Georg-August-Universität Göttingen
- Der Datenschutzbeauftragte -

Datenschutz in der Forschung

Beitrag zur Vortragswoche der eResearch Alliance
„Rechtliche Aspekte im Forschungsdatenmanagement“

Florian Hallaschka,
stellvertretender Datenschutzbeauftragter

22. März 2022

12.30 Uhr

Gliederung

I. Warum Datenschutz? Was ist Datenschutz?
II. Und was hat das mit mir als Forscher*in zu tun?
III. Tools
IV. Internationale Forschungskooperationen
V. Repositorien
VI. Vorgehensweise bei datenschutzrelevanten Forschungsprojekten - Wissenschaftliche Studien: Prozess bei Einreichung und Handreichung dazu

I. Warum Datenschutz? Was ist Datenschutz?

Warum Datenschutz? „Ich hab doch nichts zu verbergen!“

- Jede_r hat soziale Rollen
- Je nach Umständen soll das Gegenüber mehr oder weniger von einem wissen
- „Wenn sie einem Durchschnittsmenschen seine Lebenslüge nehmen, so bringen sie ihn gleichzeitig um sein Glück.“ (Ibsen, Die Wildente, 5. Akt)
  = Das Aufrechterhalten von Selbstdarstellungen muss möglich bleiben
- Bekanntwerden von Daten = Missbrauchsmöglichkeit – Identitätsdiebstahl
- Privatsphäre muss geschützt werden

BVerfGE 65, 1: Volkszählungsurteil 1983

„Informationelles Selbstbestimmungsrecht“ = „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.

Herkunft: Art. 2 Abs. 1 (Allg. Persönlichkeitsrecht) i.V.m. Art. 1 Abs. 1 (Menschenwürde) des Grundgesetzes

Datenschutz

= Schutz des informationellen Selbstbestimmungsrechts

Nicht: Schutz ***der*** Daten
(d.i. Informationssicherheit (Überschneidung mit Datenschutz)),

sondern

Schutz ***vor*** Daten
bzw. vor dem *Bekanntwerden/der unbefugten Kenntnisnahme* von Daten

Verordnung 2016/679/EU
= Europäische Datenschutz-Grundverordnung (EU-DSGVO)

Rechtsnatur der EU-DSGVO

DSGVO = Europäische Verordnung: Unmittelbar geltend in allen Mitgliedstaaten, kein nationaler Umsetzungsakt erforderlich

Aber: **Grund**verordnung, d.h. es gibt Spielräume („Öffnungs- und Präzisierungsklauseln“) für die Mitgliedstaaten

Der Niedersächsische Landtag erließ als Lückenfüllungsgesetz nur eine Woche vor Ingeltungsetzung der DSGVO ein neues Niedersächsisches Datenschutzgesetz (NDSG)

II. Und was hat das mit mir als Forscher*in zu tun?

Forschung mit personenbezogenen Daten (pbD)

DSGVO nur anwendbar auf **personenbezogene** Daten, d.h. Informationen über identifizierte oder identifizierbare Personen, zum Beispiel Name, Adresse, Matrikelnummer, IP-Adresse. (Identifizierbarkeit z.B. über Pseudonym, Standortdaten, persönliche Merkmale)

Grundsatz: Datenverarbeitung ist verboten!

Datenverarbeitung unterliegt einem

Verbot mit Erlaubnisvorbehalt!

Datenverarbeitung ist grundsätzlich verboten und **nur erlaubt mit Einwilligung der betroffenen Person oder einer anderen Rechtsgrundlage** (Art. 6 Abs. 1 DSGVO)!

Prinzipien des Datenschutzes

- **Rechtmäßigkeit**
- Verarbeitung nach Treu und Glauben
- **Erforderlichkeit**
- **Zweckbindung**
- **Transparenz**
- Richtigkeit
- **Technisch-organisatorischer Datenschutz**
- **Datenminimierung/Speicherbegrenzung**
- **Integrität und Vertraulichkeit**
- **Betroffenenrechte**
- **Rechenschaftspflicht/Dokumentationspflicht**

Das Schutzstufenkonzept der LfD Niedersachsen

Schutz-stufe	Personenbezogene Daten,	zum Beispiel	Schwere eines möglichen Schadens
A	die von den Betroffenen frei zugänglich gemacht wurden.	Telefonverzeichnis, Wahlvorschlagsverzeichnisse, eigene freizugänglich gemachte Webseite; frei zugängliche soziale Medien	geringfügig
B	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien	
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen").	Einkommen, Grundsteuer, Ordnungswidrigkeiten	überschaubar
D	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz").	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Arbeitszeugnisse, Gesundheitsdaten, Schulden, Pfändungen, Sozialdaten, Daten besonderer Kategorien nach Art. 9 DS-GVO	substantiell
E	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm	groß

