Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Forschungsvorhaben und Datenschutz

Institut für Politikwissenschaften

JGU Mainz

08.12.2022

AGENDA

1. Worum geht es überhaupt beim Datenschutz?
2. Was wird von diesem Grundrecht geschützt?
3. Erlaubnisse für die Verarbeitung personenbezogener Daten
4. Was versteht man unter „personenbezogenen Daten“ und deren „Verarbeitung“?
5. In welche verschiedenen Kategorien können personenbezogene Daten unterschieden werden?
6. Wie sind anonyme oder anonymisierte Daten abzugrenzen?
7. Die vor Beginn eines Forschungsprojekts zu stellende Frage
8. Informierte Einwilligung
9. Datenschutzerklärung
10. Cloud
11. Erhebung von Mail-Adressen und Import in SympaNewsletter-Mailingliste
12. Informationen

1. Worum geht es überhaupt beim Datenschutz?

Im Zusammenhang mit einer von der Bundesregierung in den 1980ziger Jahren geplanten Volkszählung (Zensus) hat sich das Bundesverfassungsgericht (BVerfG) mit den Voraussetzungen für die Datenerhebung zu statistischen Zwecken beschäftigt und ein Grundrecht auf informationelle Selbstbestimmung jeder natürlichen Person im sog. „Volkszählungsurteil“ vom 15.12.1983 entwickelt.

Das Grundrecht ist im Text des GG nicht ausdrücklich beschrieben, sondern wurde vom BVerfG aus der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) und der Menschenwürde (Art. 1 Abs. 1 GG) abgeleitet. Als Anlass dafür sah das BVerfG die zunehmende automatisierte Datenverarbeitung mit Computern und überhaupt moderner Technologie im Verhältnis zur bis dahin überwiegenden Speicherung in Papierakten und Karteien. Dadurch fällt es schwerer zu wissen, wer welche Daten von einem selbst wann und wofür verarbeitet.

BVerGE 65, 1 (43)

In einer Zeit der Digitalisierung ist die Gewährleistung des Grundrechts von immer größerer Bedeutung!

2. Was wird von diesem Grundrecht geschützt?

Das Recht jedes einzelnen, selbst über die Verarbeitung und Preisgabe seiner personenbezogenen Daten zu entscheiden. Das Datenschutzrecht schützt also nicht die personenbezogenen Daten an sich, sondern die natürlichen Personen, über welche die Daten Informationen enthalten.

Datenschutz kann auch als Schutz der Menschen vor Schäden oder Beeinträchtigungen definiert werden, die aus der Ansammlung und missbräuchlichen Verwendung von personenbezogenen Daten entstehen können.

In der Fachsprache wird das Grundrecht als „Verbot mit Erlaubnisvorbehalt“ bezeichnet. Das bedeutet, dass die Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, wenn sie nicht durch die betroffene Person oder sonst durch Gesetz erlaubt ist. Anders ausgedrückt sind personenbezogene Daten kein frei zugängliches Informationsmaterial, sondern jeder Zugriff ist eine Ausnahme, die begründet werden muss.

Denn jede Verarbeitung personenbezogener Daten stellt zunächst einmal ein Risiko für die Rechte und Freiheiten einer natürlichen Person dar.

BVerGE 65, 1 (42, 44)

3. Erlaubnisse für die Verarbeitung personenbezogener Daten

Art. 6 Abs. 1 S. 1 DS-GVO zählt solche Erlaubnisse auf.

Für Wissenschaft und Forschung besonders relevant sind

- Einwilligung – lit. a
- Wahrnehmung einer Aufgabe im öffentlichen Interesse – lit. e

also Datenverarbeitung auf der Grundlage einer Einwilligung oder eines Gesetzes

Beispiele für Wissenschaftsklauseln bzw. Rechtsvorschriften zur Verarbeitung personenbezogener Daten zum Zweck der Wissenschaft und Forschung sind Art. 6 Abs. 1 S. 1 lit. e i.V.m. Abs. 2, 3 i.V.m.

