



DATENSCHUTZ – LEITFADEN FÜR ABSCHLUSSARBEITEN VON STUDIERENDEN

ÖPUK - AG Datenschutz

in Form von

FAQs und Antworten



Quelle: Pixabay (FAQ) – freie kommerzielle Nutzung, kein Bildnachweis

Hinweis und Haftungsausschluss: Der vorliegende Leitfaden entstand im Rahmen der Arbeitsgruppe AG Datenschutz der Österreichischen Privatuniversitätenkonferenz (ÖPUK, AG Datenschutz) und soll Studierenden an Privatuniversitäten eine Hilfestellung im Umgang mit Daten geben, welche für Abschlussarbeiten verarbeitet werden. Die in diesem Leitfaden dargestellten Inhalte verstehen sich als Orientierungshilfe und werden ohne Gewähr bereitgestellt. Es wird seitens der Autorinnen/Autoren keine Haftung oder Gewähr übernommen, insbesondere nicht für Aktualität oder Vollständigkeit von Inhalten.

Impressum, Herausgeber, Copyright:

ÖPUK, AG Datenschutz

Autorinnen/Autoren (in alphabetischer Reihenfolge):

Johann Fels, Johanna Fischer, Nadja Hubmann, Margit Kranawetter, Daniela Megyesi, Verena Stühlinger,

Horst Treiblmaier, Helmut Zacher

Review (in alphabetischer Reihenfolge):

Mirela Imsirovic, Andrea Kolberger



1. Was bedeutet Datenschutz und was ist die DSGVO?

Unter Datenschutz versteht man den Schutz personenbezogener Daten vor Missbrauch, oft im Zusammenhang auch mit dem Schutz der Privatsphäre. Zweck und Ziel im Datenschutz ist die Sicherung des Grundrechts auf informationelle Selbstbestimmung der Einzelperson.

Jeder soll selbst bestimmen können, wem er wann welche seiner Daten und zu welchem Zweck zugänglich macht.

DSGVO ist die geläufige Abkürzung für die Datenschutz-Grundverordnung. Damit setzt die EU einen einheitlichen Rechtsrahmen für die Verarbeitung und Speicherung personenbezogener Daten. Heißt konkret: Unternehmen haben erhöhte Dokumentationspflichten. Sie müssen jederzeit in der Lage sein, die Rechtmäßigkeit ihrer Datenverarbeitungstätigkeiten gegenüber Aufsichtsbehörden nachzuweisen. Gewisse Pflichten können aber auch Studierende treffen, die im Rahmen ihrer Abschlussarbeit Daten Dritter verarbeiten.

2. Warum ist Datenschutz für meine Abschlussarbeit relevant?

Personenbezogene Daten gehören grundsätzlich immer der Person selbst. Behalten Sie dies beim Verfassen einer Abschlussarbeit stets im Fokus. Konkret heißt dies, dass personenbezogene Daten von Dritten, die z.B. im Rahmen von Interviews erhoben werden, ausschließlich unter Beachtung der rechtlichen Rahmenbedingungen verarbeitet werden dürfen. Handelt es sich hingegen um anonyme Daten (d.h. Daten ohne Personenbezug), dann sind keine weiteren Maßnahmen aus datenschutzrechtlicher Sicht erforderlich.

Die Erstellung wissenschaftlicher Arbeiten ist allerdings häufig mit der Verarbeitung personenbezogener Daten verknüpft. In so einem Fall sind jedenfalls die Bestimmungen der Datenschutz-Grundverordnung (DSGVO) und des Datenschutzgesetzes (DSG) zu beachten. Daneben gelangt das Universitätsgesetz (UG) und eventuell das Forschungsorganisationsgesetz (FOG) zur Anwendung.

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

Es gibt allerdings zwei Fälle, für die besondere Bestimmungen zur Anwendung gelangen. In diesen Anwendungsfällen steht Ihr(e) BetreuerIn für weitere Informationen zur Verfügung:

- a) Die Abschlussarbeit wird unter Beteiligung einer Ethikkommission verfasst (z.B. weil vulnerable Personengruppen eingeschlossen werden). In diesem Fall erfolgt die Datenerhebung aufgrund anderer rechtlicher Grundlagen (zumeist der Einwilligung der Betroffenen).
- b) Die Abschlussarbeit wird als Auftragsarbeit oder in Zusammenarbeit mit Dritten (z.B. einem bestimmten Unternehmen) erstellt. Auch hier unterliegt die Datenverarbeitung anderen rechtlichen Grundlagen.



