

# Sachbericht zum Verwendungsnachweis der DUV Speyer

Vorhabenbezeichnung: **Verbundprojekt „Anonymität bei integrierten und georeferenzierten Daten (AnigeD)“ / Förderkennzeichen: 16KISA093K**

Laufzeit des Vorhabens: **11/2022 - 11/2025**

Berichtszeitraum: **15.11.2022 – 31.12.2024**

## Teil I

Das Forschungsvorhaben, das an der Universität Speyer begonnen und dann wegen des Universitätswechsels des wissenschaftlichen Projektleiters an der Universität der Bundeswehr in München fortgeführt wurde, hatte die zentrale Frage zum Gegenstand, welche rechtlichen Anforderungen an eine rechtssichere Anonymisierung zu stellen sind.

Ausgangspunkt der wissenschaftlichen Analyse war die Beobachtung, dass Anonymisierung und Pseudonymisierung zwar wertvolle Werkzeuge für die Datenverarbeitung in Forschung, Wirtschaft und Verwaltung liefern, in der Praxis jedoch große Unsicherheiten bestehen, welche Verfahren tatsächlich geeignet sind. Für viele Stellen stellt daher die Auswahl eines geeigneten Anonymisierungsverfahrens eine erhebliche Herausforderung dar.

Das Vorhaben wurde in mehreren Schritten umgesetzt. Zunächst erfolgte eine Grundlagenforschung zur Anonymisierung, welche die Anforderungen im unionsrechtlichen Kontext systematisch darstellt und mit den Vorgaben des nationalen Statistikrechts abglichen. Ziel war es, die bestehenden Parallelen und Divergenzen zwischen beiden Regelungsebenen sichtbar zu machen, um eine präzisere juristische Einordnung der Anonymisierung im geltenden Normgefüge zu ermöglichen.

Abschließend hat das Projekt noch in der Speyerer Projektphase damit begonnen, sich mit einer vertieften Analyse des rechtlichen Rahmens für die wissenschaftliche Datenverarbeitung auseinanderzusetzen. Diese Forschung setzte an den gegenwärtigen Herausforderungen beim Zugang zu Forschungsdaten an, die sich im Spannungsfeld zwischen der Datenschutz-Grundverordnung (DSGVO), den nationalen datenschutzrechtlichen Bestimmungen und den vielfältigen technischen Schutzmaßnahmen bewegen. Zwar enthält die DSGVO zahlreiche Öffnungsklauseln und Privilegierungen zugunsten der wissenschaftlichen Datenverarbeitung. Doch zeigt sich in der praktischen Umsetzung, dass diese Spielräume für Forschende häufig nur schwer nutzbar sind. Viele Wissenschaftler stehen vor der Unsicherheit, ob ihre Forschungsvorhaben tatsächlich den datenschutzrechtlichen Anforderungen in vollem

Umfang genügen. Im Mittelpunkt dieses an der Universität der Bundeswehr fortgesetzten Projektabschnitts standen die Auslegung der einschlägigen Privilegierungstatbestände der DSGVO – insbesondere des Art. 89 Abs. 1 DSGVO – sowie ihr Zusammenspiel mit den entsprechenden Forschungsklauseln im nationalen Recht. Diese Untersuchung diene dazu, die bestehenden datenschutzrechtlichen Gestaltungsspielräume für Forschungseinrichtungen zu identifizieren und zugleich die bestehenden Unsicherheiten bei ihrer praktischen Anwendung sichtbar zu machen. Die Analyse mündete in der Idee, die Rechtsfigur eines zertifizierten Wissenschaftlers zu entwickeln.

Diese soll als ergänzende Garantie im Sinne der DSGVO fungieren und Forschenden einen verlässlicheren Rechtsrahmen für den Datenzugang eröffnen, ohne dabei den Schutz der betroffenen Personen zu vernachlässigen. Der Vorschlag knüpft an die bestehenden Privilegierungstatbestände an und zeigt auf, wie durch organisatorische Maßnahmen mehr Rechtssicherheit geschaffen werden kann.

Im weiteren Verlauf des Projekts wurden einzelne spezifische Fragestellungen vertieft, etwa die Auswirkungen neuer unionsrechtlicher Digitalrechtsakte und deren Verhältnis zur DSGVO. Ziel war es, systematische Zusammenhänge und mögliche Konfliktlagen zwischen verschiedenen Regelungsregimen besser zu verstehen.

