

Handbuch **DATENSCHUTZ**

Umgang mit personenbezogenen Daten
an der TU Graz



Impressum

Technische Universität Graz
Qualitätsmanagement, Evaluation & Berichtswesen
Rechbauerstraße 12
8010 Graz

Autoren

Mag.iur. Daniel Kurzmann, BA MA LL.M.
daniel.kurzmann@tugraz.at

Mag.iur. Christof Plaschke
christof.plaschke@tugraz.at

Stand

2023

Layout/Satz

Nina Eisner, polycoon e.U.

Unter dem QR-Code finden Sie die Online-Version
des Handbuchs:



Inhalt

1. Begriffsbestimmungen	8
1.1. Datenschutz-Grundverordnung	8
1.2. Personenbezogene Daten	9
1.3. Besondere Kategorien personenbezogener Daten	9
1.4. Gesundheitsdaten	10
1.5. Verarbeitung	11
1.6. Pseudonymisierte Daten	12
1.7. Anonymisierte Daten	12
1.8. Abgrenzung anonymisierte und pseudonymisierte Daten	13
1.9. Betroffene Personen	13
1.10. Verantwortlicher	14
1.11. Gemeinsam Verantwortliche	14
1.12. Auftragsverarbeiter	15
1.13. Sachlicher Anwendungsbereich	15
1.14. Räumlicher Anwendungsbereich	16
2. Grundsätze und interne Umsetzung	18
2.1. Interne Umsetzungsmaßnahmen	18
2.1.1. Datenschutzbeirat für Arbeitnehmer*innen der TU Graz	18
2.1.2. Erweiterter Datenschutzbeirat der TU Graz	19
2.1.3. Satzungsteil Datenschutzordnung der TU Graz	19

2.1.4. Rahmenbetriebsvereinbarung „Über die automatisationsgestützte Verarbeitung personenbezogener Daten von Arbeitnehmerinnen und Arbeitnehmern“	19
2.1.5. Antrag zum Einsatz einer personenbezogenen Datenverarbeitung	20
2.1.6. Datenschutzbeauftragter der TU Graz	21
2.2. Grundsätze und Rechtsgrundlagen für die Verarbeitung personenbezogener Daten	22
2.2.1. Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz	22
2.2.2. Zweckbindung	24
2.2.3. Datenminimierung	26
2.2.4. Richtigkeit	26
2.2.5. Speicherbegrenzung	27
2.2.6. Integrität und Vertraulichkeit	28
2.2.7. Rechenschaftspflicht	28
2.2.8. Datenschutzinformation	28
2.2.9. Betroffenenrechte	29
2.2.10. Informationssicherheit	32
2.2.11. Datenschutzvorfall/Data Breach	33
2.2.12. Verarbeitungsverzeichnis (Tool Proventor)	35
2.2.13. Datenschutz-Folgenabschätzung	35
3. Lehre	37
3.1. Erfüllung der Informationspflicht gegenüber den Studierenden	37

3.2. Aufbewahrungsfristen im Bereich der Lehre	38
3.2.1. Beurteilungsunterlagen	38
3.2.2. Bachelorarbeiten, Seminararbeiten	38
3.2.3. Aufbewahrung von universitätsspezifischen Daten (Prüfungsdaten)	39
3.2.4. Raumeinteilungen	40
3.3. Veröffentlichungen im Rahmen von mündlichen (Abschluss-)Prüfungen	40
3.4. Veröffentlichungen im Rahmen von schriftlichen Prüfungen	41
3.5. Unterschriftenlisten und Anwesenheitslisten	41
3.6. Fotos und Videos im Rahmen von Lehrveranstaltungen/Exkursionen	42
3.7. Aussenden von Zwischenergebnissen	42
3.8. Abgaben/Einsichtnahme	43
3.9. Datenschutz- und Geheimhaltungsverpflichtung bei Abschlussarbeiten	43
3.10. Veröffentlichungen im Rahmen von Abschlussfeiern	44
3.11. Virtuelle Lehre	44
4. Forschung	45
4.1. Datenschutz in der Forschung	45
4.2. Rollenverteilung	46
4.3. Rechtsgrundlagen	47
4.3.1. Datenschutz-Grundverordnung (DSGVO)	47
4.3.2. Datenschutzgesetz (DSG)	48

4.3.3. Forschungsorganisations-Gesetz (FOG)	49
4.4. Grundsätze der DSGVO	49
4.5. Aufbewahrungsfristen von Forschungsdaten	52
4.6. Verarbeitung von personenbezogenen Daten von Kindern	53
4.7. Empfohlene Vorgehensweise	54
4.7.1. Abklärung der organisatorischen und rechtlichen Rahmenbedingungen	54
4.7.2. Abklärung datenschutzrechtlicher Implikationen	55
5. Verwaltung	56
5.1. Einleitung	56
5.2. Personal	56
5.2.1. Bewerbungen	56
5.2.2. Initiativbewerbungen/Evidenzhaltung von Bewerbungen	57
5.2.3. Datenschutzinformation für (neue) Bedienstete	58
5.2.4. Geburtstagskalender	58
5.2.5. Mitarbeiter*innengespräche	58
5.2.6. Geheimhaltungsverpflichtung	59
5.2.7. Aufbewahrung von personenbezogenen Personaldaten	59
5.2.8. Veröffentlichung ehemaliger Bediensteter auf der (Instituts-)Webseite	60
5.2.9. Verarbeitung von personenbezogenen Daten von Kindern	61

5.2.10. Videoüberwachung	61
5.3. Veranstaltungen und Öffentlichkeitsarbeit	61
5.3.1. Veranstaltungen	61
5.3.2. Webseiten	62
5.3.3. Social Media (Facebook, Instagram, X, LinkedIn etc.)	62
5.4. Umgang mit Kontaktdaten	63
5.4.1. Kontaktdatenbanken	63
5.4.2. Versand von Einladungen und Newslettern	64
5.4.3. Anschreiben von neuen Kontakten	65
5.4.4. Kommunikation mit Bediensteten und Studierenden der TU Graz	65
6. Archivgut	66
7. Kontaktdaten	67
8. Link-Sammlung	68





Eine Zusammenfassung der wichtigsten Punkte, insbesondere der rechtlich verpflichtenden Meldung von Datenschutzvorfällen (Data Breach), finden Sie im **Informationsblatt für Bedienstete** (siehe Link-Sammlung).

¹ Verordnung 2016/679/EU des Europäischen Parlamentes und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/45/EG (Datenschutz-Grundverordnung), ABIL 201/37.

² Richtlinie 95/46/EG des Europäischen Parlament und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABIL 281/31.

³ Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 165/1999 idF I 148/2021.

⁴ Bundesgesetz über allgemeine Angelegenheiten gemäß Art 89 DSGVO und die Forschungsorganisation (Forschungsorganisationsgesetz – FOG), BGBl I 341/1981 idF I 116/2022.

1. Begriffsbestimmungen

1.1. DATENSCHUTZ-GRUNDVERORDNUNG

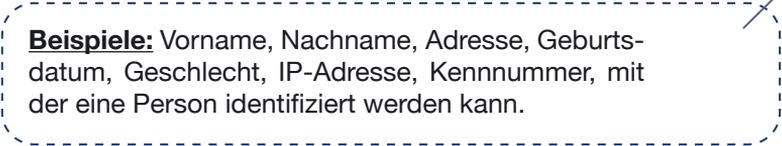
Die Datenschutz-Grundverordnung¹ (nachfolgend DSGVO) gilt seit 25. Mai 2018 und ist als EU-Verordnung in den Mitgliedsstaaten der Europäischen Union (EU) direkt anwendbar. Darüber hinaus ist sie seit 20. Juli 2018 auch in den Mitgliedsstaaten der Europäischen Freihandelszone (EFTA) geltendes Recht. Die DSGVO löst damit die Datenschutz-Richtlinie² ab und trägt zur Harmonisierung des Datenschutzrechts im Europäischen Wirtschaftsraum (EWR) bei. Zahlreiche Öffnungsklauseln ermöglichen es den nationalen Gesetzgebern, eigenständige Regelungen zu diversen Einzelfragen bzw. Teilbereichen vorzunehmen.

Mit dem Datenschutz-Anpassungsgesetz 2018 hat der österreichische Gesetzgeber das Datenschutzgesetz³ (zuvor DSG 2000) sowie diverse weitere Materienetze novelliert (u.a. das Forschungsorganisationsgesetz⁴, siehe weiterführende Informationen).

Wenn nicht explizit angegeben, bezieht sich die Bezeichnung „Daten“ in diesem Handbuch immer auf „personenbezogene Daten“ im Sinne der DSGVO.

1.2. PERSONENBEZOGENE DATEN

Im Sinne der DSGVO bezeichnet der Ausdruck „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung oder einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann (Art 4 Z 1 DSGVO).



Beispiele: Vorname, Nachname, Adresse, Geburtsdatum, Geschlecht, IP-Adresse, Kennnummer, mit der eine Person identifiziert werden kann.

1.3. BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN

Besondere Kategorien personenbezogener Daten im Sinne der DSGVO (umgangssprachlich „sensible Daten“) sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen,



religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Zudem zählen genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer Person zu den sensiblen Daten (Art 9 Abs 1 DSGVO).

Die Verarbeitung der genannten Daten ist nur zulässig, wenn eine der in Art 9 Abs 2 DSGVO aufgezählten Ausnahmen vorliegen (z.B. ausdrückliche und freiwillige Einwilligung, Verarbeitung zu Zwecken der Gesundheitsvorsorge oder der Arbeitsmedizin, wenn es dafür eine gesetzliche Grundlage gibt). Des Weiteren sind im Zusammenhang mit der Verarbeitung von sensiblen Daten höhere Anforderungen an die technischen und organisatorischen Maßnahmen zu stellen (siehe auch 2.2. – Rechtmäßigkeit sowie Integrität und Vertraulichkeit).

Ob ein sensibles Datum vorliegt, kann anhand des Verarbeitungszweckes festgestellt werden. Erfolgt die Verarbeitung z.B. zu gesundheitlichen Zwecken, handelt es sich in der Regel um Gesundheitsdaten (siehe auch nachfolgender Punkt) und somit um sensible Daten.



Beispiele: Verarbeitung von Hirnstrommessungen im Zuge von Forschungsprojekten, wobei diese einer Person zugeordnet sind oder zugeordnet werden können (ID-Nummer etc.); Verarbeitung der Sozialversicherungsnummer in einem gesundheitsbezogenen Zusammenhang.

1.4. GESUNDHEITSDATEN

Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Ob Gesundheitsdaten vorliegen, richtet sich insbesondere nach dem Zweck der Verarbeitung. Beispielsweise stellt die Sozialversicherungsnummer ein Gesundheitsdatum dar, wenn diese für Zwecke der Erbringung von Gesundheitsdienstleistungen verwendet wird.

1.5. VERARBEITUNG

Als „Verarbeitung“ gilt jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das **Erheben**, das **Erfassen**, die **Organisation**, das **Ordnen**, die **Speicherung**, die **Anpassung** oder **Veränderung**, das **Auslesen**, das **Abfragen**, die **Verwendung**, die **Offenlegung durch Übermittlung**, **Verbreitung** oder eine andere Form der **Bereitstellung**, den **Abgleich** oder die **Verknüpfung**, die **Einschränkung**, das **Löschen** oder die **Verichtung** (Art 4 Z 2 DSGVO).

Wie man aus der Definition erkennen kann, ist der Begriff der „Verarbeitung“ sehr weit auszulegen. Im Zweifelsfall liegt somit eine Verarbeitung vor.



1.6. PSEUDONYMISIERTE DATEN

Die personenbezogenen Daten (z.B. Kennnummer/ Code) werden in einer Weise verarbeitet, dass die Daten ohne Hinzuziehung zusätzlicher Informationen (z.B. Adressen, Namen) nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen (z.B. Zutritts-, Zugangs- und Zugriffskontrolle, Löschrufen etc.), die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können (Art 4 Z 5 DSGVO).

