Datenschutzrechtlicher Leitfaden für Studierende

zur Erstellung von

Bachelor-, Diplom- und Masterarbeiten sowie Dissertationen

Die Erstellung wissenschaftlicher Arbeiten ist regelmäßig mit der Verarbeitung personenbezogener Daten verknüpft. Daher sind dabei jedenfalls die Bestimmungen der Datenschutz-Grundverordnung (DSGVO) und des Datenschutzgesetzes (DSG) zu beachten. Daneben gelangt das Universitätsgesetz (UG) und ev das Forschungsorganisationsgesetz (FOG) zur Anwendung.

Handelt es sich allerdings um anonyme Daten (dh Daten ohne Personenbezug), dann sind keine weiteren Maßnahmen aus datenschutzrechtlicher Sicht erforderlich.

Begriffsbestimmung

Eine exakte Definition der im Datenschutz verwendeten Begriffe findet sich in Art 4 (DSGVO). Als wichtigste sind hier zusammengefasst hervorzuheben:

- **personenbezogene Daten:** alle Informationen, die sich auf bestimmte Personen zurückführen lassen (zB Name, Geburtsdatum, Adresse, E-Mail-Adresse, Bild, Fingerabdrücke). Es muss noch eine Identifizierung möglich sein – daher sind auch pseudonymisierte Daten weiterhin personenbezogene Daten, denn sie lassen sich mittels Pseudonym noch immer auf eine bestimmte Person zurückführen. Nur wenn eine Identifizierung gar nicht mehr möglich ist, liegt eine vollständige Anonymisierung vor – und die DSGVO ist nicht anwendbar. Besonderen Schutz genießen sog „sensible Daten“ (zB Gesundheitsdaten, Daten über politische Meinungen oder religiöse Überzeugungen)
- **Datenverarbeitung**: jeder Vorgang, der im Zusammenhang mit personenbezogenen Daten steht. Hierzu zählen Erfassen, Speichern, Lesen, Verwenden, Verändern, Weiterleiten, Abfragen, Offenlegen, Löschen etc
- **Datenverarbeiter_in**: jede_r, die_der Daten verarbeitet
- **Betroffene_r**: natürliche Person, deren Daten verarbeitet werden
- **Verantwortliche_r**: die_derjenige, die_der (allein oder gemeinsam mit andren) darüber entscheiden, ob, wie und für welchen Zweck bestimmte personenbezogene Daten verarbeitet werden

Rechtsgrundlage der Verarbeitung

Die Rechtsgrundlage zur Verarbeitung personenbezogener Daten für die Erstellung von Bachelor-/Diplom-/Masterarbeiten/Dissertationen stellen Art 6 Abs 1 lit c DSGVO iVm § 80ff UG dar.

Art 6 Abs 1 lit c DSGVO normiert die Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung, der die_der Verantwortliche unterliegt.

§§ 80ff UG stellen die rechtliche Verpflichtung dar. Es wird je nach Art der wissenschaftlichen Arbeit unterschieden:

- § 80 UG betrifft die Bachelorarbeit (Art 6 Abs 1 lit c DSGVO iVm § 80 UG);
- § 81 UG betrifft Diplom- und Masterarbeiten (Art 6 Abs 1 lit c DSGVO iVm § 81 UG);
- § 83 UG betrifft Dissertationen (Art 6 Abs 1 lit c DSGVO iVm § 83 UG)

➔ Fazit

Die Verarbeitung personenbezogener Daten im Rahmen des Verfassens wissenschaftlicher Arbeiten ist (datenschutz-) rechtlich zulässig. Die Verarbeitung stützt sich auf die gesetzlichen Bestimmungen, die die Erstellung einer wissenschaftlichen Arbeit im Rahmen eines Studiums notwendig machen. Die datenschutzrechtliche Rechtfertigung für die Verarbeitung personenbezogener Daten ist nicht die Einwilligung der Betroffenen.

Achtung: Wird die Bachelor-/Diplom-/Masterarbeit/Dissertation als Auftragsarbeit oder in Zusammenarbeit mit Dritten (zB einem bestimmten Unternehmen) erstellt, kann die Datenverarbeitung uU auf anderen rechtlichen Grundlagen beruhen.