- § 22 Landesdatenschutzgesetz (LDSG) RP
- § 37 Landeskrankenhausgesetz (LKRG) RP

4. Was versteht man unter „personenbezogenen Daten“ und deren „Verarbeitung“?

Die maßgeblichen Definitionen sind zu finden in der für die Mitgliedstaaten der EU gültigen DS-GVO (Verordnung des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (……).

Laut Artikel 4 Nr. 1 und Nr. 2 dieser Verordnung bezeichnet der Ausdruck

„personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen;

„Verarbeitung“ jeden …. Vorgang …. im Zusammenhang mit personenbezogenen Daten wie das Erheben, die Speicherung, die Übermittlung, die Verknüpfung, das Löschen u.a.“

Die maßgebliche Definition der vor Inkrafttreten der DS-GVO gültigen Fassung des Landesdatenschutzgesetzes (LDSG) a.F. lautete:

„Personenbezogene Daten sind Einzelangaben über persönliche (z.B. Geschlecht, Alter) oder sachliche (z.B. Flurstück-Nummer bei Grundeigentum) Verhältnisse bestimmter oder bestimmbarer natürlicher Personen.“

5. In welche verschiedenen Kategorien können personenbezogene Daten unterschieden werden?
5.1 Direkt und indirekt identifizierende Daten

Personen können entweder direkt oder indirekt identifiziert werden. Für eine direkte Identifizierung sind eindeutige (bestimmte bzw. personenbezogene) Merkmale (wie Name, Adresse, Geburtsdatum, Sozialversicherungsnummer) nötig.

Personen können aber auch indirekt auf der Basis mehrerer (bestimmbarer bzw. personenbeziehbarer) Merkmale, die für sich genommen keine eindeutige Zuordnung zulassen, identifiziert werden.

Z. B. kann eine genaue und seltenere Berufsbezeichnung in Verbindung mit der Angabe des Geschlechts und des Wohnortes zur Identifizierung einer Person führen.

Zwei Beispiele:
Eine Schule möchte die Auswirkungen des Projekts „Bewegte Pause“ auf die Schüler:innen überprüfen. Alle sollen einen Fragebogen ausfüllen, aber auf keinen Fall den Namen angeben und den ausgefüllten Bogen in eine „Wahlurne“ einwerfen. Allerdings wird im Fragebogen u.a. nach dem Geschlecht, dem Gewicht und der Körpergröße gefragt. Was ist, wenn auch noch nach der Klassenstufe oder gar der Klassenbezeichnung gefragt wird?

Für die Evaluation von Unterrichtsmethoden werden mit einem Fragebogen zwar keine Namen, aber Daten wie Herkunftsland, Muttersprache oder Aufenthaltsdauer in Deutschland abgefragt.

Was ist wenn, eine PES-Lehrkraft der teilnehmenden Schule das Vorhaben durchführt und die ausgefüllten Fragebögen auswertet? Es würde sich um personenbeziehbare Daten handeln, für deren Verarbeitung eine Erlaubnis benötigt würde.

5. In welche verschiedenen Kategorien können personenbezogene Daten unterschieden werden?
5.1 Direkt und indirekt identifizierende Daten

Noch ein Beispiel:
In einer Gemeinde mit weniger als 500 Einwohnern wird zur Vorbereitung auf die Dorferneuerung mit einem Fragebogen der Name der Wohnstraße, die in einem Haushalt lebende Anzahl von Personen sowie deren Alter und ein in der Gemeinde ausgeübtes Gewerbe (Schreiner, Winzer, Landwirt) abgefragt.

Damit war es im Hinblick auf die Größe und Einwohnerzahl der Gemeinde alles andere als ausgeschlossen, dass auf der Basis dieser Merkmale, die für sich genommen keine eindeutige Zuordnung zulassen, und wahrscheinlich vorhandenem Zusatzwissen auf eine bestimmte Person geschlossen und ihr die Angaben im Fragebogen zugerechnet hätten werden können.

