TECHNISCHE UNIVERSITÄT WIEN






FAQs Datenschutz

FAQs und Handlungsanleitungen zum Datenschutz an der TU Wien

Stand 11.05.2021

Version 3 (neue Fragen sind gelb markiert)

INHALT

DIE DATENSCHUTZGRUNDSÄTZE

Grundsätzlich ist im Einzelfall mit folgender Fragestellung zu klären, ob die Datenschutz-Grundverordnung (DSGVO[1] /DSG[2]) anwendbar ist:

Liegt eine ganz oder teilweise automatisierte oder nicht-automatisierte Verarbeitung personenbezogener Daten vor, die in einem Dateisystem gespeichert wird oder gespeichert werden?

"Personenbezogene Daten“ sind Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Dabei ist es unerheblich, ob private, berufliche, wirtschaftliche Informationen, Eigenschaften, Kenntnisse oder physiologische Merkmale betroffen sind. Personenbezogene Daten sind daher z.B. Name, Geburtsdatum, Adresse, Geschlecht, Einkommen, Vermögen, Lebensstil, Intelligenzquotient, Umsatz, Beschäftigtenzahl, Gewinn, Angaben zur Bonität sowie auch Bild, Stimme, Fingerabdrücke oder genetische Daten. Also alle Daten die es ermöglichen, eine Person zu identifizieren.

→ Nein: DSGVO/DSG nicht anwendbar

→ Ja: DSGVO/DSG anwendbar

Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten. Sie ist nur in den Fällen zulässig, die im Gesetz ausdrücklich genannt sind. Gemäß Art 6 (1) DSGVO ist dies zulässig und damit rechtmäßig, wenn:

1. eine Einwilligung vorliegt (Art. 6 Abs. 1a) oder
2. zum Zweck der Vertragserfüllung oder zur Erfüllung vorvertraglicher Maßnahmen (Art. 6 Abs. 1b) oder
3. wenn eine rechtliche Verpflichtung vorliegt (Art. 6 Abs. 1c) oder
4. die Daten zum Zweck des Schutzes lebenswichtiger Interessen verarbeitet werden (Art. 6 Abs. 1d) oder
5. es sich um die Wahrnehmung öffentlicher Interessen / Ausübung öffentlicher Gewalt handelt (Art. 6 Abs. 1e) oder
6. sie zur Wahrung berechtigter Interessen des Verantwortlichen erfolgt (Art. 6 Abs. 1f).

= ERLAUBNISTATBESTÄNDE

Unabhängig davon, dass eine Datenverarbeitung nur zulässig ist, wenn entweder eine Einwilligung (Punkt 1) oder ein gesetzlicher Erlaubnistatbestand (Punkte 2 bis 6) greift, müssen zusätzlich auch die Datenschutzprinzipien der DSGVO eingehalten werden:

[1] EU-Datenschutz-Grundverordnung
[2] Datenschutzgesetz

1. **Rechtmäßigkeit**: Es muss eine Rechtsgrundlage für die Verarbeitung existieren, sprich es muss einer der Erlaubnistatbestände erfüllt sein;
2. **Treu und Glauben**: Die Verarbeitung muss redlich und anständig sein (unbestimmter Rechtsbegriff);
3. **Transparenz**: Die Datenverarbeitung muss für die betroffene Person nachvollziehbar sein (vgl. Informationspflichten, Datenschutzinformation);
4. **Zweckbindungsgrundsatz**: Die Datenverarbeitung darf nur zu vorher festgelegten, eindeutigen und legitimen Zwecken erfolgen;
5. **Datensparsamkeit**: Die Datenverarbeitung muss auf das zweckgebundene, notwendige Maß beschränkt sein;
6. **Sachliche Richtigkeit**: Die Daten müssen sachlich richtig und auf dem neuestem Stand sein;
7. **Begrenzte Speicherung**: Die Daten sind frühestmöglich zu löschen, sobald die zweckgebundene Erforderlichkeit der Speicherung wegfällt;
8. **Integrität und Vertraulichkeit**: Unzulässigkeit der unbefugten oder unrechtmäßigen Verarbeitung und Schutz vor Verlust und Schädigung.

Ist einer der Erlaubnistatbestände erfüllt und kann der/die für die Verarbeitung Verantwortliche nachweisen, dass die Datenschutzprinzipien eingehalten werden, dürfen die Daten für den jeweils angegebenen Zweck grundsätzlich verarbeitet werden.