Parallel dazu wurde eine technisch-rechtliche Schnittstelle bearbeitet. Gemeinsam mit einem Kollegen vom MPI, der in das Projektkonsortium eingebunden ist, wurde eine Anonymisierungsmetrik entwickelt, die es erlaubt, Informationsabflüsse realistisch zu messen und damit eine Brücke zu den Anforderungen der DSGVO zu schlagen. Dieser Ansatz bietet eine quantifizierbare Grundlage für die Bewertung von Anonymisierungsmethoden und adressiert damit eine der zentralen Herausforderungen in der datenschutzrechtlichen Forschungspraxis.

Insgesamt hat das Projekt wesentliche Grundlagen für ein besseres Verständnis der Anonymisierung und ihrer rechtlichen Einordnung gelegt, die bestehenden Privilegierungstatbestände der DSGVO systematisch untersucht und durch die Entwicklung technischer und organisatorischer Konzepte neue Perspektiven eröffnet. Die erarbeiteten Teilergebnisse tragen dazu bei, die Datenverarbeitung rechtssicherer zu gestalten und damit sowohl für die wissenschaftliche Praxis als auch für die Weiterentwicklung des Datenschutzrechts einen nachhaltigen Beitrag zu leisten.

## Teil II

Das Projekt hat die zentrale Frage zum Gegenstand, welche rechtlichen Anforderungen an eine rechtssichere Anonymisierung zu stellen sind. Ziel war es, durch juristische Grundlagenarbeit, konzeptionelle Überlegungen sowie technische Ergänzungen einen Beitrag dazu zu leisten, wie Anonymisierung – ggf. mithilfe von Metriken – rechtssicher umgesetzt werden kann. Das Projekt wurde an der Universität Speyer begonnen und (wegen des Universitätswechsels des Projektleiters) an der Uni BW München fortgesetzt.

### I. Stand der Forschung

In einer Welt zunehmender Datenverfügbarkeit, wachsender Rechenkapazitäten und ubiquitärer Datenverarbeitung wird es immer leichter, Personen bereits anhand weniger Merkmale zu identifizieren. Lässt sich der Personenbezug unkompliziert herstellen, weitet sich damit auch der Anwendungsbereich des Datenschutzrechts stetig aus. Daraus erwächst zugleich eine erhöhte Rechtsunsicherheit: Verantwortliche müssen damit rechnen, unversehens in den Anwendungsbereich des Datenschutzrechts zu geraten, weil eine Reidentifizierung technisch möglich ist. Das hat mitunter zur Folge, dass Verantwortliche darauf verzichten, aus Furcht vor möglichen Rechtsverstößen werthaltige Daten zu nutzen kann.

Die Rechtswissenschaft steht vor der Herausforderung, die Trennlinie zwischen schutzbedürftigen personenbezogenen Daten und tatsächlich anonymisierten Informationen präzise zu bestimmen.

Anonymisierung verfolgt das Ziel, diesen Personenbezug zu entfernen, sodass die Daten nicht mehr in den Anwendungsbereich der DSGVO fallen. Dafür ist Voraussetzung, dass dem Verantwortlichen und einem potenziellen Angreifer keine Mittel zur Verfügung stehen, die er nach allgemeinem Ermessen dazu einsetzen wird, um eine betroffene Person zu identifizieren (ErwGr. 26 S. 3 DSGVO).

Für diese Einschätzung verlangt der europäische Gesetzgeber eine Abwägung aller objektiven Faktoren, wie der Kosten, des Zeitaufwands und der zur Verfügung stehenden technischen Mittel (ErwGr. 26 S. 4 DSGVO). Diese Kriterien sind jedoch bewusst offengehalten, sodass es Aufgabe der Rechtswissenschaft bleibt, sie zu präzisieren und für die Praxis handhabbar zu machen. Nur so kann Rechtssicherheit geschaffen werden.

### II. Aufgabenstellung

Obwohl die Rechtsunsicherheitsrisiken, die von dem Begriff der Anonymisierung ausgehen, als Problemlage in der Rechtswissenschaft erkannt sind, fehlt bislang eine dogmatisch überzeugende Lösung. Dazu trägt auch der unzureichende Austausch mit anderen Disziplinen, insbesondere der Informatik, der Statistik und Mathematik, bei. Bisherige Ansätze orientieren sich stark an Einzelfallbetrachtungen und bieten kein konsistentes Rahmenmodell, das auch für neue Situationen tauglich wäre.

