daten ein Verarbeitungsverzeichnis nach Art. 30 DS-GVO erstellt wurde. **[G5]**
Das Verzeichnis enthält auch Angaben dazu, ob die vom Antrag umfassten Daten an ein Drittland außerhalb des Europäischen Wirtschaftsraums oder eine internationale Organisation übermittelt werden (beispielsweise durch Übersendung an oder Einräumung eines Zugriffs für eine Stelle im Drittland) und ggf. Angaben dazu, dass die Datenübermittlungen die in Kapitel 5 der DS-GVO (internationale Datenübermittlung) niedergelegten Bedingungen einhalten. **[G6]**

8. Angaben zu angemessenen technischen und organisatorischen Maßnahmen [G7]

Dem Antrag ist eine Übersicht der getroffenen technischen und organisatorischen Maßnahmen beizufügen, die zum Schutz personenbezogener Daten, der Datensicherheit und der Vertraulichkeit getroffen wurden.

Hinweis: Dies umfasst Maßnahmen wie (nicht abschließend):

- Dokumentation im Sinne einer Inventarisierung aller Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO
- Bereitstellung von Informationen über die Verarbeitung von personenbezogenen Daten an Betroffene
- Schutz vor äußeren Einflüssen (Spionage, Hacking)

- spezifizierte, für die Verarbeitungstätigkeit ausgestattete Umgebungen (Gebäude, Räume)
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen usw.)
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept)
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen, insb. Betroffenenrechten
- Rechte- und Rollenkonzept, das gewährleistet, dass nur befugte Personen die antragsgegenständlichen personenbezogenen Daten weiterverarbeiten können sowie Weiterverarbeitungen protokolliert und unbefugte Verarbeitungen geahndet werden können;

  dieses Rechte- und Rollenkonzept muss in angemessenen regelmäßigen Abständen sowie anlassbezogen evaluiert und bei Bedarf angepasst werden
- Löschkonzept, das gewährleistet, dass die Daten zum gesetzlich geforderten Zeitpunkt gelöscht werden;

  eine Löschung muss spätestens 30 Jahre nach Beginn der antragsgegenständlichen Weiterverarbeitung erfolgen.

9. Angaben zur Datenschutz-Folgenabschätzung [G8, G9]

Hinweis: Eine Datenschutz-Folgenabschätzung muss durchgeführt werden, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. **[G8]**

Falls keine Datenschutz-Folgenabschätzung erstellt wurde, sind dem Antrag Ausführungen dazu beizufügen, weswegen eine Datenschutz-Folgenabschätzung nicht erstellt wurde. **[G9]**

10. Angaben zur Veröffentlichung

Im Data Access Portal ist durch Ankreuzen des entsprechenden Kontrollkästchens zu bestätigen, dass beim kostenlosen öffentlich Zugänglichmachen der Forschungsergebnisse innerhalb eines angemessenen Zeitraums nach Abschluss der Forschungsarbeiten (Art. 40 Abs. 8 lit. g DSA) die Rechte und Interessen der Nutzer und Nutzerinnen des betreffenden Dienstes im Einklang mit der Verordnung (EU) 2016/679 berücksichtigt werden.

Glossar	
[G1]	Siehe zur gemeinsamen Verantwortlichkeit DSK, Kurzpapier Nr. 16 (derzeit in Überarbeitung), abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf.
[G2]	Siehe zur Auftragsverarbeitung DSK, Kurzpapier Nr. 13 (derzeit in Überarbeitung), abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.
[G3]	Anonym sind personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann (EG 26 S. 5 DS-GVO).
[G4]	„Pseudonymisierung“ ist 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 (Art. 4 Nr. 5 DS-GVO). Siehe hierzu die vom Europäischen Datenschutzausschuss (EDSA) veröffentlichten Guidelines 01/2025 on Pseudonymisation, abrufbar unter https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_de
[G5]	Siehe zum Verzeichnis von Verarbeitungstätigkeiten das von der DSK bereitgestellte Muster-Formular, abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf
[G6]	Siehe zu Datenübermittlungen in Drittländer DSK, Kurzpapier Nr. 4, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf.
[G7]	Die DS-GVO fordert geeignete technische und organisatorische Maßnahmen, um die Risiken für die Rechte und Freiheiten natürlicher Personen angemessen zu mindern. Das betrifft sowohl Maßnahmen zur Gewährleistung der Rechte Betroffener (Kapitel III DS-GVO) als auch Maßnahmen zur Umsetzung der Datenschutzgrundsätze (Art. 25 Abs. 1 DS-GVO), darunter zur Datenminimierung (Art. 25 Abs. 2 DS-GVO) und zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 DS-GVO). Das Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) fordert zu einer sehr frühzeitigen Befassung des Verantwortlichen mit datenschutzrechtlichen Vorgaben bereits bei der Planung von Verarbeitungen auf. Die DS-GVO verlangt ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 24 Abs. 1 Satz 2, Art. 32 Abs. 1 Satz 1 lit. d DS-GVO) (siehe eingehend DSK, Standard-Datenschutzmodell V3.1, abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf).
[G8]	Siehe zum Risiko DSK, Kurzpapier Nr. 18, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.
[G9]	Siehe zur Datenschutz-Folgenabschätzung DSK Kurzpapier Nr. 5, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf und DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeDSK.pdf?__blob=publicationFile&v=7.