Tabelle: Übertragung der Schwere des möglichen Schadens auf das niedersächsische Schutzstufenkonzept

Verarbeitung besonderer Kategorien personenbezogener Daten

(Art. 9 lit. j) EU-DSGVO)

Immer mindestens Schutzstufe D: Daten zu

- „rassischer“ und ethnischer Herkunft
- politischen Meinungen
- religiösen oder weltanschaulichen Überzeugungen oder Gewerkschaftszugehörigkeit
- biometrische Daten zur Identifizierung einer natürlichen Person
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

dürfen nach Art. 9 Abs. 2 lit. a) DSGVO nach Einwilligung; nach Art. 9 Abs. 2 lit. j) bei Vorliegen einer Rechtsgrundlage in der wissenschaftlichen Forschung verarbeitet werden – Forschungsprivileg –; wo ihre Verarbeitung notwendig ist, sind besondere Maßnahmen zum Schutz dieser Daten notwendig („geeignete Garantien“ – Art. 89 DSGVO)

Art. 89 DSGVO: Garantien und Ausnahmen

- Verarbeitung unterliegt geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person
- Datenminimierung
- Technisch-organisatorische Maßnahmen zum Risikoausgleich
- Pseudonymisierung
- Anonymisierung
- Betroffenenrechte auf Auskunft (Art. 15), Berichtigung (Art. 16), Einschränkung der Verarbeitung (Art. 18), Widerspruchsrecht (Art. 21) einschränkbar

Datenschutz-Folgenabschätzung (Art. 35 EU-DSGVO)

- Bei Hochrisikoverarbeitung: Risikoanalyse mit Gefahren und Gegenmaßnahmen

  Bsp.: Umfrage mit Erhebung von heiklen Gesundheitsdaten

- Der DSB berät lediglich auf Anfrage, nimmt die DSFA nicht selbst vor.

- Bei Restrisiken ggf. Meldung an Aufsichtsbehörde (Landesbeauftragte für den Datenschutz Niedersachsen (LfD))

Technisch-organisatorische Maßnahmen (TOMs)

Ziele: Vertraulichkeit, Integrität, Verfügbarkeit, Wiederherstellbarkeit

- **Zutrittskontrolle**: unbefugten Zutritt zu Räumen verhindern (Chipkarte, Alarmanlage…)

- **Zugangskontrolle/Zugriffskontrolle**: unbefugten Zugang zu/Zugriff auf IT-Geräten und Daten verhindern (Verschlüsselung...)

- **Benutzerkontrolle/Eingabekontrolle**: Sicherstellen/Protokollieren, wer wann zugreift (Logfiles…)

- **Weitergabekontrolle/Transportkontrolle**: Örtlichen/logischen Transport sichern (VPN, Safe, E-Mail-Verschlüsselung…)

- **Verfügbarkeitskontrolle/Wiederherstellbarkeit**: (Backup, USV)

- **Trennungskontrolle**: (getrennte Zwecke:getrennte Speicherung)

- **Datenträgerkontrolle/Speicherkontrolle**: Unbefugtes Verändern/Löschen von Daten auf Datenträgern verhindern (verschlüsselte Festplatte, Rechte und Rollen...)

Aufweichung der Zweckbindung für Forschungsprojekte (Art. 5 Abs. 1 lit. b) EU-DSGVO)

- Erleichtert die Nachnutzung von Forschungsdaten und ermöglicht

„broad consent“

= Einwilligung in wissenschaftliche Forschung an den eigenen Daten mit weniger großen Einschränkungen oder in allgemeinerer Form

Forschungsklausel im NDSG

§ 13 NDSG – Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken

Wissenschaftliche Forschung mit pbD einschließlich Art. 9 Abs. 1 DSGVO erlaubt, wenn:

- bestimmtes Forschungsvorhaben

- Schutzwürdiges Interesse der betroffenen Person nicht entgegensteht

- oder öffentliches Interesse an der Durchführung des Forschungsvorhabens das schutzwürdige Interesse überwiegt

Im letzteren Fall: - Ergebnis der Abwägung und Begründung aufzeichnen.