5. In welche verschiedenen Kategorien können personenbezogene Daten unterschieden werden?
5.2 Pseudonyme Daten

Die DS-GVO beschreibt „Pseudonymisierung“ in Art. 4 Nr. 5 DS-GVO folgendermaßen:

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.

Bei pseudonymen Daten handelt es sich also noch um personenbezogene Daten.

„Pseudonymisieren“ meint das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung einer Person auszuschließen oder wesentlich zu erschweren.

„Pseudonymisieren“ hat das Ziel, die unmittelbare Kenntnis der vollen Identität des Betroffenen während solcher Verarbeitungsvorgänge, bei denen ein Personenbezug nicht erforderlich ist, auszuschließen.

5. In welche verschiedenen Kategorien können personenbezogene Daten unterschieden werden?
5.2 Pseudonyme Daten

Folgendes Anwendungsbeispiel:

Eine Schule nimmt seit mehreren Jahren an einer wissenschaftlichen Studie teil, für die Informationen bzw. Einzelangaben über den Verlauf der Schullaufbahnen von Schüler:innen von der 5. bis zur 10. Klassenstufe zwecks wissenschaftlicher Analyse und Grundlage für bildungspolitische Entscheidungen erhoben und verarbeitet werden sollen.

In jedem Schuljahr müssen die teilnehmenden Schüler:innen mindestens einen Fragebogen ausfüllen. Der Fragebogen enthält nie den Namen, aber für eine bestimmte Schülerin bzw. einen bestimmten Schüler immer dieselbe Nummer, damit die Informationen über die Jahre immer derselben Person zugeordnet werden können.

Dafür wird in der Schule eine sog. Referenzliste geführt, in der die Schüler:innen mit Namen und Fragebogennummer aufgezählt werden. Ein ausgefüllter Fragebogen kann über die Nummer als Pseudonym nur mit Kenntnis dieser Liste wieder einer natürlichen Person zugeordnet werden. Für die Wissenschaftler enthalten die ausgefüllten Fragebögen somit nur pseudonyme Daten.

Bei einer Online-Befragung könnte die Einwilligung der daran teilnehmenden Personen aber bei einer entsprechenden vorherigen Information in dem Versenden eines ausgefüllten Fragebogens gesehen werden.

5. In welche verschiedenen Kategorien können personenbezogene Daten unterschieden werden?
5.3 Datenminimierung (Art. 5 Absatz 1 Buchstabe c) DS-GVO)
Das Gesetz verlangt, dass personenbezogene Daten gerade auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen. Auf das notwendige Maß ist die Datenverarbeitung dann beschränkt, wenn nur solche Daten verwendet werden, ohne die der Zweck der Verarbeitung nicht erreicht werden kann.

Wenn für einen bestimmten Zweck beispielsweise die Verarbeitung des Lebensalters ausreicht, darf nicht das vollständige Geburtsdatum verarbeitet werden.

Dieses Gebot erstreckt sich aber nicht nur auf die Menge der verarbeiteten Daten, sondern auch auf die Dauer der Zugänglichkeit. Die Beschränkung auf das notwendige Maß kann also zu einem bestimmten Zeitpunkt dazu führen, dass personenbezogene Daten zu pseudonymisieren, zu anonymisieren oder ganz zu löschen sind.

Typische Maßnahmen zur Gewährleistung der Datenminimierung:
Voreinstellungen in der Software oder Datenmasken, die die erforderlichen Datenfelder verbindlich vorgeben
Pseudonymisierungs- und Anonymisierungsverfahren; Pseudonymisierung verringert die Verknüpfbarkeit eines Datenbestands mit der Identität einer Person und stellt somit eine sinnvolle Sicherheitsmaßnahme dar.

Erwägungsgrund 39 zur DS-GVO

6. Wie grenzt man personenbezogene von anonymen oder anonymisierten Daten ab?

Der Ausdruck „Anonymisieren“ bezeichnet das Verändern personenbezogener Daten dergestalt, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Einzelangaben können auch schon anonym, also ohne Bezug zu einer bestimmten oder bestimmbaren Person, erhoben werden.