Prüfen Sie Ihre personenbezogenen Daten, aktualisieren oder löschen sie diese, falls der Zweck der Verarbeitung erloschen ist: Achtung Löschfristen[3].

1 ALLGEMEINES

1.1 DARF ICH WEITERHIN MEINE AUSSENDUNGEN AN INTERNE UND EXTERNE PERSONEN MACHEN, DIE MEINEN NEWSLETTER BESTELLT HABEN/DIE ICH IN MEINEM KONTAKTNETZWERK HABE?

Ja, nur bei neuen externen Personen muss eine Einwilligung vorab erfolgen – an interne Personen darf geschickt werden (rechtliche Deckung durch Arbeitsvertrag bzw. berechtigtes Interesse des Dienstgebers).

[3] Liste ist in Arbeit

Sollte es schon Einwilligungen von externen Personen geben, muss sichergestellt werden, dass diese Einwilligungen den Anforderungen der DSGVO entsprechen. Folgendes ist dabei zu beachten:

- eindeutige Zustimmung (daher: Stillschweigen / Untätigkeit sind keine Einwilligung)
- es soll darüber Informiert werden, welche Daten verarbeitet werden und zu welchem Zweck (dies muss vor der Einwilligung geschehen)
- Einwilligung muss durch eine eindeutige bestätigende Handlung erfolgen, daher am besten schriftlich (auch ein Kästchen zum Anklicken wäre zulässig).

Die Einwilligung kann jederzeit widerrufen werden. Eine Information über das Bestehen dieser Möglichkeit des Widerrufs und wie dieser erfolgen kann, ist in jeder Aussendung / jedem Newsletter aufzunehmen.

Die TU.it bietet unterschiedliche Mailinglisten an, in die auch TU-externe Adressen eingebunden werden und in die bestehende Listen eingespielt werden können. Es bestehen vielfältige Einstellungsmöglichkeiten zur Abmeldung aus dem Verteiler, die Möglichkeit zur Selbstabmeldung ist vorgesehen. Informationen dazu finden sie hier: https://www.it.tuwien.ac.at/uptudate/list/

Vorlagen für die Einwilligung zur Zusendung von Newsletter finden Sie im „Handbuch Datenschutz bei Veranstaltungen an der TU Wien“ auf Seite 23.

Neben der Einwilligung kann die Verarbeitung personenbezogener Daten auch zur Erfüllung einer Aufgabe erforderlich sein, die das Universitätsgesetz 2002 (UG) vorschreibt. Die Aufgaben der Universität sind in § 3 UG aufgelistet. Fällt der Versand des Newsletters unter einen der dort genannten Punkte, ist der Versand auch ohne ausdrückliche Einwilligung möglich.

1.2 WIE LANGE DARF ICH MEINE DATEN SPEICHERN?

Grundsätzlich dürfen personenbezogene Daten nur so lange verarbeitet (gespeichert) werden, solange der Zweck aufrecht ist. Ist dieser nicht mehr gegeben, müssen die Daten gelöscht werden.
Bitte beachten Sie, dass die TU-Wien bzgl. Lösch- und Aufbewahrungsfristen unterschiedlichen und vielfältigen gesetzlichen Regelungen und Verpflichtungen unterliegt. Bei Unsicherheiten bzgl. der Frage, ob Sie etwas löschen dürfen oder nicht, halten Sie bitte Rücksprache mit der Abteilung Datenschutz- und Dokumentenmanagement und mit dem Archiv der TU Wien.

1.3 WAS MUSS ICH IM E-MAIL-VERKEHR BEACHTEN? GIBT ES HIER ÄNDERUNGEN?

Schicken Sie Mails, wenn möglich bcc (außer die Empfänger sollen voneinander wissen), um nicht unnötig viele Email-Adressen weiterzuleiten. Schicken Sie sowohl intern, als auch extern wirklich nur an jene Empfänger_innen, welche die personenbezogenen Daten benötigen.

E-Mails und Attachments mit personenbezogenen Daten sind zu vermeiden, hier ist sukzessive auf Links umzustellen, die nur für den / die Betroffenen einsehbar sind (Passwort!). Die entsprechenden Passwörter dürfen nicht per E-Mail verschickt werden.