Werden Namen von Personen durch Codes ersetzt, handelt es sich regelmäßig um pseudonymisierte Daten. Die Feststellung der Identität wird zwar erschwert, jedoch kann der Bezug zwischen einer Person und ihren Daten wiederhergestellt werden. Die Person ist daher zumindest identifizierbar.



Beispiele: Einweg/Hashfunktion; Nickname; teilnehmende Personen können trotz Entfernung von Daten anhand von Vorerkrankungen in Verbindung mit dem Alter identifiziert werden.

1.7. ANONYMISIERTE DATEN

Ist es ausgeschlossen, dass vorliegende Daten einer Person zugeordnet werden können, also kein

Personenbezug herstellbar ist, liegen anonymisierte bzw. anonyme Daten vor. Bei solchen Daten handelt es sich um keine personenbezogenen Daten, weshalb das Datenschutzrecht nicht zur Anwendung kommt.



Beispiel: Aggregierte Daten, die für statistische Zwecke verwendet werden und nicht (mehr) zuordenbar sind.

1.8. ABGRENZUNG ANONYMISIERTE UND PSEUDONYMISIERTE DATEN

Anonymisiert: Es ist ausgeschlossen, dass Daten einer Person zugeordnet werden können. Es ist kein Personenbezug mehr herstellbar, daher kommt das Datenschutzrecht nicht zur Anwendung.

Pseudonymisiert: Zum Beispiel wird der Name einer Person durch einen Code ersetzt (z.B. QR-Code). Die Feststellung der Identität wird zwar erschwert, aber der Bezug zwischen einer Person und ihren Daten kann wiederhergestellt werden. Die Person ist identifizierbar, es handelt sich um personenbezogene Daten, daher kommt das Datenschutzrecht zur Anwendung.

1.9. BETROFFENE PERSONEN

Betroffene Personen oder „die Betroffenen“ sind jene natürlichen oder juristischen Personen, deren personenbezogene Daten von einem Verantwortlichen oder Auftragsverarbeiter verarbeitet werden.



1.10. VERANTWORTLICHER

Verantwortlicher im Sinne der DSGVO ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Verarbeitung der personenbezogenen Daten entscheidet.

Verarbeitungstätigkeiten von Bediensteten aufgrund einer fachlichen Weisung werden dem*der Arbeitgeber*in zugerechnet. Bedienstete sind in diesem Fall nicht Verantwortliche im Sinne der DSGVO. Dies gilt auch für arbeitnehmerähnliche Dienstverhältnisse sowie für leitende Angestellte im Rahmen ihrer Weisungsunterworfenheit. Anders verhält es sich, wenn Bedienstete entgegen oder außerhalb einer Weisung des*der Arbeitgeber*in handeln und damit z.B. Eigeninteressen verfolgen. Das Handeln der Bediensteten kann demnach nicht mehr dem*der Arbeitgeber*in zugeordnet werden, weshalb die Bediensteten die Rolle des Verantwortlichen einnehmen.⁵ Eine solche Verarbeitung wäre somit nicht dem*der Arbeitgeber*in zuzurechnen.⁶

⁵ Leitinger, Gosch, *Die Zurechnung unterstellter Personen zum Verantwortlichen mit besonderem Fokus auf das Verhältnis zwischen „Mitarbeiter“ und „Arbeitgeber“*, *jusIT* 2021/46, 115 (122).

⁶ Leitinger, Gosch, *Die Weisung im Datenschutzrecht – Konsequenzen aus Datenschutzverstößen durch Mitarbeiter*, *jusIT* 2022/9, 23 (28).

1.11. GEMEINSAM VERANTWORTLICHE

Entscheiden zwei oder mehrere Verantwortliche gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten, sind diese für die Datenverarbeitung gemeinsam verantwortlich. Die gemeinsam Verantwortlichen haben in diesem Fall eine Vereinbarung abzuschließen, in welcher diese transparent regeln, wer die Erfüllung der datenschutzrechtlichen Verpflichtungen übernimmt (z.B. Informationspflicht, Betroffenen-

rechte, Data Breach etc.). Diese Vereinbarung muss schriftlich erfolgen.

Anwendungsfälle: TU Graz und (Forschungs-) Partner*innen im Zuge der gemeinsamen Verarbeitung von personenbezogenen Daten wie z.B. BioTechMed, Digital University Hub, Stipendienprogramme, NAWI Graz.

1.12. AUFTRAGSVERARBEITER

Auftragsverarbeiter ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im **Auftrag** verarbeitet. Liegt eine Auftragsverarbeitung vor ist ein Auftragsverarbeitungsvertrag abzuschließen (AVV). Wird seitens der TU Graz ein Dienstleister beauftragt, empfiehlt sich eine datenschutzrechtliche Abklärung, ob unter Umständen eine Auftragsverarbeitung vorliegt.

Werden personenbezogene Daten an Dritte übermittelt (keine Auftragsverarbeitung bzw. keine Verarbeitung in gemeinsamer Verantwortung, z.B. eine Firma erbringt als Dienstleistung die Vernichtung von Festplatten; Versendung von Briefen durch die Post), kann es im Einzelfall notwendig sein, eine Geheimhaltungsverpflichtung abzuschließen.

1.13. SACHLICHER ANWENDUNGSBEREICH

Die DSGVO gilt für die **ganz oder teilweise automatisierte Verarbeitung** personenbezogener Daten sowie für die **nichtautomatisierte Verarbeitung** personenbezogener Daten, die in einem



Dateisystem (und/oder Karteisystem, z.B. Unterlagen in einem Handordner) gespeichert sind oder gespeichert werden sollen (Art 2 DSGVO).



Beispiel: Eine Bedienstete unterhält sich mit den Betriebsräten über vorgesetzte Personen. Die in der mündlichen Unterhaltung ausgetauschten personenbezogenen Daten sind vom Anwendungsbereich der DSGVO nicht umfasst. Jedoch gilt in diesem Fall trotzdem das Grundrecht auf Datenschutz (§ 1 DSG).

1.14. RÄUMLICHER ANWENDUNGSBEREICH

Der räumliche Anwendungsbereich der DSGVO umfasst alle Datenverarbeitungen, die im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der EU erfolgen. Ob die Verarbeitung der Daten in der Union stattfindet, ist nicht entscheidend.

Hat ein Verantwortlicher oder Auftragsverarbeiter keine Niederlassung in der EU und verarbeitet dieser aber trotzdem personenbezogene Daten von Personen in der EU, ist die DSGVO anwendbar, wenn

- dieser Waren oder Dienstleistungen in der Union anbietet, oder
- das Verhalten von Personen beobachtet wird, soweit das Verhalten in der Union erfolgt (Art 3 DSGVO).



Beispiel: Im Rahmen eines internationalen Forschungsprojektes zwischen der TU Graz und einer chinesischen Universität kommt es zur gemeinsamen Analyse von Gesundheitsdaten der am Projekt teilnehmenden Proband*innen. Beide Universitäten sind zur Einhaltung der DSGVO verpflichtet, zumal die Proband*innen EU-Bürger*innen sind.



2. Grundsätze und interne Umsetzung

2.1. INTERNE UMSETZUNGSMASSNAHMEN

Um den datenschutzrechtlichen Anforderungen gerecht zu werden, hat die TU Graz den Satzungsteil Datenschutzordnung novelliert sowie eine Rahmenbetriebsvereinbarung zur Regelung der datenschutzrechtlichen Aspekte im Bereich der Verarbeitung von personenbezogenen Daten von Bediensteten beschlossen.

Im Satzungsteil Datenschutzordnung wurde der Datenschutzbeirat für Arbeitnehmer*innen zur Beschlussfassung sowie der erweiterte Datenschutzbeirat zur Beratung des Rektorates zu datenschutzrechtlichen Themen eingesetzt (siehe 2.1.1. und 2.1.2.).

2.1.1. DATENSCHUTZBEIRAT FÜR ARBEITNEHMER*INNEN DER TU GRAZ

Der Datenschutzbeirat für Arbeitnehmer*innen (<https://tu4u.tugraz.at/go/dsb-a>) behandelt alle Fragen, die sich im Zusammenhang mit der Verarbeitung von personenbezogenen Daten der Bediensteten, insbesondere mit der Einführung, dem Betrieb und der Veränderung von IKT-Systemen ergeben (siehe 2.1.4.).



2.1.2. ERWEITERTER DATENSCHUTZ- BEIRAT DER TU GRAZ

Sind nicht nur personenbezogene Daten von Bediensteten, sondern auch von Studierenden, von weiteren Universitätsangehörigen (z.B. Privatdozent*innen, Forschungsstipendiat*innen) sowie von Externen (z.B. von Bewerbenden um Stellen und Studien sowie von Bediensteten Dritter) betroffen, fällt dies in die Zuständigkeit des erweiterten Datenschutzbeirates (<https://tu4u.tugraz.at/go/dsb-e>).

Des Weiteren erstreckt sich die Zuständigkeit des Beirates auf vertrauliche Daten ohne Bezug zu natürlichen oder juristischen Personen, z. B. aus Verträgen, Arbeitsergebnissen usw., und auf Daten aus Forschungsprojekten (unter Berücksichtigung des FAIR-Data-Prinzips).

2.1.3. SATZUNGSTEIL DATENSCHUTZ- ORDNUNG DER TU GRAZ

Der Satzungsteil Datenschutzordnung der Technischen Universität Graz ist im TU4U abrufbar.

2.1.4. RAHMENBETRIEBSVEREINBARUNG „ÜBER DIE AUTOMATISATIONSGESTÜTZTE VERARBEITUNG PERSONENBEZOGENER DATEN VON ARBEITNEHMERINNEN UND ARBEITNEHMERN“

In Umsetzung der arbeitsrechtlichen und datenschutzrechtlichen Bestimmungen haben die TU Graz und die Betriebsräte eine Rahmenbetriebsvereinbarung (im Sinne der §§ 96, 96a und 97 ArbVG⁷)

⁷ Bundesgesetz vom 14. Dezember 1973 betreffend die Arbeitsverfassungsgesetz – ArbVG), BGBl I 22/1974 idF I 115/2022.

beschlossen, die für die Planung, Einführung, Verwendung und Veränderung bestehender und zukünftiger Informations- und Kommunikationssysteme im Zusammenhang mit personenbezogenen Daten der Bediensteten Anwendung findet.

2.1.5. ANTRAG ZUM EINSATZ EINER PERSONENBEZOGENEN DATENVERARBEITUNG

Um für bestehende und zukünftige Informations- und Kommunikationssysteme die Erfüllung der gesetzlichen und internen Anforderungen zu gewährleisten, steht ein Antrag zum Einsatz einer personenbezogenen Datenverarbeitung zur Verfügung. Dieser Antrag ist im TU4U abrufbar und beinhaltet drei Teile – einen allgemeinen, einen technischen sowie einen Teil zu den spezifischen technischen und organisatorischen Maßnahmen des IKT-Systems. Die Anträge können von den antragsstellenden Personen nach der datenschutzrechtlichen Einschätzung durch die Datenschutzkoordination und des IT-Security-Teams im Datenschutzbeirat für Arbeitnehmer*innen eingebracht werden. Die Bewertung des Antrages wird von den Mitgliedern des Datenschutzbeirates für Arbeitnehmer*innen vorgenommen. Beschlüsse dieses Gremiums werden auf Grundlage von Beschlüssen des Rektorats, der Betriebsräte und der Dienststellenausschüsse getroffen. Die ausgefüllten Anträge bzw. offene Fragen sind vorab an die Sitzungskoordination (datenschutz@tugraz.at) zu übermitteln.