3. Bin ich verantwortlich für Daten, die ich für die Abschlussarbeit erhebe und was bedeutet das?

Um die Verantwortung für Datenverarbeitungen klar zuzuteilen kennt das Datenschutzrecht Rollenverteilungen. Die Person, die die Verantwortung für die Sicherheit von Daten trägt, weil sie über Zwecke (z.B. Abschlussarbeit) und Mittel (z.B.: mein privater Computer) einer Verarbeitung entscheidet, heißt "Verantwortlicher" (Art. 4 Z 7 DSGVO).

Wenn im Rahmen von Abschlussarbeiten personenbezogene Daten verarbeitet werden, entscheiden idR Studierende selbst über die Mittel der Verarbeitung: z.B.: es wird der eigene Computer zur systematischen Erfassung von Erhebungsdaten verwendet oder ein Interview wird mit dem eigenen Smartphone aufgezeichnet bevor es transkribiert wird. In diesem Fall sind Studierende selbst "Verantwortliche" im Sinne der DSGVO. Das bedeutet, dass sie gegenüber Personen, deren Daten sie verarbeiten (= Betroffene) Informationspflichten trifft und sie für die Sicherheit der Daten Sorge tragen müssen (vgl. FAQ 7 und 11).

Wenn Studierende zur Verfassung der Abschlussarbeit eine Anstellung an einer Universität im Rahmen eines Forschungsprojekts erhalten, kann die Verantwortung für die Verarbeitung der Daten bei der Einrichtung selbst liegen. Indizien hierfür sind z.B., dass Erhebungsdaten am Server der Institution gespeichert werden und somit die Universität selbst über die Mittel der Verarbeitung entscheidet.

4. Was sind personenbezogene Daten?

Ob Daten dem Datenschutz unterliegen, hängt davon ab, ob es sich um personenbezogene Daten nach der Datenschutz-Grundverordnung (DSGVO) handelt oder nicht. Personenbezogene Daten sind daher ein Kernbegriff des Datenschutzes. Der Begriff der „personenbezogenen Daten“ ist gesetzlich definiert als „Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“.

Als identifizierbar bezeichnet die DSGVO eine natürliche Person, „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Somit sind personenbezogene Daten alle jene Daten, mit denen man eine natürliche Person in irgendeiner Form identifizieren kann.

Personenbezogene Daten werden sehr weit ausgelegt. Vom Datenschutz umfasst sind „alle Informationen“, die sich direkt oder indirekt auf eine Person beziehen. Beispielsweise zählen dazu Name, Adresse, Geburtsdatum, E-Mail-Adresse, Telefonnummer, Kennnummern, IP-Adresse, bis hin zu körperlichen Merkmalen und persönlichen Einstellungen. Auch ein Foto oder Fingerabdruck (biometrische Daten) fallen darunter.

5. Was sind besondere Kategorien personenbezogener Daten?



Gem. Art. 9 Abs. 1 DSGVO handelt es sich bei den besonderen Kategorien personenbezogener Daten um Daten, aus denen die

- rassistische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie um die Verarbeitung von
- genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. [Genetische Daten sind solche, die die ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person enthalten (Art. 4 Abs. 13 DSGVO). Biometrische Daten sind die physischen, physiologischen oder verhaltenstypischen Merkmale einer natürlichen Person, die mit speziellen technischen Verfahren gewonnen wurden (gem. Art. 4 Abs. 14 DSGVO).]