In der TUOwnCloud können Sie Ordner für jede_n Mitarbeiter_in freischalten. In der TUproCloud ist auch die Integration externer Projektpartner möglich.

Verwenden Sie in Ihren E-Mails immer die digitale Signatur, die von der TU.it zur Verfügung gestellt wird.

1.4 MUSS ICH ALLE E-MAILS DIE PERSONENBEZOGENE DATEN ENTHALTEN VERSCHLÜSSELN?

Personenbezogene Daten die innerhalb des TU-Wien Netzwerkes verschickt werden, müssen nicht verschlüsselt werden, da dieses jedenfalls als sicher einzustufen ist. Beachten Sie allerdings, dass eigene Mail-Server an Instituten und Abteilungen als TU-extern einzustufen sind, weshalb eine Verschlüsselung von E-Mails mit denen besondere Kategorien von personenbezogenen Daten an Externe übermittelt werden, empfohlen wird. Derzeit wird dazu die Verwendung von S/MIME-Zertifikaten empfohlen: https://www.it.tuwien.ac.at/services/zutritt-login-und-identity/identity/clientbasierte-mailverschluesselung

Diese Art der Verschlüsselung eignet sich allerdings nicht für E-Mails an Dritte (z.B.: Rechnungshof, BRZ, diverse Fördergeber). Eine Möglichkeit für die Übermittlung von personenbezogenen Daten an Dritte wäre die proCloud der TU Wien: https://www.it.tuwien.ac.at/owncloud/

An einer Gateway-basierten (opt-in) Verschlüsselung wird gearbeitet.

1.5 MUSS ICH MEINEN LAPTOP/RECHNER VERSCHLÜSSELN?

Da mobile Geräte einem höheren Verlust- oder Diebstahlsrisiko ausgesetzt sind, ist für die Speicherung personenbezogener Daten eine Verschlüsselung des jeweiligen Endgeräts unbedingt erforderlich.[4]

[4] Hinweis: Die TU.it bietet mit dem Notebook-Service Notebooks an, die bereits mit verschlüsselten Festplatten ausgeliefert werden (https://iu.zid.tuwien.ac.at/15380645.asHTML).

Die Speicherung von personenbezogenen Daten direkt auf Desktop-Rechnern ist zu vermeiden. Für die Speicherung der Daten sind Netzwerklaufwerke einzusetzen, die die Daten auf verschlüsselten Datenträgern speichern.[5]

1.6 WAS IST DAS DATENGEHEIMNIS?

Angehörige der TU Wien sind zur Einhaltung des Datengeheimnisses zu verpflichten.

Datengeheimnis nach § 6 DSG

(1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

An der TU Wien erfolgt die Verpflichtung zur Einhaltung des Datengeheimnisses elektronisch.

1.7 WIE IST MIT KUNDENDATEN/DATEN EXTERNER PERSONEN UMZUGEHEN (CRM)?

Wenn Daten zum Zweck der Vertragserfüllung verarbeitet werden, ist die Verarbeitung legitim. Nach erfolgreicher Abwicklung des Vertrages sind, unter Einhaltung der gesetzlichen Löschfristen, die Daten zu löschen. Bei Unsicherheiten bzgl. der Löschfristen, wenn Sie sich bitte an die Abteilung für Datenschutz- und Dokumentenmanagement oder an das Archiv der TU Wien.

1.8 WAS MUSS ICH TUN, WENN ICH PERSONENBEZOGENE DATEN NEU VERARBEITE (D.H. SPEICHERN, WEITERLEITEN, VERWENDEN)?

Ich muss prüfen, ob ich berechtigt bin, die personenbezogenen Daten zu verarbeiten:

a. Gibt es eine Rechtsgrundlage? (Arbeitsvertrag, sonstiges Vertragsverhältnis: zB Lieferant, Caterer, Fördergeber, Partner, rechtliche Verpflichtung) oder
b. hat die TU eine „rechtliche Verpflichtung“ zur jeweiligen Verarbeitung (z.B.: ist die Verarbeitung mit der Erfüllung einer der Aufgaben einer Universität gem. §3 UG verbunden)? Oder
c. erfolgt die Verarbeitung zur Erfüllung einer Aufgabe im öffentlichen Interesse?