2.1.6. DATENSCHUTZBEAUFTRAGTER DER TU GRAZ

Um eine ausreichende Unabhängigkeit gewährleisten zu können, wurde von der TU Graz ein externer Datenschutzbeauftragter, die x-tention Informationstechnologie GmbH, Römerstraße 80a, 4600 Wels mit Wirkung ab 14. Mai 2018 bestellt.

Die Aufgaben des externen Datenschutzbeauftragten sind die

- Unterrichtung und Beratung des Rektorates in Bezug auf die Pflichten aus der DSGVO und anderer Datenschutzvorschriften;
- Überwachung und Überprüfung der Einhaltung der DSGVO und anderer Datenschutzvorschriften sowie der Datenschutzstrategie, einschließlich der Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung der an der operativen Umsetzung beteiligten Bediensteten;
- Prüfung und Dokumentation von Meldungen an die zuständige Aufsichtsbehörde;
- Schulung der Bediensteten hinsichtlich der Pflichten aus der DSGVO;
- Zusammenarbeit und Anlaufstelle für die zuständige Aufsichtsbehörde.



2.2. GRUNDSÄTZE UND RECHTSGRUNDLAGEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

Die Datenschutzkoordination empfiehlt bei jeder Datenverarbeitung die Prüfung der nachfolgenden Grundsätze. Sind diese erfüllt, ist die Datenverarbeitung regelmäßig zulässig.

2.2.1. RECHTMÄSSIGKEIT, VERARBEITUNG NACH TREU UND GLAUBEN, TRANSPARENZ

Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, außer es liegt eine Ausnahme (Rechtsgrundlagen in Art 6 DSGVO) von diesem Verbot vor („Erlaubnisvorbehalt“).

Eine Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen die Möglichkeit haben müssen, von der Verarbeitung ihrer Daten Kenntnis zu erlangen. Die heimliche Verarbeitung von personenbezogenen Daten betroffener Personen soll damit verhindert werden. In enger Verbindung mit der Verarbeitung nach Treu und Glauben steht der Grundsatz der Transparenz. Betroffene Personen müssen demnach über die Verarbeitung ihrer personenbezogenen Daten in verständlicher Sprache und umfassend informiert werden (z.B. Information über den Umfang der Datenverarbeitung, die Identität des Verantwortlichen, Zwecke der Datenverarbeitung, Rechte der Betroffenen usw.). Diese Informationen werden den betroffenen Personen in einer



Datenschutzerklärung dargelegt. Transparenz in Hinblick auf die Verarbeitung von personenbezogenen Daten kann u.a. auch im Wege des Datenschutzes durch Technik (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) hergestellt werden.

Eine rechtmäßige Verarbeitung liegt vor, wenn alle Grundsätze (siehe 2.2.) erfüllt sind und eine der nachfolgenden Rechtsgrundlagen vorliegt:

- die betroffene Person hat ihre freiwillige Einwilligung zur Verarbeitung gegeben (Art 6 Abs 1 lit a DSGVO) (die Einwilligung kann jederzeit und ohne Angabe von Gründen widerrufen werden);
- die Verarbeitung ist für die Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen erforderlich (Art 6 Abs 1 lit b DSGVO);
- die Verarbeitung ist zur Erfüllung gesetzlicher Verpflichtungen erforderlich (Art 6 Abs 1 lit c DSGVO);
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich (Art 6 Abs 1 lit d DSGVO);
- die Verarbeitung ist zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse (Ausübung öffentlicher Gewalt) liegt, erforderlich (Art 6 Abs 1 lit e DSGVO);
- die Verarbeitung ist zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich (Art 6 Abs 1 lit f DSGVO).

Details zu den Rechtsgrundlagen können in Art 6 DSGVO nachgelesen werden bzw. zur Einwilligung auch in Art 7 DSGVO.

Für eine Einwilligungserklärung (nach Art 6 Abs 1 lit a DSGVO) steht eine Vorlage im TU4U (<https://tu4u.tugraz.at/go/ds-vorlagen>) zur Verfügung, die ausschließlich zusammen mit einer Datenschutzerklärung zu verwenden ist. Jene Zwecke, die auf der Rechtsgrundlage der Einwilligung beruhen, sind in der Vorlage zur Einwilligungserklärung anzuführen. Diese müssen mit den Angaben in der Datenschutzerklärung übereinstimmen (z.B. Einwilligung zum Newsletterversand, Einwilligung in die Verarbeitung der Daten für ein konkret bezeichnetes Forschungsprojekt oder einen konkreten Forschungsbereich – siehe 5.). Die Zwecke in der Datenschutzerklärung müssen daher mit jenen in der Einwilligungserklärung übereinstimmen.

Beachte: Die Einwilligungserklärung ist ausschließlich für jene Zwecke notwendig, für welche die Einwilligung nach Art 6 Abs 1 lit a DSGVO erteilt wird. Für andere Rechtsgrundlagen ist KEINE Einwilligungserklärung notwendig! Stützen sich die Verarbeitungen auf andere Rechtsgrundlagen (wie z.B. öffentliches/berechtigtes Interesse, Vertrag etc. – also nicht auf die Einwilligung), reicht es aus, die Informationen in der Datenschutzerklärung den Betroffenen zur Kenntnis zu bringen.

2.2.2. ZWECKBINDUNG

Der Zweck der Erhebung von personenbezogenen Daten und der anschließenden Datenverarbeitung

muss bereits zum Zeitpunkt der Datenerhebung festgelegt sein. Die Erhebung und Verarbeitung darf dabei nur für **festgelegte, eindeutige und legitime Zwecke** (einschlägige Rechtsgrundlage, kein Verstoß gegen geltende Normen) erfolgen. Darüber hinaus muss der Zweck hinreichend bestimmt sein.

Durch die Zweckfestlegung wird bestimmt, welche personenbezogenen Daten notwendig sind (Datenminimierung – welche Daten werden für die Erreichung des Zwecks benötigt?) und wie lange diese gespeichert werden dürfen (Speicherbegrenzung – wie lange werden die Daten benötigt?). Aufgrund dieser Anforderungen und der Beweisspflicht des Verantwortlichen empfiehlt es sich, den Zweck der Datenverarbeitung jedenfalls in Schriftform zu dokumentieren (z.B. durch den Antrag zum Einsatz einer personenbezogenen Datenverarbeitung und/oder durch die Aufnahme der Datenverarbeitung in das Verarbeitungsverzeichnis).

Ein festgelegter, eindeutiger und legitimer Zweck ergibt sich häufig aus gesetzlichen Bestimmungen, aus vertraglichen Vereinbarungen und/oder aus der praktischen Übung.

Folgende Fragen können unterstützend zur Abklärung dafür dienen, ob ein ausreichender Verarbeitungszweck vorliegt:

- Für welchen Zweck werden die Daten verarbeitet?
- Ist dieser Zweck rechtmäßig?
- Sind die zu erhebenden Daten ausreichend definiert?



Können diese Fragen beantwortet werden, liegt regelmäßig ein festgelegter, eindeutiger und legitimer Verarbeitungszweck vor.

2.2.3. DATENMINIMIERUNG

Wie bereits bei der Zweckbindung beschrieben, dürfen nur jene personenbezogenen Daten verarbeitet werden, die für die Erreichung des konkreten Zweckes erforderlich sind. Der Grundsatz der Datenminimierung ergänzt daher den Grundsatz der Zweckbindung. Werden auch Daten verarbeitet, die für die Zweckerreichung nicht dringend benötigt werden (z.B. kein Bezug der Daten zum Verarbeitungszweck, d.h. der festgelegte Zweck kann durch die verarbeiteten Daten nicht gefördert werden, da es gelindere Mittel gibt) liegt eine Verletzung des Grundsatzes der Datenminimierung vor. Es ist auch stets zu prüfen, ob der Verarbeitungszweck auch mit anonymisierten Daten erreicht werden kann.



Beispiel: Es werden nur Daten verarbeitet, die für eine eindeutige und notwendige Identifizierung der Betroffenen erforderlich sind. In diesem Fall liegt keine Verletzung des Grundsatzes der Datenminimierung vor.

2.2.4. RICHTIGKEIT

Die verarbeiteten personenbezogenen Daten müssen sachlich richtig (der Realität entsprechen) und erforderlichenfalls auf dem neuesten Stand sein. Erfordert der festgelegte Verarbeitungszweck den neuesten Stand der Daten, ist dieser auch dem-

entsprechend sicherzustellen (z.B. Daten für Zutrittsberechtigungen).

2.2.5. SPEICHERBEGRENZUNG

Der Grundsatz der Speicherbegrenzung besagt, dass eine Identifizierung der betroffenen Personen nur solange möglich sein darf, wie dies für die Erreichung des festgelegten Verarbeitungszweckes notwendig ist. Erfordert der Zweck der Datenverarbeitung z.B. die Speicherung der Daten nicht mehr, so sind diese zu löschen. Es findet somit eine zeitliche Begrenzung der Verarbeitung von personenbezogenen Daten statt. Es sollte sichergestellt werden, dass Fristen für die Löschung definiert werden und regelmäßige Überprüfungen stattfinden.

Ob es gesetzliche Aufbewahrungsfristen gibt bzw. ob ein konkreter Verarbeitungszweck vorliegt, kann häufig aus den jeweiligen Materiengesetzen (z.B. BAO, UG, BilDokG 2020) geklärt werden. Zur Klärung etwaiger Fristen wird daher die Kontaktaufnahme mit der zuständigen Fachabteilung empfohlen.



Beispiel: Liegt ein Datensatz vor, der die Identifizierung einer Person ermöglicht und werden für den festgelegten Verarbeitungszweck einige Daten, welche die Person identifizierbar machen, nicht mehr benötigt, ist der Bezug zur betroffenen Person zu entfernen. Aus dem Datensatz sind daher die identifizierenden Merkmale zu löschen. Sind Daten in pseudonymisierter Form vorhanden, kann es daher ausreichend sein, die Zuordnungslisten zu löschen.

2.2.6. INTEGRITÄT UND VERTRAULICHKEIT

Die Sicherheit der verarbeiteten personenbezogenen Daten muss jederzeit gewährleistet sein. Die Daten sind vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (TOM – technische und organisatorische Maßnahmen am Stand der Technik) zu schützen (z.B. Berechtigungen, Zugangskontrolle, Zugriffskontrolle, Wiederherstellbarkeit).

2.2.7. RECHENSCHAFTSPFLICHT

Der Verantwortliche ist zur Einhaltung der vorhin beschriebenen Grundsätze verpflichtet und er muss deren Einhaltung auch nachweisen können (z.B. bei einer Prüfung der Datenschutzbehörde, in gerichtlichen Verfahren). Empfohlen wird daher eine schriftliche Dokumentation z.B. in Form des Verarbeitungsverzeichnisses, Dokumentation der Grundsätze und das Treffen geeigneter technischer und organisatorischer Maßnahmen.

2.2.8. DATENSCHUTZINFORMATION

Der Verantwortliche ist dazu verpflichtet, die Betroffenen über die Verarbeitung von personenbezogenen Daten zu informieren. Die zu erteilenden Informationen sind in Art 13 und 14 DSGVO aufgelistet und umfassen folgende Informationen:

- Name und Kontaktdaten des Verantwortlichen;

- Kontaktdaten des Datenschutzbeauftragten;
- Informationen über die verarbeiteten Datenkategorien (z.B. Bedienstete, Studierende) Art von personenbezogenen Daten (z.B. Vor- und Nachname, Titel, Adresse, IP-Adresse);
- Rechtsgrundlage und Verarbeitungszweck;
- Angaben zu etwaigen Empfängern (Empfänger sollten so konkret wie möglich angegeben werden) bzw. Information über die Übermittlung in ein Drittland (außerhalb EU/EWR);
- Angaben zur Speicherdauer (konkrete Fristen oder Kriterien für die Festlegung der Speicherdauer);
- Rechte der betroffenen Personen;
- Beschwerderecht bei der zuständigen Aufsichtsbehörde (in Österreich die österreichische Datenschutzbehörde).