Grundsätzlich ist die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO untersagt. Eine Reihe von Ausnahmen, nach denen die Verarbeitung besonderer Kategorien personenbezogener Daten wiederum gestattet ist, finden sich in Art. 9 Abs. 2 lit. a-j DSGVO. Danach ist die Verarbeitung besonderer Kategorien personenbezogener Daten u.a. dann zulässig, wenn die betroffene Person in die Verarbeitung ausdrücklich eingewilligt hat. Als Einwilligung der betroffenen Person gilt jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Diese Einwilligung kann schriftlich, elektronisch oder auch mündlich erfolgen und muss im jeweiligen Kontext eindeutig das Einverständnis der betroffenen Person zur Datenverarbeitung signalisieren. Stillschweigen, bereits vorangekreuzte Kästchen oder Untätigkeit können keine Einwilligung darstellen. Wenn die Verarbeitung mehreren Zwecken dient, ist für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig. Bei besonderen Kategorien personenbezogener Daten ist eine ausdrückliche Einwilligung erforderlich.

6. Welche Folgen hat das für meine Abschlussarbeit, wenn ich personenbezogene Daten verarbeite?

Bei jeder Verarbeitung von personenbezogenen Daten müssen die Betroffenen über die beabsichtigte Datenverwendung umfassend informiert werden. Darunter fällt u.a. die Information welche Daten genau (z.B. Adressdaten), zu welchem Zweck und auf Basis welcher Rechtsgrundlage (z.B. Gesetz, Einwilligung) gespeichert und verarbeitet werden, ob die Daten auch an Dritte weitergegeben (wenn ja an wen) und wie lange diese gespeichert werden.

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



Stützt sich eine Datenverarbeitung auf eine gesetzliche Basis, entfällt die Einholung einer Einwilligung zur Datenverarbeitung bei den Betroffenen (z.B. InterviewpartnerInnen). Die Information ist in diesen Fällen ausreichend.

Ist keine gesetzliche Grundlage vorhanden, ist zusätzlich zur Information eine Einwilligung der/des Betroffenen einzuholen. In der Einverständniserklärung ist anzuführen welche Daten zu welchem Zweck an welchem Ort gespeichert und verarbeitet werden.

7. Welche Grundsätze muss ich bei der Verarbeitung personenbezogener Daten einhalten?

Es gelten folgende Grundsätze die bei jeder Verarbeitung von personenbezogenen Daten einzuhalten sind.

- **Rechtmäßigkeit**
Die bildet die legitime Basis der Datenverarbeitung. Ohne Rechtmäßigkeit gem. Artikel 6 DSGVO (Vertrag, Gesetz, Einwilligung, berechtigtes Interesse) darf keine Verarbeitung stattfinden.
- **Treu und Glauben**
Ein ordnungsgemäßer, vertraulicher Umgang mit den Daten wird vorausgesetzt (ähnlich Vertrauensgrundsatz im Straßenverkehr).
- **Transparenz**
Die Datenverarbeitung muss für die betroffene Person nachvollziehbar sein und es besteht die Pflicht zur Information Die Datenschutzerklärung informiert in klarer und einfacher Sprache über den Verantwortlichen und den Datenfluss.
- **Zweckbindung**
Beispiel: Die Daten werden zum Zwecke der Verfassung einer bestimmten wissenschaftlichen Arbeit erhoben. Sie dürfen diese Daten dann nicht ohne weiteres für andere Zwecke (Weitergabe der Rohdaten für eine andere wissenschaftliche Arbeit, Marketing) verwenden.
- **Datensparsamkeit / Datenminimierung**
Erheben bzw verarbeiten Sie nur Daten, die für die wissenschaftliche Arbeit notwendig sind. Bei jedem Datenfeld ist zu hinterfragen, wofür die Daten konkret und wie lange diese benötigt werden.
- **Sachliche Richtigkeit**
Die Daten müssen sachlich richtig und auf dem neuesten Stand sein. Diese Anforderung ergibt sich auch aus der „guten wissenschaftlichen Praxis“.
- **Begrenzte Speicherung**
Ein Personenbezug ist frühestmöglich zu löschen, nämlich sobald die zweckgebundene Erforderlichkeit der Speicherung wegfällt. Das anonyme Endergebnis bzw. Rohdaten können und müssen zum Nachweis der guten wissenschaftlichen Praxis aufbewahrt werden.
- **Integrität und Vertraulichkeit**
Gehen Sie sorgsam mit den (Roh)daten um. Vor allem bei mobilen Datenträgern ist besondere Sorgfalt notwendig, zB durch Verschlüsselung.