Zum anderen können personenbezogen erhobene Daten später anonymisiert werden, d.h. der Bezug zu einer Person wird z.B. dadurch aufgehoben, dass in einem Datensatz die identifizierenden Daten gelöscht werden.

Anonym erhobene bzw. im Verlauf der weiteren Datenverarbeitung anonymisierte Daten unterliegen nicht dem Datenschutzrecht. Datenschutzrechtliche Nutzungsbeschränkungen bestehen für solche Daten nicht (vgl. Erwägungsgründe 26, 28 zur DS-GVO).

6. Wie grenzt man personenbezogene von anonymen oder anonymisierten Daten ab?

Das Weglassen des Namens oder der Anschrift als unmittelbar identifizierende Daten und die lediglich unvollständige Speicherung der IP-Adresse (sog. personenbeziehbares Datum) reicht mitunter nicht aus, um eine Anonymität zu erreichen.

Die Zuordnung einer Einzelangabe zu einer betroffenen Person muss aber auch nicht schlechthin ausgeschlossen sein, sondern es genügt für eine erfolgreiche Anonymisierung, wenn eine Zuordnung bzw. eine Identifizierung einer natürlichen Person anhand der vorhandenen Daten nach der Lebenserfahrung nicht zu erwarten ist.

Zur Beantwortung der Frage, ob trotz erhobener personenbeziehbarer Daten von anonymen Daten auszugehen ist, muss eine Analyse des Risikos für eine Re-Identifizierung im Einzelfall erfolgen.

Anonymität ist letztlich eine Frage der Wahrscheinlichkeit.

7. Die vor Beginn eines Forschungsprojekts zu stellende Frage

Schon das BVerfG hat in dem oben erwähnten „Volkszählungsurteil“ ausgeführt, dass immer zu prüfen ist, ob das Ziel einer Datenerhebung nicht auch durch anonymisierte Ermittlung erreicht werden kann und wenn dies nicht möglich ist, die Verarbeitung personenbezogener Daten sich auf das erforderliche Minimum zu beschränken hat.

Kann der Zweck der Forschung mit verhältnismäßigem Aufwand auch mit ausschließlich anonymen Daten erreicht werden?

Einzelangaben können anonym, also ohne Bezug zu einer bestimmten oder bestimmbaren Person, erhoben werden.

Unterscheidung zwischen Querschnitt- und Längsschnittstudie mit mehreren Messzeitpunkten, Follow Up-Erhebung

Zunächst personenbezogen erhobene Daten können später anonymisiert werden, d.h. der Bezug zu einer Person wird z.B. dadurch aufgehoben, dass in einem Datensatz die identifizierenden Daten gelöscht werden.

8. Informierte Einwilligung

Kerninhalte einer Information finden sich in den Erwägungsgründen 32 und 42 zur DS-GVO

Grundsätzlich gilt, dass für eine wirksame Einwilligung die betroffenen Personen über Rechte nach Art. 13 Abs. 2 lit. b bis d DS-GVO und über die wesentlichen Modalitäten der vorgesehenen Datenverarbeitung aufzuklären sind.

Nur wer hinreichend abschätzen kann, welche Folgen die Erteilung oder Nichterteilung einer Einwilligung für ihn haben wird, kann selbstbestimmt darüber entscheiden, ob er der Erhebung und Verwendung seiner Daten zustimmt.

Zu folgenden Fragen müssen die Betroffenen im Einzelnen aufgeklärt werden, damit sie in der Lage sind abzuschätzen, in was sie mit der Teilnahme an einem Projekt im Hinblick auf die Datenverarbeitung einwilligen:

Welchem Zweck dient die Datenverarbeitung? Welche Instrumente werden eingesetzt (Fragebogen, Interview, Test, Video)
Wer ist verantwortlich, wie erfolgt die Durchführung der Umfrage?
Ist die Befragung anonym oder personenbeziehbar?
Wie wird ggf. die Anonymität gewährleistet?
Wer erhält ggf. Kenntnis bzw. Zugang zu personenbezogenen Daten?
Werden Daten an Dritte übermittelt oder veröffentlicht?
Wann werden die Daten gelöscht?