Das rechtswissenschaftliche Teilprojekt im Rahmen des Projektverbundes AnigeD hat sich zum Ziel gesetzt, diese Lücke zu schließen, indem es die in der Rechtsordnung angelegten materiellen Maßstäbe für Anonymisierung systematisch analysiert und – soweit möglich – in formalisierte Kriterien überführt. Es soll das Fundament dafür legen, eine einheitlichere und vor allem rechtssichere Kategorisierung von Daten zu ermöglichen, welche die Trennlinie zwischen personenbezogenen und anonymisierten Daten hinreichend klar erkennbar macht. Die Anwendungspraxis profitiert dann von einem klareren Maßstab, der weniger Raum für subjektive Wertungen lässt und zugleich ein höheres Maß an Rechtssicherheit ermöglicht. Der Ansatz des Projekts besteht darin, Erkenntnisse aus anderen wissenschaftlichen Disziplinen, insbesondere der Technikwissenschaften, einzubeziehen und rechtswissenschaftlich zu reflektieren, um ein praxistaugliches, interdisziplinär fundiertes Ergebnis hervorzubringen.

### III. Projektarbeiten

#### 1. Grundlagenarbeit zur Anonymisierung im unionsrechtlichen Kontext

Ein erster Schwerpunkt der Forschungstätigkeit lag darin, das systematische Verhältnis zwischen der DS-GVO und anderen unionsrechtlichen Digitalrechtsakten zu entschlüsseln. Während die DSGVO als Magna Charta des Schutzes personenbezogener Daten gilt, treten zunehmend sektorale Regelungen hinzu, die ebenfalls Anforderungen an den Umgang mit Daten formulieren. Dazu gehören insbesondere der europäische Daten-Governance-Act (DGA), der Data Act (DA), der Digital Markets Act (DMA), der Digital Services Act (DSA) sowie die KI-VO. Auch diese rekurren auf die Rechtsfigur der Anonymisierung.

Bislang fehlte eine umfassende rechtsdogmatische Einordnung, wie diese neuen Vorschriften sich mit den bestehenden Grundsätzen der DSGVO vereinbaren lassen. Das Projekt untersuchte daher systematisch, inwiefern die Vorgaben zur Anonymisierung und Pseudonymisierung in diesen Rechtsakten – insbesondere mit Blick auf georeferenzierte Daten – mit den Grundsätzen der DSGVO kollidieren oder harmonieren.

Daneben legten die Forschenden auch einen besonderen Fokus auf die Vorgaben des nationalen Statistikrechts – insbesondere des Bundesstatistikgesetzes (BStatG). Auch dieses stellt Anforderungen an eine Anonymisierung – grenzt seine Begrifflichkeiten aber nicht gegen die Vorgaben der DS-GVO ab und lässt offen, inwieweit es sich von den Vorgaben der DS-GVO unterscheidet und mit diesen vereinbar ist. Durch die Gegenüberstellung und rechtliche Analyse beider Regelungsbereiche konnten Unstimmigkeiten, aber auch Parallelen herausgearbeitet werden.

Diese Arbeiten bilden eine wesentliche Grundlage, um künftige Forschungsvorhaben rechtlich sicher einzuordnen, und bieten zugleich Orientierung für den Gesetzgeber, wie eine kohärente Normenlandschaft geschaffen werden kann.

#### 2. Entwicklung der Figur des „zertifizierten Wissenschaftlers“

Nicht zuletzt in Anbetracht der derzeitigen Vorarbeiten zu einem Forschungsdatenzugangsgesetz, mit welchem das Bundesministerium für Bildung und Forschung „den Zugang zu Daten für die Wissenschaft verbessern und Rahmenbedingungen

für die Weitergabe, Aufbewahrung und Sicherung gestalten“ will, hat das Projekt einen besonderen Fokus auf die (Weiter-)Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken gelegt. Diese spielen gerade für georeferenzierte Daten eine besondere Rolle. Denn die wissenschaftliche Forschung ist häufig auf die Verfügbarkeit ortsbezogener Daten angewiesen.

Die Forschungsaufgabe in dieser Teilprojektphase bestand zunächst darin, die Privilegierungstatbestände der DSGVO herauszuarbeiten und zu eruieren, ob diese Privilegierungen in der Praxis hinreichend wirksam sind. Zentrale normative Stellschraube ist insoweit Art. 89 DSGVO. Die Vorschrift verweist auf die Einhaltung geeigneter Garantien verweist, die durch technische und organisatorische Maßnahmen sicherzustellen sind.

Obleich diese Regelungen auf europäischer Ebene eine klare Privilegierung für die Verarbeitung zu Forschungszwecken erkennen lassen, zeigte die bisherige Forschungspraxis in Deutschland und anderen Mitgliedstaaten erhebliche Unsicherheiten. Forschende berichten immer wieder von Schwierigkeiten beim Datenzugang, von einer unklaren Anwendbarkeit der Rechtsgrundlagen und von einem erheblichen Risiko, dass ihre Arbeit als nicht konform mit den Datenschutzvorschriften eingestuft werden könnte.