Wenn dies alles nachweisbar erfüllt ist, dürfen personenbezogene Daten verarbeitet werden.

8. Wer ist ‚Betroffene‘ / ‚Betroffener‘ im Sinne der DSGVO und welche Verantwortung habe ich gegenüber diesen Personen?



„Betroffene“ / „Betroffener“ (auch „Datensubjekt“ genannt) nach der DSGVO ist jede natürliche Person, deren personenbezogene Daten in elektronischer oder Papierform verarbeitet werden. Juristische Personen (Behörden, Vereine oder Gesellschaften) sind keine „Betroffenen“.

Die Verarbeitung von personenbezogenen Daten betrifft alle Verwendungsvorgänge, die u.a. Daten erheben, erfassen, ordnen und organisieren, speichern, verändern, anpassen, abfragen, auslesen, übermitteln, verbreiten, bereitstellen, verknüpfen, löschen, vernichten oder einschränken.

Als Autorin / Autor einer Abschlussarbeit bin ich nach der DSGVO verantwortlich. Betroffenenrechte können mir gegenüber geltend gemacht werden.

Ich als die „Verantwortliche“ / der „Verantwortliche“ als Verfasserin / als Verfasser einer Abschlussarbeit habe in meiner Verantwortung vor der Verarbeitung der Daten über die Datenverarbeitung zu informieren bzw. eine freiwillige Einwilligung der „Betroffenen“ / des „Betroffenen“ einzuholen, aus der unmissverständlich das Einverständnis zur Verarbeitung der personenbezogenen Daten hervorgeht. Die Verwendung sensibler Daten (beispielsweise Gesundheitsdaten) erfordert eine ausdrückliche Einwilligung. Sollte eine Einwilligung später widerrufen werden, habe ich allein die bis zu diesem Zeitpunkt verarbeiteten Daten zu verwenden.

Weiters habe ich als die „Verantwortliche“ / der „Verantwortliche“ als Autorin / Autor einer Abschlussarbeit dem / der „Betroffenen“ meine Kontaktdaten bekanntzugeben und verantwortungsvoll über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden. Der Zweck sowie die Mittel müssen vorab transparent dargestellt bzw. der / dem „Betroffenen“ mitgeteilt werden.

Es liegt in meiner Verantwortung gegenüber der / dem „Betroffenen“, dass alle von mir vorgenommenen Verarbeitungen der personenbezogenen Daten der EU-Datenschutz-Grundverordnung entsprechen.

Um die angemessene Sicherheit der anvertrauten Daten zu gewährleisten, habe ich als die Verfasserin / der Verfasser der Abschlussarbeit diese Daten vor unbefugter Verarbeitung, bzw. Schädigung oder Verlust zu schützen.

Ich habe der / dem „Betroffenen“ Auskunft zu erteilen und eine eventuell gewünschte Berichtigung vorzunehmen.

9. Was sind Datensicherheitsmaßnahmen (TOM)?

Die DSGVO sieht vor, dass für die Verarbeitung von personenbezogenen Daten adäquate Sicherheitsmaßnahmen zu setzen sind. Datensicherheitsmaßnahmen sind technische und organisatorische Maßnahmen zum Schutz von Daten (sog. TOMs); dies kann z.B.: durch Verschlüsselung, Pseudonymisierung, Zugriffssicherung (Passwortschutz), etc. erfolgen.

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 Daten, soweit möglich kein Informationsaustausch via soziale Medien oder sonst in der Öffentlichkeit, Vorsicht bei der Verwendung von öffentlichen WLANs;
- sichere Aufbewahrung der personenbezogenen 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 beschränkt;
- Löschen der personenbezogenen Daten nach der vereinbarten Aufbewahrungsdauer. 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 entlehrende Stelle).

Die Speicherdauer beträgt für Daten und Forschungsmaterial mindestens 10 Jahre und bis zu 30 Jahre (§ 2f Abs 3 FOG).