Muster mit den beschriebenen Informationspflichten zur individuellen Anpassung sind im TU4U abrufbar. Diese können nach erfolgter Anpassung als Datenschutzerklärung für die unterschiedlichsten Datenverarbeitungen dienen wie z.B. Veranstaltungen, Newsletter, Exkursionen oder Umfragen.

2.2.9. BETROFFENENRECHTE

Betroffenen Personen kommen im Datenschutzrecht bestimmte Rechte zu, die sie gegenüber



dem Verantwortlichen geltend machen können. Betroffenenrechte können grundsätzlich formlos oder im Rahmen des internen Prozesses eingebracht werden. Sollten sich betroffene Personen direkt an eine OE der TU Graz wenden, wird unter Hinweis auf die offizielle Webseite (<https://security.tugraz.at/datenschutz/dsgvo/rechte/>) um Weiterleitung der Anfragen an datenschutz@tugraz.at gebeten. Die TU Graz ist gesetzlich verpflichtet, Betroffenenrechte unter Einhaltung einer **Frist von einem Monat** zu erledigen. Folgende Rechte können den betroffenen Personen zustehen:

■ **Recht auf Auskunft über die verarbeiteten Daten**

Mit diesem Recht kann die betroffene Person Informationen über die sie betreffenden personenbezogenen Daten verlangen (insbesondere Verwendungszweck, Datenkategorien, Empfänger). Im Fall des Eingriffs in Rechte Dritter oder exzessiver und offensichtlich unbegründeter Ansuchen, können wir die Beauskunftung ablehnen oder einen Kostenersatz verlangen. Die Auskunft wird binnen eines Monats erteilt (begründete Fristerstreckung ist möglich).

■ **Recht auf Berichtigung der Daten**

Dieses Recht gewährt der betroffenen Personen einen Anspruch auf Berichtigung ihrer sie betreffenden unrichtigen oder unvollständigen Daten.

■ **Recht auf Einschränkung der Datenverarbeitung besteht**

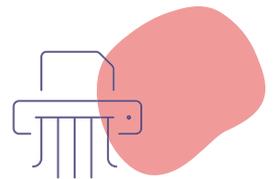
- für die Dauer der Prüfung der bestrittenen Richtigkeit der Daten;

- für die Dauer der Prüfung des überwiegenden berechtigten/öffentlichen Interesses im Fall eines Widerspruchs;
 - im Fall einer unrechtmäßigen Verarbeitung, wenn die betroffene Person keine Löschung der Daten wünscht.
-
- **Recht auf Datenübertragbarkeit**

Dieses Recht besteht hinsichtlich jener Daten, welche die betroffene Person der TU Graz selbst bereitgestellt hat und die von der TU Graz auf Grundlage einer Einwilligung oder die zur Erfüllung eines mit der betroffenen Person geschlossenen Vertrags automationsunterstützt verarbeitet werden. Rechte und Freiheiten Dritter dürfen dadurch nicht beeinträchtigt werden.
-
- **Recht auf Löschung**

Personenbezogene Daten sind zu löschen bzw. besteht ein Recht auf Löschung,

 - falls die Daten für die Zwecke, für die sie verarbeitet wurden, nicht mehr notwendig sind;
 - falls die Einwilligung, auf die sich die Verarbeitung stützt, widerrufen und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt;
 - falls Widerspruch gegen die Verarbeitung eingelegt wird und es keine schutzwürdigen Gründe für die Verarbeitung gibt;
 - falls die Verarbeitung der personenbezogenen Daten unrechtmäßig ist;
 - falls sich die Löschung der personenbezogenen Daten aus rechtlichen Pflichten ergibt.



- **Recht auf Widerspruch gegen die Datenverarbeitung**

Aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, besteht das Recht, jederzeit gegen die Verarbeitung der personenbezogenen Daten, deren Verarbeitung aufgrund von berechtigten oder öffentlichen Interessen erfolgt, Widerspruch einzulegen.

- **Recht auf Widerruf gegen die Datenverarbeitung**

Dieses Recht kann jederzeit und ohne Begründung geltend gemacht werden (nur bei Rechtsgrundlage der Einwilligung). Mit der Ausübung dieses Rechts wird jedoch die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung nicht berührt.

2.2.10. INFORMATIONSSICHERHEIT

Neben den rechtlichen Komponenten ist die Informationssicherheit ein zentraler Aspekt des Datenschutzes (u.a. Art 32 DSGVO). Der Anwendungsbereich erstreckt sich dabei über die Verarbeitung von personenbezogenen Daten hinaus und umfasst auch nicht-personenbezogene Daten. Von zentraler Bedeutung sind dabei die Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) der Daten. Daneben ist Art 25 DSGVO zu beachten, der die Berücksichtigung von Privacy by Design (Datenschutz durch Technikgestaltung) sowie Privacy by Default (datenschutzfreundliche Voreinstellungen) im Zuge der Verarbeitung von personenbezogenen Daten normiert.

Bitte beachten Sie diesbezüglich die Richtlinie zur Informationssicherheit der TU Graz. Nähere Informationen zu diesem Thema sind unter isrl.tugraz.at abrufbar.

2.2.11. DATENSCHUTZVORFALL/ DATA BREACH

Ein sogenannter Data Breach oder Datenschutzvorfall liegt vor, wenn eine Verletzung des Schutzes der personenbezogenen Daten, die im Rahmen der Tätigkeit an der TU Graz verarbeitet werden (Kontaktdaten von Studierenden, Prüfungsdaten, Daten an Veranstaltungen teilnehmender Personen, Daten von Bediensteten etc.) vorliegt.

Mögliche Szenarien:

- Diebstahl oder Verlust von Laptops, Speichermedien (USB-Sticks) o.Ä., auf denen personenbezogene Daten gespeichert sind (unabhängig davon, in wessen Eigentum sich das Endgerät/der Datenträger befindet);
- Einbruch in Räumlichkeiten und Entwendung von Dokumenten, die personenbezogene Daten enthalten;
- Aussendung einer E-Mail an mehrere Personen im CC, ohne das ein eindeutiger, festgelegter und legitimer Zweck für die Führung der Personen im CC vorliegt;



- Hackerangriff;
- Login einer fremden/unbefugten Person in einen Account.

Sobald ein (möglicher) Data Breach bemerkt wird, ist dieser umgehend an databreach@tugraz.at oder über das Online-Formular (<https://security.tugraz.at/datenschutz/dsgvo/databreach/>) unter Bekanntgabe aller bekannten Informationen zu melden. Sollte Unklarheit darüber bestehen, ob ein relevanter Vorfall vorliegt, ist trotzdem eine interne Meldung zu empfehlen

**Tipp: Besser einmal zu oft melden,
als einmal zu wenig.**

Eine sofortige Meldung ist äußerst wichtig, da die TU Graz einen potentiellen Vorfall **innerhalb von 72 Stunden an die Datenschutzbehörde melden** muss (keine Fristhemmung an Wochenenden oder Feiertagen). Innerhalb dieser Frist erfolgt eine interne Evaluierung des Vorfalls durch die Datenschutzkoordination, das IT-Security-Team und den Datenschutzbeauftragten. Dabei wird geprüft, ob durch den Vorfall ein Risiko für die Rechte und Freiheiten der betroffenen Personen gegeben ist und dadurch eine tatsächliche Meldepflicht durch die TU Graz an die Datenschutzbehörde vorliegt.

Weiterführende Informationen sind unter <https://security.tugraz.at/datenschutz/dsgvo/databreach/> abrufbar.



2.2.12. VERARBEITUNGSVERZEICHNIS (TOOL PROVENTOR)

Verantwortliche und Auftragsverarbeiter sind gesetzlich dazu verpflichtet, ein Verarbeitungsverzeichnis (VVZ) zu führen (Art 30 DSGVO). Das VVZ stellt eine Übersicht aller Verarbeitungstätigkeiten personenbezogener Daten dar. Dadurch erfüllt die TU Graz die Rechenschaftspflicht gegenüber der Aufsichtsbehörde, welche dann – im Anlassfall einer Beschwerde oder auch von Amts wegen – ihre Kontrollrechte ausüben kann.

An der TU Graz wird für die Dokumentation von Verarbeitungsvorgängen das Tool „PROVENTOR“ verwendet. Einträge werden dabei auf Prozess-Ebene vorgenommen. Die zentralen Organisationseinheiten verfügen über einen Zugang zu diesem Tool, dessen Einträge von den Organisationseinheiten laufend zu evaluieren und bei Änderungen entsprechend zu aktualisieren sind.

Weiterführende Informationen zum VVZ finden Sie unter <https://tu4u.tugraz.at/go/vvz>.

2.2.13. DATENSCHUTZ- FOLGENABSCHÄTZUNG

Hat eine Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen, sind Verantwortliche und Auftragsverarbeiter gesetzlich dazu verpflichtet eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (Art 35 DSGVO).

⁸ Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II. Nr. 278/2018.

⁹ Datenschutz-Folgenabschätzung-Ausnahmen-Verordnung (DSFA-AV), BGBl. II Nr. 108/2018.

Die österreichische Datenschutzbehörde hat in diesem Zusammenhang zwei Verordnungen erlassen, nämlich die sog. „Blacklist-VO“⁸ und die sog. „Whitelist-VO“⁹. Während die Blacklist jene Verarbeitungen auflistet, im Zuge derer jedenfalls eine DSFA durchzuführen ist (z.B. beim Einsatz neuer Technologien), enthält die Whitelist einen Ausnahmekatalog von Verarbeitungen, für die die Durchführung einer DSFA nicht erforderlich ist (z.B. für Forschungsverarbeitungen).



© Kinn Studio-AdobeStock

3. Lehre

3.1. ERFÜLLUNG DER INFORMATIONSPFLICHT GEGENÜBER DEN STUDIERENDEN

Die Informationspflicht gegenüber den Studierenden wird bei der Zulassung bzw. über die gesammelten Datenschutzerklärungen auf der Webseite der OE Studienservice <https://www.tugraz.at/tu-graz/organisationsstruktur/serviceeinrichtungen-und-stabsstellen/studienservice/> erfüllt.

Zusätzlich werden Informationen zum Datenschutz im Einzelfall vor der Verwendung von spezifischen Tools erteilt (z.B. TeachCenter).

Werden über die allgemeinen Datenschutzerklärungen hinaus personenbezogene Daten von Studierenden verarbeitet (z.B. Fotoaufnahmen im Rahmen von Exkursionen in Lehrveranstaltungen), wird empfohlen, die Studierenden vorab darüber zu informieren bzw. im Falle der Veröffentlichung in externen Medien eine freiwillige Einwilligung nach Art 6 DSGVO einzuholen. Im Zuge der Veröffentlichung auf Social-Media-Plattformen ist verpflichtend eine freiwillige Einwilligung nach Art 49 DSGVO erforderlich.

Die Information kann u.a. durch die Verwendung der Vorlagen im TU4U (<https://tu4u.tugraz.at/go/ds-vorlagen>) sowie deren Implementierung z.B. im TeachCenter erfolgen.



3.2. AUFBEWAHRUNGSFRISTEN IM BEREICH DER LEHRE

¹⁰ TU Graz, Vizerektorat
Lehre, BOOKLET: LEHRE
AN DER TU GRAZ (2021)
69 (70).

Bitte beachten Sie hierzu die Information aus dem Booklet: Lehre an der TU Graz.¹⁰

3.2.1. BEURTEILUNGSUNTERLAGEN

Die Beurteilungsunterlagen (insbesondere Korrekturen schriftlicher Prüfungen und Prüfungsarbeiten) sind, insofern sie nicht den Studierenden ausgehändigt werden, mindestens sechs Monate und maximal ein Jahr aufzubewahren (§ 79 Abs 5 UG¹¹, Satzungsteil Studienrecht¹²).