- Über die Verarbeitung ist der Datenschutzbeauftragte zu unterrichten.

- Forschungsdaten anonymisieren, sobald nach Forschungszweck möglich

Bis dahin: - Merkmale, die Personenbezug herstellen, getrennt speichern
- nur zusammenführen, soweit der Forschungszweck dies erfordert.

Forschungsklausel im NDSG

- pbD aus Forschungsvorhaben dürfen nur veröffentlicht werden, wenn

1. Einwilligung der betroffenen Person oder

2. für Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich

- Absehen von Art. 15, 16, 18 und 21 DSGVO möglich, soweit und solange die Inanspruchnahme dieser Rechte voraussichtlich die Verwirklichung der jeweiligen wissenschaftlichen oder historischen Forschungszwecke unmöglich macht oder ernsthaft beeinträchtigt und Ausschluss dieser Rechte für die Erfüllung dieser Zwecke notwendig ist.

Außerhalb des Geltungsbereichs des NDSG (and. B.land, privat, Ausland):

- Übermittlung an Dritte nur, wenn sich diese verpflichten, die Daten ausschließlich für das von ihnen bezeichnete Forschungsvorhaben und nach Abs. 1 bis 3 zu verarbeiten und Schutzmaßnahmen nach § 17 NDSG für Art.-9- Abs.1-Daten oder gleichwertige Maßnahmen zu treffen
Übermittlung ist der LfD in diesem Fall rechtzeitig vorher anzuzeigen

Informationspflichten (Art. 13 DSGVO)

Bereits bei Beginn einer Datenverarbeitung Hinweisblatt:

- *Namen und Kontaktdaten des Verantwortlichen und seines Vertreters*
- *Namen und Kontaktdaten des DSB*
- *Verarbeitungszweck und Rechtsgrundlage*
- *(Kategorien von) Empfänger(n) der Daten*
- *Absicht der Übermittlung in Drittländer mit Angabe des dortigen Datenschutzniveaus*
- *Speicherdauer*
- *Bestehen von Betroffenenrechten (nicht: Datenübertragbarkeit (Art. 20 Abs. 3 S. 2))*
- *Falls Einwilligung: Widerruflichkeit angeben*
- *Bestehen eines Beschwerderechts gegenüber einer Aufsichtsbehörde (s. Art. 77 DSGVO), z. B. der LfD*
- *Bereitstellung der Daten verpflichtend? Folgen der Nichtbereitstellung*
- *Bestehen einer automatischen Entscheidungsfindung?*

Muster deutsch/englisch auf der Homepage des Datenschutzbeauftragten

Weitere Informationspflichten Art. 14 EU-DSGVO

Abweichende Informationspflichten bei Erhebung nicht direkt bei der betroffenen Person (Gegensatz zur „Direkterhebung“), z.B.

Angabe der Datenquelle erforderlich.

Information kann nach Art. 14 Abs. 5 lit. b) S. 1 DSGVO bei Gefährdung des Forschungsziels ausnahmsweise unterbleiben (Güterabwägung!), *gilt nicht für Zweckänderung bereits vorher erhobener Daten; über diese ist Mitteilung zu machen, Art. 13 Abs. 3 bzw. 14 Abs. 4 DSGVO*

Muster auf der Homepage des Datenschutzbeauftragten (deutsch)

Einwilligungserklärungen
1.Erwachsene (Art. 7 EU-DSGVO)

- Einwilligungen = informierte Einwilligungen: Zu Dokumentationszwecken dauerhaft aufzubewahren.

Daher besonders wichtig bei elektronischen Einwilligungen:

- *Zeitstempel der Einwilligung*
- *Tatsache der Einwilligung*
- *zugrundeliegender Einwilligungstext ist dauerhaft vorzuhalten*

- Einwilligung jetzt auch **formlos**, aber: eindeutig und aktiv (**Opt-in**). Wegen der **Beweisbarkeit** sollte man bei elektronischer oder schriftlicher Form bleiben

Einwilligungserklärungen
2. Kinder (Art. 8 Abs. 1 EU-DSGVO)

- Kinder können erst ab 16 Jahren selbst einwilligen

- Sonst: durch (beide) Sorgeberechtigte, Kinder ab 14 können sich wehren

- Betrifft an der Uni z.B. XLAB, YLAB, Kinder-Uni - schon die Anmeldung!