9. Datenschutzerklärung

Der Begriff wird regelmäßig im Zusammenhang mit der Internetpräsenz eines Verantwortlichen und der dort angebotenen eigenen Inhalte verwendet.

Beispiel für die Bestandteile einer Datenschutzerklärung zum Internet-Angebot des LfDI

https://www.datenschutz.rlp.de/de/datenschutzerklaerung/

Die Datenschutzerklärung dient der Information der betroffenen Person. Sie soll Transparenz darüber herstellen, dass und in welchem Umfang personenbezogene Daten verarbeitet werden oder künftig noch verarbeitet werden sollen. Insofern schaffen diese Informationen die Grundlage, dass die betroffene Person von ihren Rechten Gebrauch machen kann.

Letztlich geht es um die Information gemäß Art. 13 DS-GVO

10. Speicherung von zum Zweck der Forschung erhobenen personenbezogenen Daten in einer Cloud

Falls personenbezogene Daten auf der Grundlage einer Einwilligung verarbeitet werden sollen, sollte auf die Datenspeicherung in einer Cloud in der Information eingegangen werden.

Allgemeine Informationen zur Nutzung eines Cloud-Speichers finden Sie unter

https://www.datenschutz.rlp.de/de/themenfelder-themen/cloud-speicher-sicher-nutzen/

Wegen der sich aus dem EuGH-Urteil in der Rechtssache Schrems II vom 16. Juli 2020 ergebenden Schwierigkeiten ist ein deutscher oder europäischer Anbieter vorzugswürdig.

Zusätzliche Informationen finden Sie unter

https://www.datenschutz.rlp.de/de/themenfelder-themen/schrems-ii/

im Internet-Angebot des Landesbeauftragten.

Seafile mit der JGU als Verantwortlichem ist daher vorzugswürdig.

11. Erhebung von Mail-Adressen und Import in SympaNewsletter-Mailingliste

Darf ich Mailadressen, die ich in einer Umfrage erhebe, ohne Weiteres in einen solchen Mail-Verteiler importieren?

Die Daten müssten dazu lokal auf meinem Computer (zwischen)gespeichert werden.

Eine Mailadresse kann als personenbezogenes Datum gelten. Im Falle einer informierten Einwilligung ist die Übernahme in einen Verteiler und eine Kontaktaufnahme für andere Zwecke möglich.

https://lists.uni-mainz.de/sympa/

Auflistung der an der Uni Mainz verfügbaren Mailinglisten:
https://lists.uni-mainz.de//sympa/lists
Man kann auf die vermeintlichen Mailadressen klicken und erhält dann weitere Infos zu dieser Gruppe/Liste

Erklärung von Sympa Funktionen an der Uni Mainz:
https://lists.uni-mainz.de/sympa/help/introduction-features.html

12. Weitere Informationen gibt‘s in bzw. unter

Bundesverfassungsgericht, Entscheidungsband 65, 1

Landesdatenschutzgesetz Rheinland-Pfalz – Handkommentar, Hrsg. Prof. Dr. Dieter Kugelmann**;** *1. Auflage 2020, Nomos-Verlag*

https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/ChecklisteWissenschaftlicheUntersuchungen.pdf

Auch der Hessische Beauftragte für den Datenschutz bietet eine Hilfestellung an: „Datenschutzkonzepte für akademische Abschlussarbeiten oder Promotionsvorhaben“

https://www.bmj.de/DE/Themen/FokusThemen/DSGVO/DSVGO_node.html

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Michael Smolle

Bereichsleiter

beim Landesbeauftragten für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

Postanschrift: Postfach 30 40
55020 Mainz

Büroanschrift: Hintere Bleiche 34
55116 Mainz

Telefon: +49 (6131) 208-220
Telefax: +49 (6131) 208-2497

E-Mail: m.smolle@datenschutz.rlp.de

Web: www.datenschutz.rlp.de