10. Welche Vorkehrungen muss ich im Hinblick auf Daten treffen, die ich für meine Abschlussarbeit erhebe?

VOR Erhebung von personenbezogenen Daten:

Erstellung eines Data Management Plans (**DMP**):

Im Rahmen dieses Plans sollten Studierende die folgenden Fragen beantworten:

- Für den Fall der Rekrutierung von teilnehmenden Personen:
Wie rekrutiere ich teilnehmende Personen datenschutzkonform?
- **Wie informiere** ich teilnehmende Personen über die Erhebung deren personenbezogener Daten?
- **Welche** Daten erhebe ich?
 - Handelt es sich dabei um personenbezogene Daten?
 - Benötige ich überhaupt personenbezogene Daten oder kann ich auch mit anonymen oder anonymisierten / bereits veröffentlichten Daten arbeiten?
 - Welche Daten sind über längere Zeit zu welchem Zweck in personenbezogener Form zu verarbeiten? (z.B.: Informations- und Einwilligungserklärungen zum Nachweis der guten wissenschaftlichen Praxis und Forschungsethik)
 - Handelt es sich bei den Erhebungsdaten um besondere Kategorien personenbezogener Daten?
- **Wie lange, wo, wie und zu welchem Zweck** bewahre ich die Daten auf (analog? digital)?
 - Wie lange, wo, wie und zu welchem Zweck bewahre ich personenbezogene Daten auf?
 - Wie lange benötige ich Daten überhaupt in personenbezogener Form? (z.B.: bis Datensätze, welche zu verschiedenen Zeitpunkten erhoben wurden, zusammengeführt wurden)
 - Wie pseudonymisiere ich Erhebungsdaten?
 - Wie anonymisiere ich Erhebungsdaten, sodass keine Rückschlüsse auf teilnehmende Personen mehr möglich sind?
 - Wie lange, wo, wie und zu welchem Zweck bewahre ich Rohdaten auf?
 - Wie lange, wo und wie bewahre ich Analysedaten auf?



- **Wie schütze ich diese Daten und wer hat Zugang zu diesen?**
 - Welche technischen und organisatorischen Maßnahmen zum Datenschutz (TOM) treffe ich? Für den Fall der Verarbeitung von besonderen Kategorien personenbezogener Daten: Welche besonderen technischen und organisatorischen Maßnahmen zum Datenschutz (TOM) treffe ich?
- **In welcher Form publiziere ich Daten?** Für den Fall der Publikation von personenbezogenen Daten: Liegt hierfür eine Rechtsgrundlage vor?

11. Wie verhalte ich mich, wenn Daten verloren gehen?

Als Verantwortlicher müssen Sie im Fall einer Datenpanne tätig werden.

Datenpanne bedeutet (unvollständige Aufzählung)

- unbeabsichtigtes Löschen von Daten;
- Verlust von Laptop / externer Festplatte / USB;
- Mail mit personenbezogenen Daten an einen falschen Empfänger.

Überlegen Sie zu Beginn Ihrer Arbeit, was eine Datenpanne für die betroffenen Personen bedeuten würde, damit Sie rasch handeln können, wenn dieser Fall eintritt.

Der Artikel 33 DSGVO regelt die Vorgehensweise: Wenn durch die Datenpanne Betroffene in ihren Rechten und Freiheiten einem Risiko ausgesetzt sind, müssen Sie dies der Aufsichtsbehörde innerhalb von 72 h melden. Für Österreich ist dies die österreichische Datenschutzbehörde (vgl.: <https://www.dsb.gv.at/>). Hat die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten einer natürlicher Personen zur Folge, so ist auch die betroffene Person unverzüglich von der Verletzung zu verständigen (Artikel 34 DSGVO).

Weiterführende Informationen:

- **Frei zugängliche e-learning Kurse – IMOOX: www.imoox.at**
 - Univ.-Prof. Dr. Mag. Nikolaus Forgó (Universität Wien) (2021):
Rechtlich sicher forschen; Link: <https://imoox.at/course/RESIFO>
 - Univ.-Prof. Dr. Mag. Nikolaus Forgó (Universität Wien) (2021):
Rechtlich sicher publizieren; Link: <https://imoox.at/course/RESIPU>
- **BMBWF (Hrsg) (2020): Praxisleitfaden für Integrität und Wissenschaft:**
<https://oeawi.at/events/praxisleitfaden-fuer-integritaet-und-ethik/>