¹¹ Bundesgesetz über die
Organisation der Universität
und ihre Studien (Univer-
sitätsgesetz 2002 – UG),
BGBl I 120/2002
idF I 177/2021.

¹² Satzungsteil Studien-
recht der TU Graz,
SA 92000 STSR 124-03,
§ 22 Abs 4.

Ebenfalls für mindestens sechs Monate aufzubewahren ist das Prüfungsprotokoll. Dieses verbleibt meist bei den Prüfenden selbst und enthält Prüfungsgegenstand, Ort bzw. Form und Beginn/Ende der Prüfung, den Namen der prüfenden Person oder die Namen der Mitglieder der Prüfungskommission, die Namen der Studierenden, die gestellten Fragen, die erteilten Beurteilungen, die Gründe für die negative Beurteilung sowie allfällige besondere Vorkommnisse.

¹³ TU Graz, Vizerektorat
Lehre, BOOKLET: LEHRE
AN DER TU GRAZ (2021)
80 (81).

¹⁴ Satzungsteil Plagiat der
TU Graz, SA 91000 PLAG
150-02, § 2; Satzungsteil
Studienrecht der TU Graz,
SA 92000 STSR 124-03,
§ 22.

3.2.2. BACHELORARBEITEN, SEMINARARBEITEN

Um wissenschaftliches Fehlverhalten zu erkennen, können Bachelor¹³- und Seminararbeiten zum Zweck der elektronischen Plagiatskontrolle über die für die Aufbewahrung von Beurteilungsunterlagen genannten Fristen hinaus gespeichert werden.¹⁴

3.2.3. AUFBEWAHRUNG VON UNIVERSITÄTSSPEZIFISCHEN DATEN (PRÜFUNGSDATEN)

Im BilDokG¹⁵ sind jene personenbezogenen Daten von Studierenden aufgezählt, die zu deren Evidenzhaltung notwendig sind, wie z.B. Matrikelnummer, Namen, Geburtsdatum, Staatsangehörigkeit, Geschlecht, Anschrift am Heimatort oder E-Mail-Adresse.¹⁶

¹⁵ Bundesgesetz über die Dokumentation im Bildungswesen (Bildungsdokumentationsgesetz 2020 – BilDokG 2020), BGBl I 20/2021 idF I 227/2022.

¹⁶ § 9 BilDokG 2020.

Nach dem UG sind Prüfungsdaten für mindestens 80 Jahre in geeigneter Form aufzubewahren.

Folgende Daten sind davon umfasst:¹⁷

¹⁷ § 53 UG IVm § 9 Z 15 BilDokG 2020.

- 1.) Bezeichnung von Prüfungen oder das Thema der wissenschaftlichen oder künstlerischen Arbeiten;
- 2.) die vergebenen ECTS-Anrechnungspunkte;
- 3.) die Beurteilung;
- 4.) die Namen der prüfenden oder der beurteilenden Personen;
- 5.) das Datum der Prüfung oder der Beurteilung;
- 6.) der Name und die Matrikelnummer der oder des Studierenden;
- 7.) Studienberechtigungsprüfung;
- 8.) Daten des Eignungs-, Aufnahme- und Auswahlverfahrens;



In Erfüllung dieser gesetzlichen Vorgabe werden die genannten Daten von der TU Graz zentral durch das Informations- und Verwaltungssystem TUGRAZonline aufbewahrt.

3.2.4. RAUMEINTEILUNGEN

Grundsätzlich lässt sich feststellen, dass Raumeinteilungen in den meisten Fällen personenbezogene Daten enthalten (z.B. Matrikelnummer), weshalb die damit verbundene Verarbeitung in den Anwendungsbereich der DSGVO bzw. des DSG fällt. Es wird daher empfohlen, Raumeinteilungen im Rahmen der technischen Möglichkeiten grundsätzlich in digitaler Form vorzunehmen, wobei die Grundsätze Privacy by Design und Privacy by Default zu beachten sind (siehe 2.2.10.). Eine Veröffentlichung von Raumeinteilungen wird nicht empfohlen.

3.3. VERÖFFENTLICHUNGEN IM RAHMEN VON MÜNDLICHEN (ABSCHLUSS-)PRÜFUNGEN

Aus dem UG sowie dem Satzungsteil Studienrecht der TU Graz ergibt sich, dass mündliche (Abschluss-)Prüfungen grundsätzlich öffentlich stattfinden haben. Ziel dieser Regelung ist es, eine gewisse Objektivität und Kontrolle von Prüfungsentscheidungen zu garantieren (Zweck der Bestimmung)¹⁸. Die öffentliche Verkündung des Prüfungsergebnisses im Rahmen von mündlichen Prüfungen ist daher aus datenschutzrechtlicher Sicht unbedenklich.

¹⁸ Vgl. BOOKLET: LEHRE AN DER TU GRAZ, 66.

In Ermangelung eines festgelegten, eindeutigen und legitimen Zwecks wird die **namentliche** Veröffentlichung von Prüfungskandidat*innen (z.B. durch öffentlichen Aushang) aus datenschutzrechtlicher Sicht nicht empfohlen.

3.4. VERÖFFENTLICHUNGEN IM RAHMEN VON SCHRIFTLICHEN PRÜFUNGEN

Prüfungsergebnisse von schriftlichen Prüfungen dürfen nur der konkreten geprüften Person zugänglich gemacht werden. Eine Veröffentlichung von Prüfungsergebnissen in Kombination z.B. mit Namen/Matrikelnummer sollte daher unterbleiben. Eine Veröffentlichung im TU Graz TeachCenter für alle Teilnehmenden oder ein Aussenden von PDF-Notenlisten stellt eine Verletzung des Datenschutzrechts dar.

3.5. UNTERSCHRIFTENLISTEN UND ANWESENHEITSLISTEN

In Lehrveranstaltungen mit Anwesenheitspflicht muss die Anwesenheit der Studierenden nachgewiesen und dokumentiert werden. Unterschriften- bzw. Anwesenheitslisten, die diesen Zweck erfüllen, sind auch aus datenschutzrechtlicher Sicht unbedenklich. Beachten Sie dabei allerdings, nur relevante Daten zu erheben und die Liste nach frühestens sechs Monaten bzw. spätestens einem Jahr (da es sich um Beurteilungsunterlagen handelt) zu löschen.



3.6. FOTOS UND VIDEOS IM RAHMEN VON LEHRVERANSTALTUNGEN/ EXKURSIONEN

Möchten Sie im Einzelfall im Zuge einer Lehrveranstaltung/Exkursion Fotos und/oder Videos anfertigen, achten Sie bitte – wie unter dem Punkt Veranstaltungen (siehe 5.3.) detaillierter ausgeführt – auf die Einhaltung der wesentlichen Punkte: Informieren Sie die Betroffenen (in der Regel Studierende) darüber, dass Fotos und/oder Videos gemacht werden; ob und wo diese veröffentlicht werden; dass sie insbesondere ein Widerspruchsrecht haben, welches sie am besten bereits vor der Lehrveranstaltung/Exkursion ausüben, indem sie der Leitung zu erkennen geben, dass sie nicht fotografiert und/oder gefilmt werden möchten.

Es wird empfohlen, die Informationspflicht durch eine eigene Datenschutzerklärung möglichst frühzeitig zu erfüllen. Eine Vorlage dazu finden Sie im TU4U unter „Datenschutzerklärung für Exkursionen“.

Möchten Sie Fotos und/oder Videos der Studierenden an Externe weitergeben bzw. auf Social-Media-Kanälen veröffentlichen, ist die Einholung einer freiwilligen Einwilligung notwendig.

3.7. AUSSENDEN VON ZWISCHENERGEBNISSEN

Zwischenergebnisse können mit dem Programm „Serienbrief“ ausgesendet werden. Nähere Informationen zur technischen Vorgehensweise erhalten Sie unter <https://bigmailtugraz.at/verteiler/faq.shtml>.



3.8. ABGABEN/EINSICHTNAHME

Bitte beachten Sie hierzu die Information aus dem Booklet: Lehre an der TU Graz.¹⁹

¹⁹ BOOKLET: LEHRE AN DER TU GRAZ, 69.

Die Einsichtnahme ist so zu gestalten, dass Informationen grundsätzlich nur betroffenen Studierenden zugänglich gemacht bzw. mitgeteilt werden. Ebenso empfiehlt sich für die Abgabe von Hausübungen z.B. ein verschließbares Postfach oder ein Briefkasten am Sekretariat.

3.9. DATENSCHUTZ- UND GEHEIMHALTUNGSVERPFLICHTUNG BEI ABSCHLUSSARBEITEN

Werden Abschlussarbeiten durch externe Gutachter*innen begutachtet, ist der Abschluss einer Datenschutz- und Geheimhaltungsverpflichtung zu empfehlen.

Beispiel: Wird die Dissertation von Dekanats- oder Institutsbediensteten an externe Gutachter*innen übermittelt, wird den Gutachter*innen von diesen eine Datenschutz- und Geheimhaltungsverpflichtung zur vorherigen Unterzeichnung vorgelegt. Wird die Dissertation von dem*der Dissertanten*in eigenständig an die Gutachter*innen übermittelt, wird angeraten, diese auf die Übermittlung der Datenschutz- und Geheimhaltungsverpflichtung hinzuweisen.



Nähere Informationen zum Prozess sowie eine Vorlage der Datenschutz- und Geheimhaltungsverpflichtung für externe Gutachter*innen finden Sie im TU4U unter <https://tu4u.tugraz.at/studierende/mein-studienabschluss/dissertation/>.

3.10. VERÖFFENTLICHUNGEN IM RAHMEN VON ABSCHLUSSFEIERN

Die Veröffentlichung der Namen der Teilnehmenden sowie die Verlesung von bestimmten Daten wie z.B. Geburtsdatum oder Datum der Reifeprüfung ist im Rahmen von Abschlussfeiern aus datenschutzrechtlicher Sicht grundsätzlich möglich. Es wird aber empfohlen, die Studierenden im Zuge der Anmeldung zur Abschlussfeier mittels einer kurzen Datenschutzerklärung über die Verlesung zu informieren. Eine Vorlage ist unter datenschutz@tugraz.at erhältlich. Eine Einwilligung der Teilnehmenden ist in diesem Fall daher nicht erforderlich.

Werden personenbezogene Daten im Zuge des Studienabschlusses oder Abschlussfeiern an Externe weitergegeben (z.B. Zeitung, andere Hochschule etc.), ist vorab eine freiwillige Einwilligung der Absolvent*innen erforderlich.

3.11. VIRTUELLE LEHRE

Vorgaben zum Umgang mit personenbezogenen Daten im Zusammenhang mit virtueller Lehre finden Sie im Abschnitt IV des Satzungsteils Studienrecht der TU Graz.