Die Projektmitglieder haben es sich zur Aufgabe gemacht, diese Lücke zwischen rechtlicher Normierung und praktischer Umsetzbarkeit zu schließen. Parallel zur Grundlagenarbeit haben sie die Figur des „zertifizierten Wissenschaftlers“ entwickelt. Dieses Konzept setzt an den in Art. 89 DSGVO genannten Garantien an, die bislang rechtlich wenig konkretisiert sind. Es soll gezielt die Schwierigkeiten der Wissenschaft, an Daten zu gelangen, adressieren.

Die Idee besteht darin, die Gewährleistung datenschutzkonformer Verarbeitung nicht allein durch technische Maßnahmen wie Anonymisierung zu sichern, sondern auch durch eine personenbezogene Zertifizierung. Forschende, die einen bestimmten Qualifikations- und Verhaltensstandard nachweisen, könnten einen besonderen rechtlichen Status erlangen, der ihnen den Zugang zu Forschungsdaten erleichtert.

Hierzu stellten sich drei zentrale Fragen, die sich noch in der Bearbeitung befinden:

1. Welche inhaltlichen Anforderungen müsste eine solche Zertifizierung umfassen (z. B. Schulungen, datenschutzrechtliche Kenntnisse, Vertragsstrafen)?
2. Auf welcher normativen Grundlage könnte die Zertifizierung verankert werden (z. B. im geplanten Forschungsdatenzugangsgesetz)?
3. Wie bettet sich die Figur in bestehende datenschutzrechtliche Mechanismen wie datenschutzrechtliche Sanktionen ein? Oder sind darüber hinausgehende Maßnahmen nötig?

Ziel der Arbeiten ist ein differenzierter Vorschlag, wie die Forschungsfreiheit und der Datenschutz durch eine solche institutionalisierte Garantie in ein angemessenes Gleichgewicht gebracht werden können. Im Rahmen der Recherche war auch der projektinterne Austausch von besonders wertvoller Bedeutung, um Einblicke zum Ablauf in der Praxis (wie den Forschungsdatenzentren (FDZ)) einzubeziehen und bisherige Erfahrungen von Forschenden zu berücksichtigen, damit die Figur so praxistauglich wie möglich entwickelt werden kann, ohne gleichzeitig den Datenschutz aus den Augen zu verlieren.

### 3. Formalisierung der materiellen Kriterien

Eine Stärke des Projekts lag in der interdisziplinären Zusammenarbeit mit externen Partnern, insbesondere mit dem Max-Planck-Institut. Ziel war es, einen quantifizierbaren Ansatz zur Bewertung der Wirksamkeit von Anonymisierungsmethoden zu entwickeln.

Die Frage, wie sich die rechtlich maßgeblichen Kriterien zur Beurteilung einer Anonymisierung konkretisieren lassen, ist bislang ungelöst. Das Projekt setzte hier an und wollte diese Maßstäbe in ein kohärentes, formalisiertes Modell überführen. Ausgangspunkt war das Konzept des sog. Grundrisikos: Jede Person ist unabhängig von einer konkreten Datenverarbeitung einem gewissen Risiko ausgesetzt, dass andere über sie im Wege der verarbeitenden Informationen Erkenntnisse erlangen. Dieses Risiko besteht selbst dann, wenn ein Datensatz nicht weitergegeben wird. Unklar ist jedoch, wie dieses Grundrisiko zu quantifizieren ist.

Im nächsten Schritt haben die Forschenden untersucht, wie sich die Veröffentlichung oder Weitergabe eines Datensatzes auf dieses Grundrisiko auswirkt – die sog. Risikoverschiebung. Sie haben verschiedene Vorschläge zu ihrer Messung im Hinblick auf ihre rechtliche Tragfähigkeit und praktische Handhabbarkeit analysiert. Schließlich galt es zu bewerten, in welchem Umfang eine solche Risikoverschiebung noch zulässig ist, damit ein Datensatz als anonym gelten darf. Auch hierfür sind normative Vorgaben erforderlich, um Legitimität zu gewährleisten.

Die bisherigen Ansätze, wie etwa „Differential Privacy“ (DP), verfolgen die Begrenzung von Informationsabflüssen, erweisen sich aus juristischer Perspektive jedoch als schwer interpretierbar. Insbesondere der zentrale Parameter „Epsilon“ ist kaum operationalisierbar und kann nicht zuverlässig zur Rechtssicherheit beitragen.