Dokumentations- und Rechenschaftspflichten
Art. 5 Abs. 2, 24 Abs. 1 und 3 EU-DSGVO

Um eine eventuelle Haftung oder Bußgelder zu vermeiden, muss „alles“ dokumentiert und aufbewahrt werden, z.B. (Auswahl!):

- Einwilligungserklärungen

- Datenschutz-Folgenabschätzungen (DSFA, früher: „Vorabkontrollen“) bei besonders datenintensiven oder „gefährlichen“ Vorhaben; ggf. schriftliche Angabe der Gründe, warum keine DSFA stattfand

- Einhaltung tech.-org. Maßnahmen (TOM)

- Einhaltung der Informationspflichten

- Rechenschaftsberichte bei Datenpannen

Auftragsverarbeitung (Art. 28 ff. EU-DSGVO)

Immer dann, wenn Datenverarbeitung „outgesourct“ wird, also eine außenstehende Person/Institution (zumindest theoretisch) Zugriff auf personenbezogene Daten nehmen kann (z.B. Anbieter von Umfragesoftware, Fernwartung von Systemen), ist ein Auftragsverarbeitungsvertrag (AVV) zu schließen.

Auftragsverarbeiter müssen (durch Zertifizierungen dokumentiert!) vertrauenswürdig sein → prüfen!

Beispiele für geprüfte Umfrage-Verarbeitende:

GWDG (Lime Survey) – abgedeckt über Rahmenvertrag
Unipark/Questback – Vertrag erhältlich beim Anbieter
SoSciSurvey – Vertrag erhältlich beim Anbieter
Respondi – Vertrag erhältlich beim Anbieter
Im Zweifel den Datenschutzbeauftragten fragen!

Gemeinsame Verantwortlichkeit (Art. 26 EU-DSGVO)

Wichtig für Forschungskooperationen

Immer dann, wenn zwei oder mehr Daten Verarbeitende **gemeinsam Mittel und Zwecke der Datenverarbeitung festlegen**, ist an eine Gemeinsame Verantwortlichkeit zweier oder mehrerer Verantwortlicher zu denken.
Diese erfordert einen Vertrag zwischen den Parteien, der die Wirkungskreise (falls aufgeteilt) und die Zuständigkeit für die Sicherstellung der Betroffenenrechte und Informationsrechte festlegt. Es kann zur Vereinfachung für die betroffenen Personen ein gemeinsamer Ansprechpartner bestimmt werden. Dies z.B. als Annex zum Kooperationsvertrag.

Übermittlung von Daten in ein Drittland (Art. 44 ff. EU-DSGVO)

- Art. 45: Angemessenheitsbeschluss (Schweiz, Israel, Argentinien, Uruguay, Japan, Kanada (nur komm.), Neuseeland, Andorra, Man, Jersey, Guernsey, Färöer, geplant: Großbritannien)
- Art. 46: Geeignete Garantien, z.B.
  - rechtlich bindende und durchsetzbare Vereinbarung (problematisch in Unrechtsstaaten bzw. Staaten mit zweifelhaften Geheimdiensten)
  - **Standarddatenschutzklauseln** (seit Scheitern des Privacy Shield bei USA einzige Möglichkeit, aber nur wenn zus. Maßnahmen wie Verschlüsselung)
  - Genehmigte Zertifizierung oder genehmigte Vertragswerke
- Art. 47: Verbindliche interne Datenschutzklauseln (konzernintern)
- Art. 48: Aufgrund Urteils nur bei Gegenseitigkeit
- Art. 49: Ausnahmen
  - Einwilligung, Vertragserfüllung etc.: **Nicht für Behörden** in Ausübung ihrer hoheitlichen Tätigkeit
  → je nachdem, ob die Universität Göttingen gerade als Behörde handelt (Double Degree, Prüfungsbewertung)
  oder nicht (Organisation freiwilliger Austauschprogramme)

Betroffenenrechte (Art. 12-22 DSGVO)

-Information (Art. 12-14)

-Auskunft (Art. 15)

-Berichtigung (Art. 16)

-Löschung, Recht auf Vergessenwerden (Art. 17)

-Einschränkung der Verarbeitung (Sperrung) (Art. 18)

-Datenportabilität (Art. 20 – nicht bei Erfüllg. öffentl. Aufgaben (20 III 2))

-Widerspruch (Art. 21)

…und natürlich ganz allgemein der Widerruf von Einwilligungen (Art. 7 III)

Sanktionen bei Verstößen (Art. 82 DSGVO)

Es besteht bei jedem Verstoß gegen Rechte der betroffenen Person ein **Schadensersatzanspruch** gegen den Verantwortlichen für alle materiellen und immateriellen (!) Schäden, also **auch für „bloße“ Rufschädigung**.