Verantwortliche

Das Datenschutzrecht kennt Rollenverteilungen. Werden Daten nur „im Auftrag“ und nach Weisung anderer verarbeitet, handelt es sich um eine „Datenverarbeitung im Auftrag“ gemäß Art 28 DSGVO. Werden Daten „gemeinsam“ mit einem oder mehreren anderen verarbeitet, spricht man von „gemeinsam Verantwortliche“ im Sinne von Art 26 DSGVO. Beide „Varianten“ erfordern entsprechende Vereinbarungen zwischen den Partner_innen, in welchen die Grundlagen der Zusammenarbeit betreffend Datenschutz ausdrücklich geklärt werden müssen. Als weitere Möglichkeit kennt das Datenschutzrecht die Datenverarbeitung durch mehrere, eigenständige Kooperationspartner_innen für einen jeweils eigenen Zweck (weder im fremden, noch im gemeinsamen Interesse). Weder gibt es eine_einen Partner_in, der genau bestimmt und beschränkt, wie die Daten zu verarbeiten sind, noch wird gemeinsam über die Datenverarbeitung entschieden. Die Kooperationspartner_innen entscheiden jeweils eigenständig über die Verarbeitung. Es liegen jeweils „eigene Verantwortungen“ vor (auch wenn dieselben Daten verarbeitet dh verwendet werden).

Bei der Erstellung einer Bachelor-, Diplom- oder Masterarbeit sowie bei Dissertationen arbeitet die_der Studierende eigenverantwortlich – vor allem was die Verwendung der erforderlichen Mittel und Daten betrifft. Die_der Studierende, die_der entscheidet, wie die Daten verwendet werden, ist für die Wahrung der Datensicherheit und der Betroffenenrechte (wie zB Informationspflicht – siehe unten) verantwortlich und dient als Ansprechpartner_in für die Betroffenen.

➔ Fazit

Studierende sind bei der Erstellung ihrer akademischen Arbeiten als Verantwortliche zu qualifizieren und sind daher selbst für die Einhaltung der (daten-) schutzrechtlichen Rahmenbedingungen verantwortlich.

Informationspflicht

Bei jeder Verarbeitung von personenbezogenen Daten müssen die Betroffenen über die beabsichtigte Datenverwendung umfassend informiert werden. Die TU Wien stellt Studierenden dazu ein Muster-Schreiben „Information zur Erhebung und Verarbeitung von personenbezogenen Daten“ zur Verfügung. Dieses Muster erhebt keinen Anspruch auf Richtigkeit und Vollständigkeit und die TU Wien übernimmt keine Haftung bei der Verwendung des Musters – siehe dazu „Verantwortlichkeiten“. Das Muster-Schreiben muss für den Einzelfall individuell angepasst und ergänzt werden (gelb markierte Stellen).

➔ Fazit

Als Verantwortliche im Sinne der DSGVO sind Studierende verpflichtet, für die Erfüllung der Informationspflicht Sorge zu tragen. Es empfiehlt sich daher, sich auf den eigenen Unterlagen den Empfang des Informationsschreibens durch die_den Betroffenen bestätigen zu lassen, um gegebenenfalls auch nachweisen zu können, dass der Informationspflicht nachgekommen wurde.

Alternativ könnte dieser Nachweis auch in Form einer Check-Liste oä erbracht werden, in welcher die Check-Box „DSGVO-Information erteilt“ bei Erfüllung des Kriteriums entsprechend gekennzeichnet wird.

Sonstige Betroffenenrechte

Als Verantwortliche stehen die Studierenden auch betreffend der sonstigen Betroffenenrechte in der Pflicht. Dazu zählen

- Recht auf **Auskunft** über die betreffenden personenbezogenen Daten (Art 15 DSGVO)
- Recht auf **Berichtigung** (Art 16 DSGVO) oder **Löschung** (Art 17 DSGVO) oder auf **Einschränkung**

der Verarbeitung (Art 18 DSGVO) unter den in den angeführten Bestimmungen beschriebenen Voraussetzungen

- Recht auf **Beschwerde**, welche bei der Österreichischen Datenschutzbehörde, Barichgasse 40-42, 1030 Wien, Telefon: +43 1 52 152-0, E-Mail: dsb@dsb.gv.at als zuständige Aufsichtsbehörde einzubringen ist.

Weitere – hier nicht anwendbare – Rechte der Betroffenen:

- Recht auf Widerruf einer allenfalls erteilten Einwilligung
- Recht auf Widerspruch gegen die Datenverarbeitung
- Recht auf Datenübertragbarkeit (Art 20 DSGVO), sofern die bezughabende Datenverarbeitung auf einer Einwilligung oder Vertragserfüllung beruht und mit Hilfe automatisierter Verfahren erfolgt - soweit technisch machbar

Art 11 DSGVO sieht zudem vor, dass eine separate Rückführbarkeit von Daten auf Personen nicht gewährleistet werden muss, nur um die Betroffenenrechte wahren zu können.

➔ Fazit

Als Verantwortliche im Sinne der DSGVO sind Studierende verpflichtet, für die Erfüllung der Betroffenenrechte Sorge zu tragen.