[5] Hinweis: TU.it stellt mit dem Service TUfiles ein Netzwerklaufwerk zur Verfügung. Die Daten werden in den Datacentern sicher auf verschlüsselten Festplatten gespeichert (https://www.it.tuwien.ac.at/tufiles/).

d. Besteht ein berechtigtes Interesse an der Verarbeitung, welches das Datenschutzinteresse des_der Betroffenen überwiegt?
e. habe ich eine Einwilligung der betroffenen Person zur Datenverarbeitung?

Falls ich berechtigt bin, die personenbezogenen Daten zu verarbeiten, muss ich der Informationspflicht nachkommen und auf die Betroffenenrechte hinweisen („Datenschutzerklärung“).

1.9 DÜRFEN PERSONENBEZOGENE AUSKÜNFTE AM TELEFON GEGEBEN WERDEN?

Wenn die Identität des Gesprächspartners nicht feststeht, sollte ein Rückruf oder eine schriftliche Anfrage vereinbart werden. Im Zweifel muss stets die Identität des_der Anrufer_in geklärt werden.

1.10 ICH BETREIBE FÜR MEIN/EN INSTITUT/FORSCHUNGSBEREICH EINEN SOCIAL-MEDIA-ACCOUNT. DARF ICH DAS?

Der Gerichtshof der Europäischen Union hat entschieden, dass der Betreiber einer Facebook-Fanseite für die Verarbeitung der personenbezogenen Daten mitverantwortlich ist.[6] Was heißt das für die Seitenbetreiber_Innen? Welche personenbezogenen Daten werden hier wie verarbeitet?

Aus dem Urteil[7]:

„Die Betreiber von Fanpages […] können mit Hilfe der Funktion Facebook Insight, die ihnen Facebook als nicht abdingbaren Teil des Benutzungsverhältnisses kostenfrei zur Verfügung stellt, anonymisierte statistische Daten betreffend die Nutzer dieser Seiten erhalten. Diese Daten werden mit Hilfe sogenannter Cookies gesammelt, die jeweils einen eindeutigen Benutzercode enthalten, der für zwei Jahre aktiv ist und den Facebook auf der Festplatte des Computers oder einem anderen Datenträger der Besucher der Fanpage speichert. Der Benutzercode, der mit den Anmeldungsdaten solcher Nutzer, die bei Facebook registriert sind, verknüpft werden kann, wird beim Aufrufen der Fanpages erhoben und verarbeitet. […] Nach Ansicht des Gerichtshofs kann der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, diesen nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien.“

Das heißt nicht, dass das Betreiben von Facebook-Seiten illegal ist, sondern, dass Betreiber von Facebook-Seiten (und in weiterer Folge auch für andere Social-Media-Seiten) gemeinsam mit Facebook dafür verantwortlich sind, dass der Datenschutz eingehalten wird und für Datenschutzverstöße durch Fa-

[6] Siehe: https://derstandard.at/2000080989027/EuGH-Facebook-Fanpages-mitverantwortlich-fuer-Datenschutzverstoesse (zuletzt abgerufen am 07.05.2021)
[7] Presseaussendung zum Urteil: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081de.pdf (zuletzt abgerufen am 07.05.2021)

cebook mithaften. Die Haftung reicht soweit, wie eine Mitwirkung an Facebooks Datenverarbeitung angenommen werden kann. D.h. es geht nur um die Verarbeitung von Daten, die über die Facebook-Seite oder ein Social-Plugin erhoben wurden[8].

Heißt das nun, dass Sie Ihre Seiten löschen müssen? Nicht unbedingt. Sie sollten sich aber die Frage stellen, ob es tatsächlich notwendig ist, eine Facebook-Seite oder andere Social-Media-Seiten zu betreiben. Dazu empfiehlt es sich, folgendes zu prüfen:

- Wie hoch ist der Rücklauf?
- Wie hoch ist die Anzahl der tatsächlichen Interaktionen (Kommentare und Nachrichten zu Beiträgen)?
- Wie viele „Likes" erhält ein Beitrag im Durchschnitt?
- Wofür wird die Seite genutzt?
- Welchen Mehrwert bringt der Auftritt für mein Institut/Projekt/meinen Forschungsbereich?
- Gibt es andere Möglichkeiten, eine ähnlich hohe Reichweite zu erzielen?
- Wie viel Zeit beansprucht die Wartung der Fanseite?