Bußgeldrahmen bei Verstößen (Art. 83 DSGVO)

(Nur) **soweit Beteiligung am wirtschaftlichen Wettbewerb** (§ 20 Abs. 5 NDSG) und je nach Schwere des Verstoßes (jeder, auch ein kleiner kann bestraft werden!)

bis zu 10.000.000 Euro oder 2% des Jahresumsatzes weltweit

oder

bis zu 20.000.000 Euro oder 4% des Jahresumsatzes weltweit

Ordnungswidrigkeiten, Straftaten (§§ 59, 60 NDSG)

III. Tools für die Forschung

Laut der **Informationssicherheitsrichtlinie der Universität Göttingen (ISRL)** dürfen externe/kommerzielle Diensteanbieter grundsätzlich nicht genutzt werden.
Insbesondere dürfen **personenbezogene Daten nicht auf privaten Endgeräten oder in privaten Clouds gespeichert sein.**
Eine Dropbox ist hier ebensowenig geeignet wie die iCloud oder eine private Version von OneDrive. Vorzuziehen ist die OwnCloud der GWDG. In Ausnahmefällen können unter Vorlage eines schlüssigen Konzepts zur Datensicherheit Sondergenehmigungen beantragt werden. Mehr dazu im Vortrag von Herrn Dr. Beck am Mittwoch.
Auch eine Weiterleitung dienstlicher E-Mails an GMail und andere priv. Provider ist verboten.

IV. Internationale Forschungskooperationen

Bereits im Vorfeld eines Kooperationsvertrages ist der Datenschutz zu bedenken:
- Ist das Drittland sicher?
- Wie kann ein ausreichendes Datenschutzniveau beim Datentransfer in ein unsicheres Drittland ermöglicht werden?
- Welche Art von Vertrag liegt vor? Gemeinsame Verantwortlichkeit oder Auftragsverarbeitung?
- Wer ist federführend verantwortlich?

Kooperationsverträge sind der Abt. Wissenschaftsrecht und Trägerstiftung (Abt. 8) und dem (stellvertretenden) Datenschutzbeauftragten vorzulegen.

V. Repositorien

Zurverfügunghaltung für andere Forscher*innen ist Übermittlung von Daten
- Einwilligung der Betroffenen (ggf. *broad consent*) erforderlich
- Festgelegtes, strenges Antragsverfahren
- Aufbewahrungsdauer klären
- restriktives Rollen- und Rechtekonzept (need to know)
- gezielte Freischaltung der Daten
- nur für genau bestimmte Forschungsvorhaben Dritter (es müssen detaillierte Antragsverfahren für die Nutzung von Daten aus dem Repositorium vorangestellt werden)
- Differenzierung nach Rohdaten (besonders streng), pseudonymisierten und anonymisierten Daten (weniger streng)
- Differenzierung nach Schutzstufen, Bestimmung der TOMs
- Differenzierung nach dem Ort des Zugriffs (Deutschland, EU/EWR, Nicht-EU-Ausland)

- Anfrage beim jeweils zuständigen DSB erforderlich

VI. Vorgehensweise bei datenschutzrelevanten Forschungsprojekten/wissenschaftlichen Studien: Einreichung gem. Handreichung auf der DSB-Homepage

Vor Durchführung der Studie Einreichung beim Datenschutzbeauftragten:

- Angaben zum Studiendesign

- Datensicherungskonzept/technisch-organisatorische Maßnahmen

- Fragebogen [Datenminimierung? Privacy by Design/Default]

- Hinweisblatt Art. 13/14 (Homepage des Datenschutzbeauftragten)

- Einwilligungsbelehrung und -erklärung

- Ggf. Vertrag zur Auftragsdatenverarbeitung

Weitere Hinweise in der „Handreichung Wissenschaftliche Umfragen/Studien“ auf der Homepage des Datenschutzbeauftragten

Vielen Dank für Ihre Aufmerksamkeit!

Florian Hallaschka
Stellvertretender Datenschutzbeauftragter
der Georg-August-Universität Göttingen
(ohne Universitätsmedizin)
Goßlerstraße 5/7
37073 Göttingen
Tel.: +49-(0)551-39-24689
E-Mail: datenschutz@uni-goettingen.de
Homepage: https://www.uni-goettingen.de/de/576209.html