Das Projekt entwickelte daher eine alternative Metrik, die nicht theoretische, sondern realistische Informationsabflüsse misst. Dieser Ansatz hat den Vorteil, dass er unmittelbar mit den rechtlichen Vorgaben der DSGVO in Einklang gebracht werden kann: Die Frage, ob eine Verarbeitung ein „hohes Risiko“ für die Rechte der Betroffenen im Sinne von Art. 35 DSGVO darstellt, lässt sich anhand der Metrik wesentlich klarer beantworten. Damit entstand in der juristisch-informatischen Zusammenarbeit ein Werkzeug, das künftig in der datenschutzrechtlichen Praxis eingesetzt werden könnte, um die Angemessenheit von Anonymisierungsmaßnahmen nachzuweisen.

## IV. Wichtigsten Positionen des zahlenmäßigen Nachweises

Die Zuwendungen wurden in erster Linie für folgende Positionen eingesetzt:

- (zum ganz überwiegenden Teil) Personalkosten für wissenschaftliche Mitarbeitende, um juristische Grundlagen- und Recherchearbeit durchzuführen sowie die Forschungsergebnisse zu dokumentieren und zu veröffentlichen, um die wissenschaftliche Anschlussfähigkeit zu sichern.
- (in sehr überschaubarem Umfang) Reisekosten für die interdisziplinäre Zusammenarbeit, insbesondere zur Teilnahme an den Werkstattgesprächen mit den Projektpartnern sowie an Fachkonferenzen des Netzwerks AnoSiDat, um sich über

Erkenntnisse auszutauschen und unterschiedliche Ansätze kennenzulernen. Die Mittel wurden in geringerem Umfang als beantragt beansprucht.

- (In geringem Umfang) Sachmittel für Publikationskosten und Arbeitsmaterialien, um die Forschungsergebnisse der breiten Öffentlichkeit zugänglich zu machen.

Die Mittelverwendung erwies sich als notwendig und angemessen, da ohne die umfangreiche personelle Unterstützung die umfassende dogmatische Grundlagenarbeit nicht zu leisten gewesen wäre und die Kooperation mit den technischen Partnern von zentraler Bedeutung für die Validierung der Ergebnisse war.

## V. Veröffentlichungen und wissenschaftliche Anschlussfähigkeit

Bereits veröffentlicht wurde ein Beitrag zum Mobilitätsdatengesetz mit dem Fokus auf den datenschutzrechtlichen Herausforderungen (insb. der Anonymisierung der Daten), [NJW 2024, 2379 - 2384](#).

Daneben entstand in der Zusammenarbeit zwischen Herrn Wagner und Herrn Francis vom MPI der Aufsatz mit dem Titel „Towards more accurate and useful data anonymity vulnerability measures“ (<https://doi.org/10.48550/arXiv.2403.06595>). Zudem haben die Forschenden an Beiträgen von Projektpartnern mitgewirkt und diese um eine rechtliche Einschätzung ergänzt (bspw. am Artikel zu Aufdeckungsrisiken und Bereitstellungsmöglichkeiten synthetischer Daten am Beispiel der Verdienststrukturerhebung 2018, der im Rahmen des AnigeD-Projekts verfasst wurde).

Die Veröffentlichungen zu den rechtlichen Herausforderungen einer Anonymisierung, die die gesamte Grundlagenarbeit als Monographie zusammenfasst, sowie der Beitrag zur Figur des zertifizierten Wissenschaftlers wurden in der Projektphase an der Uni BW fortgesetzt und stehen nunmehr kurz vor dem Abschluss.

Alle Beiträge sollen – soweit möglich – durch eine Open-Access-Veröffentlichung der breiten Fachöffentlichkeit zur Verfügung stehen und dadurch für eine wissenschaftliche Anschlussfähigkeit bürgen. Die Forschungsbeiträge sind so konzipiert, dass sie in die Rechtspraxis ausstrahlen. So können sie etwa Aufsichtsbehörden als Ausgangspunkt dienen, um Verfahren zur Zertifizierung von Anonymisierungsverfahren zu entwickeln. Diese Zertifizierungen sind ein wichtiger Baustein, um die Rechtssicherheit bei der Anonymisierung von Daten und damit insgesamt die Datenverfügbarkeit zu erhöhen. Auch Gerichte, Forschungsdatenzentren, Statistikbehörden und der Gesetzgeber (des geplanten Forschungsdatenzugangsgesetzes) können auf die Erkenntnisse zurückgreifen. Der öffentliche Zugang zu der Forschungstätigkeit ist durch die geplante Verwertung folglich gesichert.