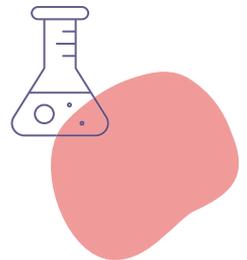


4. Forschung

4.1. DATENSCHUTZ IN DER FORSCHUNG

In der Forschung nehmen Daten eine zentrale Rolle ein. Welche rechtlichen Bestimmungen im konkreten Forschungsprojekt zu beachten sind, hängt zunächst davon ab, ob es sich bei den dabei verarbeiteten Daten um personenbezogene oder nicht-personenbezogene Daten handelt (siehe 1.2.). Nicht-personenbezogene Daten bzw. anonyme Daten lassen keinen Rückschluss (mehr) auf eine natürliche Person zu, sodass diese nicht unter die Bestimmungen der DSGVO fallen. In diesem Fall empfehlen wir dennoch zu prüfen, ob und wenn ja, welche anderen rechtlichen Bestimmungen zu beachten sind (z.B. Gesetz, Verordnung, Vertrag oder Richtlinie). Kommt es zu einer Verarbeitung von personenbezogenen Daten, sind für das konkrete Forschungsprojekt die Regeln der DSGVO anzuwenden. Gleiches gilt für gemischte Datensätze, wenn also personenbezogene und nicht personenbezogene Daten untrennbar miteinander verbunden sind. Im Forschungskontext kann zwischen den zwei folgenden Gruppen personenbezogener Daten unterschieden werden:

- 1.) Daten, die für die Verwaltung eines Forschungsprojekts verarbeitet werden (z.B. Stundenlisten, Abrechnungen, Lohnkonten, Dienstverträge – „administrative Forschungsdaten“) und



- 2.) Daten, die Gegenstand des wissenschaftlichen Forschungsprojekts sind (z.B. Proband*innen-Daten, Ergebnisse, Publikationen – „inhaltliche Forschungsdaten“).

4.2. ROLLENVERTEILUNG

Im Zusammenhang mit Forschungsverarbeitungen lassen sich in der DSGVO grundsätzlich drei verschiedene Rollen mit jeweils unterschiedlichen rechtlichen Pflichten unterscheiden:

1.) Verantwortlicher ist, wer die Zwecke (das „Warum“) und Mittel (das „Wie“) einer Verarbeitung festlegt. Entscheiden Forscher*innen – und damit die TU Graz – in einem Forschungsprojekt über dessen Ausrichtung, Konzeption, Ziel und Thema sowie über die (Einteilung der) Finanzierung oder Fördersumme, ist die TU Graz als Verantwortlicher im Sinne der DSGVO zu sehen. Demnach muss sie die Rechtsgrundlage der Verarbeitung und die Informationspflicht gegenüber Betroffenen sicherstellen sowie die Betroffenenrechte gewährleisten.

2.) Auftragsverarbeiter ist, wer im Auftrag und auf Weisung des Verantwortlichen personenbezogene Daten verarbeitet. Beauftragt die TU Graz in einem Forschungsprojekt ein Unternehmen zur Durchführung einer Dienstleistung, wird das Unternehmen als Auftragsverarbeiter für die TU Graz tätig. Wird hingegen die TU Graz mit der Durchführung einer Dienstleistung von einem Unternehmen beauftragt, ist sie Auftragsverarbeiter für das Unternehmen. In diesen Fällen ist der Abschluss



eines Auftragsverarbeitungsvertrages nach Art 28 DSGVO angezeigt, siehe Vorlage im TU4U (<https://tu4u.tugraz.at/go/ds-forschung>) auf Deutsch und Englisch.

3.) Gemeinsame Verantwortung liegt vor, wenn zwei oder mehrere Verantwortliche gemeinsam über die Zwecke und Mittel einer Verarbeitung entscheiden. Wenn also in einem gemeinsamen Forschungsprojekt z.B. zwischen TU Graz und Uni Graz beide Universitäten dessen Ausrichtung und Finanzierung festlegen, liegt eine gemeinsame Verantwortung vor. In diesem Fall ist der Abschluss einer Vereinbarung über die gemeinsame Verantwortung nach Art 26 DSGVO angezeigt, siehe Vorlage im TU4U (<https://tu4u.tugraz.at/go/ds-forschung>) auf Deutsch und Englisch.

4.3. RECHTSGRUNDLAGEN

4.3.1. DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Werden im Zuge des konkreten Forschungsprojekts personenbezogene Daten (administrative und/oder inhaltliche Forschungsdaten) verarbeitet, kommen neben den rechtlichen Bestimmungen der DSGVO gleichzeitig stets jene nach dem Datenschutzgesetz (DSG) und dem Forschungsorganisationsgesetz (FOG) in Betracht. Da die Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist (siehe 2.2.1.), wird zunächst eine Ausnahme benötigt. Für administrative Forschungsdaten kommt einer der in Art 6 DSGVO aufgezählten Ausnahme- bzw. Rechtmäßigkeitsgründe zur Anwendung.

Um das Spannungsverhältnis zwischen dem Grundrecht auf Wissenschaftsfreiheit und jenem auf Datenschutz aufzulösen, enthält die DSGVO eine Wissenschaftsprivilegierung. Unter Setzung entsprechender Datensicherheitsmaßnahmen (z.B. Zutritts- und Zugriffsbeschränkung sowie Verschlüsselung) greift für inhaltliche Forschungsdaten daher die Ausnahme in Art 89 DSGVO, die stets gleichzeitig mit § 7 DSG zu lesen ist.

4.3.2. DATENSCHUTZGESETZ (DSG)

Wenn das Ziel des konkreten Forschungsprojekts keine personenbezogenen Ergebnisse sind, dürfen diese nach dem DSG in drei Fällen verarbeitet werden, nämlich erstens, wenn die Daten öffentlich zugänglich sind, zweitens, wenn die Daten bereits für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt wurden, oder drittens, wenn es sich bei den Daten um pseudonymisierte Daten handelt (siehe 1.6.) und Forscher*innen den Personenbezug mit rechtlich zulässigen Mitteln nicht mehr herstellen können (§ 7 Abs 1 DSG).

Treffen die genannten Voraussetzungen auf das konkrete Forschungsprojekt nicht zu, ist im nächsten Schritt zu prüfen, ob für die konkrete Verarbeitung eine besondere gesetzliche Vorschrift zur Anwendung kommt (z.B. aus dem FOG, siehe 4.3.3.), die Einwilligung der Betroffenen bzw. Proband*innen eingeholt werden muss oder gegebenenfalls eine Genehmigung durch die österreichische Datenschutzbehörde erforderlich ist (§ 7 Abs 2 DSG).

4.3.3. FORSCHUNGSORGANISATIONS-GESETZ (FOG)

Wenn für das konkrete Forschungsprojekt keine der Rechtsgrundlagen in § 7 DSGVO einschlägig ist, kommt § 2d FOG in Betracht. Nach dieser Bestimmung dürfen Universitäten personenbezogene Daten für Forschungszwecke grundsätzlich verarbeiten. Voraussetzung dafür ist, dass diese entweder pseudonymisiert werden oder Veröffentlichungen nicht oder nur in anonymisierter oder pseudonymisierter Form erfolgen (§ 2d Abs 2 Z 1 FOG).

Für die Frage, welche Rechtsgrundlage in Ihrem Forschungsprojekt zur Anwendung kommt, kontaktieren Sie gerne die Datenschutzkoordination unter datenschutz@tugraz.at.

4.4. GRUNDSÄTZE DER DSGVO

In 2.2. werden die Grundsätze der DSGVO erläutert, die grundsätzlich auch im Forschungskontext zu beachten sind. Gleichzeitig gibt es im Zusammenhang mit Forschungsverarbeitungen einige „Aufweichungen“ von den strengen DSGVO-Grundsätzen:

Dem **Grundsatz der Zweckbindung** zufolge dürfen personenbezogene Daten nur dann verarbeitet werden, wenn dafür ein Zweck festgelegt wird, der eindeutig ist und gegen keine rechtlichen Vorschriften verstößt. Eine Weiterverarbeitung von personenbezogenen Daten ist im Forschungskontext grundsätzlich möglich (Art 5 Abs 1 lit b DSGVO).





Beispiel: Wenn es im konkreten Forschungsprojekt um Verkehrsprävention geht, könnte der festgelegte Zweck der Verarbeitung wie folgt lauten: „Forschungsprojekt A zur Erarbeitung von neuen Methoden der Verkehrsprävention“.

Nach dem **Grundsatz der Datenminimierung** dürfen nur jene personenbezogenen Daten verarbeitet werden, die unbedingt erforderlich sind, um den festgelegten Zweck zu erreichen. Daraus folgt eine 3-Stufen-Prüfung (Art 89 Abs 1 iVm Art 5 Abs 1 lit c und Art 6 Abs 4 DSGVO):

Stufe 1: Wenn der Zweck des konkreten Forschungsprojektes auch mit nicht-personenbezogenen Daten erreicht werden kann, sollten lediglich anonyme Daten verarbeitet werden.

Stufe 2: Wenn der Zweck nicht mit anonymen Daten erreicht werden kann, ist zu prüfen, ob der Zweck auch mit personenbezogenen Daten in pseudonymisierter Form erreicht werden kann.

Stufe 3: Erst wenn der Zweck weder mit anonymen noch mit pseudonymisierten Daten erreicht werden kann, können personenbezogene Daten in nicht-pseudonymisierter Form verarbeitet werden.





Beispiel: In einem konkreten Forschungsprojekt wird der Zweck verfolgt, neue Methoden der Verkehrsprävention zu erarbeiten. Aus diesem Grund füllen 20 Proband*innen Fragebögen aus und nehmen an Probefahrten auf einem Testgelände teil. Der Zweck kann nicht mit anonymen Daten erreicht werden, weil die Angaben der Proband*innen in den Fragebögen mit ihren jeweiligen Probefahrten in Verbindung gesetzt werden (Stufe 1). Da der Zweck nicht mit anonymen Daten erreicht werden kann, empfehlen wir die Dokumentation der diesbezüglichen Gründe. Nach Prüfung der Stufe 2 kommen Forscher*innen zum Ergebnis, dass der von ihnen festgelegte Zweck mit pseudonymisierten Daten erreicht werden kann.

Beispielsweise kann den Proband*innen jeweils ein Code zugewiesen werden, den die Forscher*innen auf einer Liste notieren (z.B. „Max Mustermann“ = Code 1234/5). Auf einer anderen Liste verknüpfen die Forscher*innen den Code mit dem jeweiligen Fragebogen und der jeweiligen Probefahrt der Proband*innen. Diese Zuordnungsliste wird zugangs- und zutrittsverschlüsselt aufbewahrt, sodass nur die im Projektbeteiligten Forscher*innen bzw. ausgewählte Mitarbeiter*innen zum Zweck der Auswertung den Personenbezug herstellen können. Sobald der Personenbezug für die Forscher*innen nicht mehr relevant ist, löschen diese die Zuordnungsliste. Damit liegen anonymisierte Daten vor.

Dem **Grundsatz der Speicherbegrenzung** zufolge dürfen personenbezogene Daten nur solange gespeichert werden, wie es für den festgelegten

Verarbeitungszweck erforderlich ist. Bei Verarbeitungen im Forschungskontext kann eine Speicherung auch länger erfolgen, nämlich dann, wenn geeignete technische und organisatorische Maßnahmen wie z.B. Zugriffs-, Zutrittskonzept und Verschlüsselung durchgeführt werden (Art 5 Abs 1 lit e DSGVO).

4.5. AUFBEWAHRUNGSFRISTEN VON FORSCHUNGSDATEN

Die DSGVO enthält keine konkreten Aufbewahrungsfristen, sondern gibt diesbezüglich nur allgemeine Grundsätze vor (siehe 2.2.5.). Wenn in gesetzlichen Bestimmungen, internen Richtlinien oder in Verträgen (Fördervertrag, Konsortialvertrag etc.) nichts Abweichendes bestimmt ist, gilt Folgendes:

Administrative Forschungsdaten sind an der TU Graz längstens nach 15 Jahren zu löschen.

Inhaltliche Forschungsdaten dürfen aufgrund der Wissenschaftsprivilegierung der DSGVO auch länger gespeichert werden, sofern geeignete technische und organisatorische Maßnahmen durchgeführt werden (z.B. Zugriffs- und Zutrittskonzept).