Datensicherheit

Das Datenschutzrecht sieht jedenfalls vor, dass bei der Verarbeitung personenbezogene Daten geeignete technische und organisatorische Schutzmaßnahmen zu beachten sind. Diese zu ergreifen ist die Aufgabe der_des Verantwortlichen.

➔ Fazit

Als Verantwortliche im Sinne der DSGVO sind Studierende verpflichtet, für die Sicherheit der verarbeiteten Daten Sorge zu tragen. Insbesondere zu erwähnen ist:

- **Vertraulicher Umgang** mit personenbezogenen, verarbeiteten Daten, soweit möglich (kein Informationsaustausch via soziale Medien oder sonst in der Öffentlichkeit, Vorsicht bei der Verwendung von öffentlichen WLANs)
- **Sichere Aufbewahrung** der personenbezogenen verarbeiteten Daten
- Keine Speicherung der Daten **außerhalb des EU/EWR-Raumes**
- Schutz der Daten vor unberechtigtem Zutritt/Zugang/Zugriff (Passwort, sorgsamer Umgang mit externen Speichermedien)
- **Datenminimierung** dh auf das notwendige Maß der erforderlichen Daten beschränken
- **Löschen** der personenbezogenen Daten nach der vereinbarten Aufbewahrungsdauer. Löschen meint die physischer Vernichtung (zB mittels Shredder) - ein Verschieben von Daten in den Papierkorb oder eine Ablage von Papierunterlagen im „normalen“ Altpapier reicht jedenfalls nicht aus. Löschen des Speichers im allenfalls verwendeten Aufnahmegerät (das gilt insbesondere für Leihgeräte vor Retournierung an die entlehnende Stelle)
- Die **Speicherdauer** beträgt für Daten und Forschungsmaterial bis zu 30 Jahre (§ 2f Abs 3 FOG)

Wir wünschen viel Erfolg und gutes Gelingen!

ToDo – Datenschutz step-by-step

Eine Anleitung für die Erstellung von Bachelor-/Diplom-/Masterarbeiten/Dissertationen.

1.) Welche Daten werden benötigt?

Handelt es sich um Daten mit Personenbezug oder liegen lediglich anonyme Daten vor?

- ✓ Anonyme Daten: keine weiteren Maßnahmen aus datenschutzrechtlicher Sicht erforderlich
- ✓ Personenbezogene Daten: Datenschutzmaßnahmen erforderlich

2.) Adaptierung des bereitgestellten „Informationsblatts" entsprechend der geplanten Datenerhebung

a.) Welche Daten werden genau erhoben? – Anführung im Informationsblatt unter Punkt „Art der verarbeiteten personenbezogenen Daten"

Werden auch sensible Daten erhoben? Das sind:

- ✓ Gesundheitsdaten
- ✓ Daten zur rassischen oder ethnischen Herkunft
- ✓ politische Meinung
- ✓ religiöse oder weltanschauliche Überzeugung
- ✓ Gewerkschaftszugehörigkeit
- ✓ genetische oder biometrische Daten
- ✓ Daten zu Sexualleben oder sexueller Orientierung

Falls ja – Aktivierung des/der bezughabenden Feldes/Felder, im Informationsblatt unter Punkt „Art der verarbeiteten personenbezogenen Daten" („besondere Datenkategorien")

b.) Warum werden die Daten erhoben? – Ergänzung des Informationsblatts unter Punkt „Zweck der Datenverarbeitung"

c.) Wie werden die Daten erhoben? - Ergänzung des Informationsblatts unter Punkt „Beschreibung der Datenverarbeitung"

d.) Wer wird die erhobenen Daten noch sehen, erhalten? - Ergänzung des Informationsblatts unter Punkt „Übermittlungsempfänger_innen und Drittstaatenübermittlungen"

e.) Anführen der eigenen Kontaktinformationen im Informationsblatt unter Punkt „Verantwortlicher/r" und „Kontaktdaten"

3.) Pseudonymisierung als Datenschutzmaßnahmen

Bei der **Pseudonymisierung** wird der Name und andere, vorhandene Identifikationsmerkmale (zB Geburtsdatum) durch ein Pseudonym (zB Buchstaben- oder Zahlenkombination oder eine andere Bezeichnung „Kandidat A", „Interviewpartner 1" etc) ersetzt, um die Feststellung der Identität der Betroffenen zu verhindern.

Anonymisierung hingegen bedeutet, personenbezogener Daten derart zu verändern, dass diese Daten einer Person gar nicht (mehr) zugeordnet werden können (auch nicht über einen „Decodierungs-Schlüssel").

Die Pseudonymisierung ermöglicht also – unter Zuhilfenahme eines Schlüssels – die Zuordnung von Daten zu einer Person, was ohne diesen Schlüssel nicht (mehr) möglich ist. Entscheidend ist also, ob eine Zusammenführung von Person und Daten noch möglich ist. Nicht verhindert, sondern lediglich erschwert ist die Identitätsfeststellung, wenn als Kennzeichen zB Initialen und Geburtsdatum verwendet werden. Dies ist als Pseudonymisierungsmaßnahme nicht hinreichend.
Je aussagekräftiger die Datenansammlung ist (zB Einkommen, Krankheitsgeschichte, Wohnort, Größe), desto größer ist die theoretische Möglichkeit, diese auch ohne Schlüssel einer bestimmten Person zuzuordnen und diese identifizieren zu können. Für eine wirksame Pseudonymisierung reicht es dann unter Umständen nicht aus, nur den Namen durch ein Pseudonym zu ersetzen – sondern auch die ergänzenden Daten zu pseudonymisieren oder zu kategorisieren (zB Altersgruppe 20-30 Jahre), um die ungewollte Identitätsfeststellung zu vermeiden.

Beispiele:

A.) Möchten Studierende die Daten Ihrer Erhebungen unter Bezugnahme auf eine_n bestimmte_n Interviewpartner_in in Ihren Arbeiten einfließen lassen, so ist diese_r in der Arbeit nur mit einem bestimmten Pseudonym (zB IP [Interviewpartner] Nr. 89) zu benennen. Über die eigenen Unterlagen (den „Schlüssel“) kann dieses Pseudonym im Bedarfsfall einer bestimmten, interviewten Person zugeordnet werden (Max Mustermann, geb. 1.1.9999, Größe: X, Beruf: Datenschützer). Für Dritte ist eine Identifizierung nicht möglich.
✓ wirksame Pseudonymisierung

B.) Wird neben dem Pseudonym (IP 89) ein weiteres Merkmal genannt (Geburtsdatum) ist die Wahrscheinlichkeit einer Decodierung durch Dritte (auch ohne Besitz des „Schlüssels“) sehr wahrscheinlich.
X unwirksame Pseudonymisierung

C.) Hier könnte zB durch Erstellung von Alterskategorien Abhilfe geschaffen werden: IP 89, Alterskategorie 40-50 Jahre
✓ wirksame Pseudonymisierung

D.) Wird der Schlüssel vernichtet, sodass die Rückführbarkeit auf eine bestimmte natürliche Person (auf eine_n bestimmten Interviewpartner_in) unmöglich ist, liegt eine Anonymisierung vor. Anonyme Daten unterliegen nicht (mehr) dem Datenschutz. Die (anonymen) Daten selbst können weiterhin verwendet werden.

E.) Die (geheime) Abstimmung bei Wahlen beruht auf dem Prinzip der Anonymisierung (Wahlgeheimnis). Es ist zwar noch nachvollziehbar, wer gewählt hat, aber eine Zuordnung zwischen Wahlzettel und Wähler ist nicht mehr möglich.

4.) Wie kann ich gewährleisten, dass die erhobenen Daten sicher aufbewahrt werden?

- ✓ Sichern Sie verwendete PCs/Laptops und sonstige Devices mit einem Passwort
- ✓ Seien Sie sorgsam mit den verwendeten Unterlagen (in Papierform) wie auch den elektronischen Speichermedien (USB-Sticks, Laptops)
- ✓ Versuchen Sie eine Speicherung in Clouds (insbesondere von Anbietern außerhalb des EU/EWR-Raumes) zu vermeiden
- ✓ Tauschen Sie sich nicht über die interviewten Personen unter Namensnennung aus – weder schriftlich in sozialen Medien, noch in Gesprächen in der Öffentlichkeit
- ✓ Achten Sie die Privatsphäre der interviewten Personen so, wie Sie Ihre eigene Privatsphäre geschützt wissen wollen
- ✓ In dem bereitgestellten Informationsblatt wird eine Aufbewahrungsdauer von 30 Jahren empfohlen. Löschen Sie die personenbezogenen Daten nach der vereinbarten Aufbewahrungsdauer. Dies bezieht sich auf Unterlagen in Papierform wie auch auf elektronischen Medien. Löschen meint die physische Vernichtung (zB mittels Shredder) - ein Verschieben von Daten in den Papierkorb oder eine Ablage von Papierunterlagen im „normalen“ Altpapier reicht jedenfalls nicht aus. Löschen des Speichers im allenfalls verwendeten Aufnahmegerät (das gilt insbesondere für Leihgeräte vor Retournierung an die entlehnende Stelle)