Der TU-internen Richtlinie zur Sicherung guter wissenschaftlicher Praxis zufolge sind „für Veröffentlichungen grundlegende Daten unbeschadet anderer gesetzlicher Bestimmungen auf haltbaren und gesicherten Trägern in der Institution, in der sie generiert wurden, für mindestens 10 Jahre aufzubewahren, soweit dies möglich und zumutbar ist“.²⁰

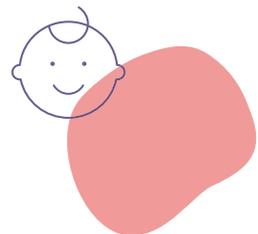
²⁰ TU Graz, Richtlinie zur Sicherung guter wissenschaftlicher Praxis, RL 92000 SGWP 050-04, § 4.



Beispiel: Wenn nichts Abweichendes bestimmt ist, empfehlen wir die Löschung der administrativen Forschungsdaten, also der Stundenlisten, Abrechnungen, Lohnkonten, Dienstverträge usw. 15 Jahre nach Abschluss des konkreten Forschungsprojekts. Inhaltliche Forschungsdaten (im vorangegangenen Beispiel wären das die ausgefüllten Fragebögen, die Auswertungen, Zuordnungslisten, Aufzeichnungen über die Probefahrt der Proband*innen, deren Einwilligungen und Informationen usw. sind zum Nachweis guter wissenschaftlicher Praxis – soweit möglich und zumutbar – mindestens 10 Jahre lang zu speichern.

4.6. VERARBEITUNG VON PERSONENBEZOGENEN DATEN VON KINDERN

Die Verarbeitung von personenbezogenen Daten von unmündigen Minderjährigen (Kinder bis zum 14. Lebensjahr) ist nur rechtmäßig, wenn ein Träger der elterlichen Verantwortung die Einwilligung in die Datenverarbeitung erteilt (Art 8 DSGVO iVm § 4 DSGVO). Mündige Minderjährige (Kinder ab dem vollendeten 14. Lebensjahr) können selbst in die Datenverarbeitung einwilligen. Diese Altersgrenzen beziehen sich jedoch nur auf das Datenschutzrecht, weshalb sie keine Anwendung auf z.B. zugrundeliegende Vertragsverhältnisse haben. Hier kommen weiterhin die Rechtsnormen des österreichischen Zivilrechts zur Anwendung (in Bezug auf Geschäftsfähigkeit bzw. Einsichts- und Urteilsfähigkeit).



Der Verantwortliche muss zur Einholung der Einwilligung der Träger der elterlichen Verantwortung im Rahmen der verfügbaren Technik angemessene Anstrengungen unternehmen, um sicherzustellen, dass die Einwilligung tatsächlich von diesen erteilt wurde (z.B. im Online-Kontext Authentifizierung durch die elektronische Signatur der Träger der elterlichen Verantwortung; Bestätigungslink an die E-Mail-Adresse des Trägers der elterlichen Verantwortung).

Datenschutzinformationen (siehe 2.2.8.), die den Betroffenen in diesem Zusammenhang bereitzustellen sind, sollten vom Verantwortlichen in einfacher und verständlicher Sprache möglichst kindgerecht aufbereitet und formuliert werden (Art 12 Abs 1 DSGVO).

4.7. EMPFOHLENE VORGEHENSWEISE

4.7.1. ABKLÄRUNG DER ORGANISATORISCHEN UND RECHTLICHEN RAHMENBEDINGUNGEN

Wenn Ihr Forschungsprojekt einen arbeitsrechtlichen Bezug aufweist (z.B. weil Arbeitnehmer*innen der TU Graz als Proband*innen mitwirken sollen), empfehlen wir zur arbeitsrechtlichen Abklärung die Kontaktaufnahme mit dem **Vizerektorat für Personal und Finanzen**. Zur allgemeinen rechtlichen Abklärung (z.B. Zivilrecht, Versicherung etc.) kontaktieren Sie die **OE Recht und Versicherungsmanagement**.



4.7.2. ABKLÄRUNG DATENSCHUTZ-RECHTLICHER IMPLIKATIONEN

Ist im Rahmen Ihres geplanten Forschungsvorhabens die Verarbeitung personenbezogener Daten vorgesehen (siehe 1.2.), kontaktieren Sie die **Datenschutzkoordination** unter datenschutz@tugraz.at.



© Kinn Studio – AdobeStock

5. Verwaltung

5.1. EINLEITUNG

Die Handlungsanleitungen bzw. Vorgehensweise im Zuge der diversen Verwaltungstätigkeiten sind im TU4U-Bereich der zuständigen Fachabteilungen bzw. in den internen Richtlinien und Verordnungen beschrieben. Die dort abgebildeten Prozesse entsprechen grundsätzlich den datenschutzrechtlichen Vorgaben (Abrechnung von Dienstreisen, Reisekostenabrechnung von Gastvortragenden, Kurzkrankenstände, Archivierungen etc.).

Den Bediensteten der TU Graz steht im TU4U ein kurzes und kompaktes Informationsblatt zu einigen wichtigen Punkten des Datenschutzes und der Datensicherheit zur Verfügung (<https://tu4u.tugraz.at/bedienstete/organisation-und-administration/datenschutz-und-datensicherheit/forschung-lehre-und-verwaltung/verwaltung/datenschutz-informationsblatt-fuer-arbeitnehmerinnen>).

5.2. PERSONAL

5.2.1. BEWERBUNGEN

Die Personalabteilung informiert Bewerbende in ihrer Datenschutzerklärung über die Verarbeitung der personenbezogenen Daten im Rahmen des Bewerbungsverfahrens.

Die Löschung/Anonymisierung der personenbezogenen Bewerbungsdaten wird im System automa-

tisch sieben Monate nach Abschluss des Bewerbungsverfahrens durchgeführt. Physische Bewerbungsdaten sind entsprechend der genannten Frist datenschutzkonform zu vernichten. Eine längere Speicherung der Daten ist nur nach vorheriger freiwilliger Einwilligung der Bewerbenden zum Zweck der Evidenzhaltung möglich (18 Monate).

Weshalb sollten Bewerbungsdaten sieben Monate aufbewahrt werden?

Bewerbende können Ansprüche nach § 29 Abs 1 GlBG²¹ (Verletzung des Gleichbehandlungsgebotes auf Grund ethnischer Zugehörigkeit, Religion oder Weltanschauung, Alter oder sexuelle Orientierung) binnen sechs Monaten gerichtlich geltend machen. Die Bewerbungsunterlagen sind somit zur etwaigen Beweisführung notwendig. Die sieben Monate ergeben sich aus der Zustellung bzw. dem Postweg im Zuge der gerichtlichen Geltendmachung von Ansprüchen.

²¹ Bundesgesetz über die Gleichbehandlung (Gleichbehandlungsgesetz – GlBG), BGBl I 66/2004 idF I 16/2020.

5.2.2. INITIATIVBEWERBUNGEN / EVIDENZHALTUNG VON BEWERBUNGEN

Für Initiativbewerbungen, die nicht von Relevanz sind, wird grundsätzlich eine umgehende Löschung empfohlen.

Initiativbewerbungen, die von Relevanz sind, oder Bewerbungsunterlagen in einem laufenden Bewerbungsverfahren, die für zukünftige Stellen von Interesse sind, können unter Einholung einer Einwilligung der Bewerbenden zum Zweck der Evidenzhaltung aufbewahrt werden. Nach Ablauf der vereinbarten Frist empfiehlt sich die neuerliche Einholung einer Einwilligung zur Evidenzhaltung oder die Löschung der Bewerbungsdaten.

5.2.3. DATENSCHUTZINFORMATION FÜR (NEUE) BEDIENSTETE

(Neue) Bedienstete werden bei Dienstantritt über die Verarbeitung von personenbezogenen Daten im Arbeitsverhältnis informiert. Die Datenschutzerklärung für (neue) Bedienstete der TU Graz ist im TU4U-Bereich der Personalabteilung abrufbar.

5.2.4. GEBURTSTAGSKALENDER

Das digitale und analoge Führen von Geburtstagskalendern wird grundsätzlich nicht empfohlen.

5.2.5. MITARBEITER*INNENGEsprÄCHE

Die Protokolle der Mitarbeiter*innengespräche können zwei bis drei Jahre aufbewahrt werden. Damit soll es den Beteiligten ermöglicht werden, besprochene Ziele bzw. Vereinbarungen rückwirkend einzusehen. Vereinbarte Schritte der Vorjahre können somit in den jährlich durchzuführenden Mitarbeiter*innengesprächen evaluiert werden.

Der Inhalt des Gesprächs ist vertraulich und hat damit nur zwischen den Gesprächspartner*innen zu verbleiben (Führungskraft und der*dem jeweiligen Bediensteten). Eine zentrale Aufbewahrung am Sekretariat wird daher nicht empfohlen. Analog kann die Aufbewahrung in Papierform in versperrten Schränken der Führungskraft und bei den Bediensteten erfolgen. In digitaler Form kann dieses von Bediensteten eingescannt, in der Cloud abgelegt und mit der Führungskraft geteilt werden.

Eine weitere Möglichkeit wäre die Speicherung des Protokolls am persönlichen Laufwerk.

5.2.6. GEHEIMHALTUNGSVERPFLICHTUNG

Bedienstete und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis, die im Rahmen ihrer berufsmäßigen Beschäftigung personenbezogene Daten verarbeiten, sind von Arbeitgeberseite zur Geheimhaltung dieser Daten zu verpflichten (ausgenommen eine solche besteht schon kraft Gesetzes). Im Regelfall werden die Bediensteten und Personen in einem arbeitnehmerähnlichen Verhältnis in den Arbeits- bzw. Dienstverträgen zur Wahrung des Datengeheimnisses nach § 6 DSGVO verpflichtet. Bestehen Zweifel, ob eine Person durch eine solche Klausel zur Geheimhaltung verpflichtet wurde, wird eine diesbezügliche Abklärung mit der Personalabteilung empfohlen.



5.2.7. AUFBEWAHRUNG VON PERSONENBEZOGENEN PERSONALDATEN

Im Allgemeinen werden Personalakten in der OE Personalabteilung aufbewahrt und sind nicht dezentral an den Instituten/OE zu führen.

Davon ausgenommen sind zwei Arten von Dokumenten, die dezentral zu verwalten sind:

- 1.) Originale Reisebelege
(Aufbewahrung von sieben Jahren)

- 2.) Dienstverträge von Projektmitarbeitenden (die Aufbewahrungsfrist richtet sich nach den Richtlinien bzw. vertraglichen Vereinbarungen mit dem jeweiligen Fördergebern)

5.2.8. VERÖFFENTLICHUNG EHEMALIGER BEDIENSTETER AUF DER (INSTITUTS-)WEBSEITE

Aufgrund der datenschutzrechtlichen Bestimmungen wird für die Verarbeitung von personenbezogenen Daten von ehemaligen Bediensteten (ausgenommen sind ehemalige Leitungspersonen sowie Personen, die im Rahmen von historischen Berichten bzw. von herausragenden Leistungen angeführt werden) die Einholung einer Einwilligung empfohlen.

Da die TU Graz im Zweifelsfall den Nachweis des Vorliegens der Einwilligung zu erbringen hat, empfiehlt es sich diese jedenfalls in Schriftform einzuholen. Um die schriftliche Einholung der Einwilligung zu erleichtern, stellt die Datenschutzkoordination auf Anfrage eine Vorlage für die Einwilligung und der beizulegenden Datenschutzerklärung zur Verfügung.



5.2.9. VERARBEITUNG VON PERSONENBEZOGENEN DATEN VON KINDERN

Siehe 4.6.

5.2.10. VIDEOÜBERWACHUNG

Rechtliche Fragen zur Videoüberwachung betreffen grundsätzlich arbeitsrechtliche Aspekte und sollten deshalb vorab mit dem für das Personal zuständigen Vizerektorat abgeklärt werden. Neben dem Arbeitsrecht ist auch das Datenschutzrecht zu beachten, weshalb im TU4U (<https://tu4u.tugraz.at/go/videoueberwachung>) eine umfassende Handlungsempfehlung zu datenschutzrechtlichen Fragestellungen rund um das Thema Videoanlagen zum Abruf bereit steht.

5.3. VERANSTALTUNGEN UND ÖFFENTLICHKEITSARBEIT

5.3.1. VERANSTALTUNGEN

Im Zusammenhang mit Veranstaltungen treten gleich mehrere datenschutzrechtliche Fragen auf. Eine dieser Fragen ist, wie mit Anmelde- und Teilnehmendenlisten umgegangen werden soll oder ob Fotos von Teilnehmenden/Vortragenden angefertigt und auch veröffentlicht werden dürfen. Im TU4U (<https://tu4u.tugraz.at/go/datenschutz-bei-veranstaltungen>) ist eine umfassende Handlungsempfehlung zu datenschutzrechtlichen und urheberrechtlichen Fragen im Zusammenhang mit Veranstaltungen abrufbar. Es stehen daneben auch

diverse Vorlagen für für Datenschutzerklärungen sowie Hinweisschilder für Foto- und/oder Videoaufnahmen zum Download bereit.

5.3.2. WEBSEITEN

FAQ zu rechtlichen Fragen im Zusammenhang mit Websites sind im TU4U (<https://tu4u.tugraz.at/go/webseitenerstellung-recht>) abrufbar. Diese dienen als Handlungsempfehlung für die Erstellung und Betreuung von Webseiten der TU Graz.

5.3.3. SOCIAL MEDIA (FACEBOOK, INSTAGRAM, X, LINKEDIN ETC.)

Die Veröffentlichung von personenbezogenen Daten (Vor- und Nachname, Fotoaufnahmen etc.) auf Social-Media-Kanälen der TU Graz ist nach derzeitiger Rechtslage grundsätzlich nur nach Einholung einer ausdrücklichen Einwilligung nach Art 49 DSGVO zulässig. Die Einwilligung wird in diesem Fall für die Übermittlung der Daten in ein nicht sicheres Drittland (USA) benötigt.²²

²² Vgl. EuGH 16.06.2020, C-311/18 (Schrems II).

Eine Vorlage für die Einwilligungserklärung sowie für die Datenschutzerklärung ist im TU4U (<https://tu4u.tugraz.at/go/ds-vorlagen>) abrufbar.



5.4. UMGANG MIT KONTAKTDATEN

5.4.1. KONTAKTDATENBANKEN

Im Zuge des Führens von Kontaktdatenbanken sind die oben angeführten Grundsätze zu beachten. Dazu empfiehlt sich eine konsequente Wartung, die insbesondere folgende Punkte sicherstellt:

- Kontaktdaten werden rechtmäßig und transparent verarbeitet (Informationspflicht - Datenschutzerklärung);
- bereits erhobene oder neu erhobene Kontaktdaten werden nur für jene Zwecke verarbeitet, für die sie auch erfasst wurden (Übereinstimmung der Angaben in der Datenschutzerklärung mit den tatsächlichen Verarbeitungszwecken);
- es werden nur jene Daten verarbeitet (und zuvor erfasst), die für die Zweck-erreichung zwingend notwendig sind;
- die Richtigkeit und Aktualität der Daten ist jederzeit sichergestellt;
- dem Stand der Technik entsprechende technische und organisatorische Maßnahmen wurden getroffen, um die Datensicherheit zu gewährleisten;
- die Rechte der betroffenen Personen können jederzeit gewahrt werden, damit z.B. Aussendungen nach einem Widerruf nicht mehr erfolgen.



Beispiele: Die Zweckbindung ist nicht gegeben, wenn Sie Forschungspartner*innen, deren Kontaktdaten Sie zum Zweck der Vernetzung und des fachlichen Austausches im Forschungsgebiet erfasst haben, Einladungen zu Vereinsveranstaltungen zukommen lassen, die in keinem Zusammenhang mit der Forschungstätigkeit stehen.

5.4.2. VERSAND VON EINLADUNGEN UND NEWSLETTERN

Für das Versenden von Einladungen und Newslettern per E-Mail gilt es, die empfangenden Personen grundsätzlich in BCC (Blind Carbon Copy) zu setzen.²³ Kontaktdatenbanken sind unter Berücksichtigung von unzustellbaren Nachrichten (per Post oder per E-Mail) richtig und aktuell zu halten.

²³ Vgl. DSB 11.05.2020, 2020-0.288.477 (Offener Verteiler).

Den empfangenden Personen muss die Möglichkeit gegeben werden, sich von Aussendungen der TU Graz abzumelden bzw. die Löschung aus Kontaktdatenbanken der TU Graz zu beantragen. Diesen Anforderungen kann entsprochen werden, indem in jeder elektronischen oder postalischen Nachricht ein Abmelde-Button oder eine entsprechende (E-Mail-)Adresse enthalten ist, an der die Abmeldung durch Kontaktaufnahme nachschweigend durchgeführt werden kann.

Unter Einhaltung der Grundsätze der DSGVO sind z.B. Einladungen zu Veranstaltungen an Kontakte möglich, die bereits an der gleichen oder einer ähnlichen Veranstaltung (z.B. gleiches Forschungs-

gebiet) teilgenommen haben oder die ihre Einwilligung zum Erhalt von Veranstaltungseinladungen bzw. Newsletter der TU Graz erteilt haben (§ 174 TKG 2021)²⁴.

²⁴ Vgl. Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2021 – TKG 2021), BGBl I 190/2021 idF I 180/2022.

5.4.3. ANSCHREIBEN VON NEUEN KONTAKTEN

Im Zuge der Kontaktaufnahme mit einer natürlichen oder juristischen Person, die durch Internetrecherche ausfindig gemacht wurde, sollte darauf geachtet werden, zu welchem Zweck die natürliche oder juristische Person ihre Kontaktdaten im Internet veröffentlicht hat. Ist dieser Zweck kompatibel mit dem Zweck der Kontaktaufnahme, ist ein Kontaktieren unter Angabe der Datenquelle (z.B. Unternehmenswebseite) grundsätzlich möglich. Je nach Einzelfall ist in weiterer Folge darauf zu achten, dass die Informationspflicht erfüllt und die Grundsätze beachtet werden.

5.4.4. KOMMUNIKATION MIT BEDIENTETEN UND STUDIERENDEN DER TU GRAZ

Zur Kommunikation mit Bediensteten und Studierenden der TU Graz wird empfohlen, ausschließlich die dazu zur Verfügung stehende TU Graz E-Mail-Adresse zu verwenden (sowohl Absender als auch Empfänger).



6. Archivgut

²⁵ Bundesgesetz über die Sicherung, Aufbewahrung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz), BGBl I 162/199 idF I 32/2018.

²⁶ Verordnung des Bundeskanzlers über die Kennzeichnung, Anbietung und Archivierung von Schriftgut des Bundes (Bundesarchivgutverordnung), BGBl II 367/2002 idF II 305/2017.

Handelt es sich bei Daten z.B. nach dem Bundesarchivgesetz²⁵ der Bundesarchivgutverordnung²⁶ bzw. der Archivordnung der TU Graz um Archivgut, so liegt damit eine mögliche gesetzliche Grundlage vor, welche die Aufbewahrung der personenbezogenen Daten legitimiert. Eine Aufbewahrung nach diesen gesetzlichen Bestimmungen wäre zudem ein eindeutiger, festgelegter und legitimer Zweck nach der DSGVO, der dem datenschutzrechtlichen Grundsatz der Speicherbegrenzung entspricht (siehe 2.2.5.). Nähere Informationen zur Aufbewahrung von Unterlagen im Archiv sind im TU4U-Bereich der zuständigen Fachabteilung verfügbar.



7. Kontaktdaten

Datenschutzbeauftragter

x-tention Informationstechnologie GmbH
Römerstraße 80A
4600 Wels
datenschutzbeauftragter@tugraz.at

Datenschutzkoordination

Mag.iur. Daniel Kurzmann, BA MA LL.M.
datenschutz@tugraz.at
+43 316 873 - 6003

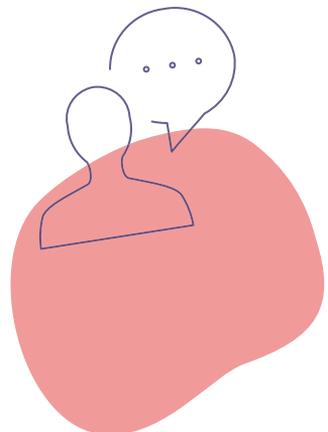
Mag.iur. Christof Plaschke
datenschutz@tugraz.at
+43 316 873 - 6047

Anna-Maria Henögl
(Verarbeitungsverzeichnis)
datenschutz@tugraz.at
+43 316 873 - 6067

Informationssicherheit

DI Reinfried O. Peter, MSc
it-security@tugraz.at
+43 316 873 - 6390

Mag.iur. Marcel Schudi
it-security@tugraz.at
+43 316 873 - 7697



8. Link-Sammlung

Vorlagen für Datenschutzerklärungen,
eine Werknutzungsbewilligung,
sowie eine Einwilligungserklärung
nach Art 49 Abs 1 lit a DSGVO
<https://tu4u.tugraz.at/go/ds-vorlagen>

Booklet: Lehre an der TU Graz. Studienrechtliche
Fragen und Antworten
[https://tu4u.tugraz.at/bedienstete/lehre/
booklet-lehre-an-der-tu-graz/](https://tu4u.tugraz.at/bedienstete/lehre/booklet-lehre-an-der-tu-graz/)

Datenschutz-und Geheimhaltungsverpflichtung
für externe Gutachter/innen von Dissertationen
[https://tu4u.tugraz.at/fileadmin/
Studierende_und_Bedienstete/
D-E_Formulare_Forms/Datenschutz-
und_Geheimhaltungsverpflichtung_Diss_Externe.pdf](https://tu4u.tugraz.at/fileadmin/Studierende_und_Bedienstete/D-E_Formulare_Forms/Datenschutz-und_Geheimhaltungsverpflichtung_Diss_Externe.pdf)

Einwilligungserklärung
nach Art 6 Abs 1 lit a DSGVO
<https://tu4u.tugraz.at/go/ds-vorlagen>

Satzungsteil Datenschutzordnung
der Technischen Universität Graz
[https://tu4u.tugraz.at/fileadmin/public/
Studierende_und_Bedienstete/
Satzung_und_Geschaeftsordnungen_der_TU_Graz/
Datenschutzordnung_Satzungsteil_7.8.2019.pdf](https://tu4u.tugraz.at/fileadmin/public/Studierende_und_Bedienstete/Satzung_und_Geschaeftsordnungen_der_TU_Graz/Datenschutzordnung_Satzungsteil_7.8.2019.pdf)

Rahmenbetriebsvereinbarung über die automatisationsgestützte Verarbeitung personenbezogener Daten von Arbeitnehmerinnen und Arbeitnehmer

https://tu4u.tugraz.at/fileadmin/user_upload/redaktion/Betriebsvereinbarungen/Datenschutz_Rahmenbetriebsvereinbarung.pdf

Videoüberwachungs- und -aufzeichnungsanlagen an der TU Graz

<https://tu4u.tugraz.at/go/videoueberwachung>

Informationsblatt für TU Graz Bedienstete zur Informationssicherheit und zum Datenschutz

<https://tu4u.tugraz.at/bedienstete/organisation-und-administration/datenschutz-und-datensicherheit/forschung-lehre-und-verwaltung/verwaltung/datenschutz-informationsblatt-fuer-arbeitnehmerinnen>

Antrag zum Einsatz einer personenbezogenen Datenverarbeitung

<https://tu4u.tugraz.at/bedienstete/organisation-und-administration/datenschutz-und-datensicherheit/forschung-lehre-und-verwaltung/verwaltung/antrag-zum-einsatz-einer-personenbezogenen-datenverarbeitung/>