Kommen Sie zum Schluss, dass das Betreiben der Fanseite einen tatsächlichen Mehrwert generiert, ist es jedenfalls notwendig, die Benutzer_innen darüber zu informieren, welche Daten gespeichert werden. Ein Beispiel für die notwendigen Informationen finden Sie hier: https://www.facebook.com/notes/kanzlei-keese-haufs/datenschutzhinweise-für-die-fanpage/1076429195844483/

1.11 WAS IST EINE DVR-NUMMER?

Die DVR-Nummer wurde für das Datenverarbeitungsregister bei der Datenschutzbehörde vor der Einführung der DSGVO verwendet. Seit am 25. Mai 2018 die DSGVO in Kraft getreten ist, muss die TU Wien über diese Verarbeitungen ein sogenanntes „Verzeichnis der Verarbeitungen" (kurz: Verarbeitungsverzeichnis) führen, welches die DVR-Nummer komplett ablöst.

[8] Detaillierte Informationen finden Sie hier: https://allfacebook.de/policy/eugh-urteil (zuletzt abgerufen am 07.05.2021).

2 VERANSTALTUNGEN

2.1 WIE GEHE ICH MIT MEINEN TEILNEHMER_INNENLISTEN (VON VERANSTALTUNGEN, KONFERENZEN ETC.), KONTAKTLISTEN, KUNDENDATEIEN, E-MAIL-VERTEILERLISTEN, NEWSLETTER-ABONNENT_INNEN-LISTEN UM?

Bei Veranstaltungen der TU-Wien, die Studierende, Alumni oder ganz allgemein einen Forschungsbereich der TU-Wien betreffen, gehen wir davon aus, dass dies durch §3 Universitätsgesetze 2002 - UG (Aufgaben einer Universität) Deckung findet. Damit besteht eine gesetzliche Grundlage für die Verarbeitung von Daten zum Zweck der Veranstaltungsabwicklung.

Betrifft die Datenverarbeitung Bereiche die nicht zu den gesetzlich normierten Aufgaben einer Universität gehören, muss geprüft werden, ob es eine andere Rechtsgrundlage für die Verarbeitung gibt, beispielsweise eine vertragliche Grundlage oder eine Einwilligung. Wenn es eine solche nicht gibt, ist eine Einwilligung einzuholen. In diesem Fall ist folgendermaßen vorzugehen:

Bestehende Listen durchforsten, ob sie aktuell und richtig sind und noch gebraucht werden. Falls ja, überprüfen, ob eine gültige Einwilligung vorliegt. Falls nein, elektronisch löschen (lokal löschen, Papierkorb entleeren) bzw. Papier vernichten (shreddern). Wird der Kontakt noch benötigt und liegt keine gültige Einwilligung vor, ist diese einzuholen.

Vorlagen für die Einwilligung zur Zusendung von Newsletter finden Sie im „Handbuch Datenschutz bei Veranstaltungen an der TU Wien“ auf Seite 23.

2.2 WIE GEHE ICH MIT NEUEN KONTAKTEN AUS VERANSTALTUNGEN, KONFERENZEN, MESSEN ETC. UM, DIE ICH AUFBEWAHREN/ABSPEICHERN MÖCHTE?

Auch hier gilt 2.1. Betroffene Person sind über die Datenverarbeitung zu informieren (Datenschutzerklärung), gegebenenfalls sind Einwilligungserklärungen zu unterschreiben[9].

Für den Versand von E-Mails an mehrere Personen bietet die TU.it ein Mailing list service (siehe https://list.tuwien.ac.at/sympa/). Bestehende Listen können eingespielt werden. Es bestehen vielfältige Einstellungsmöglichkeiten zur Abmeldung aus dem Verteiler, die Möglichkeit zur Selbstabmeldung ist vorgesehen.

[9] Die Einwilligung muss klarstellen, wozu man zustimmt (welche Daten, an Wen, zu welchem Zweck, Widerrufsmöglichkeit).

Vorlagen für die Einwilligung zur Zusendung von Newsletter finden Sie im „Handbuch Datenschutz bei Veranstaltungen an der TU Wien“ auf Seite 23.

2.3 WIE GEHE ICH MIT VISITENKARTEN UM, DIE ICH ERHALTE?

Die Übergabe einer Visitenkarte kann als implizite Einwilligung zur personenbezogenen Datenverarbeitung verstanden werden. Es ist keine zu unterzeichnende Einwilligung der betroffenen Person erforderlich, ich darf den Kontakt in Papierform (Visitenkarte) aufheben und speichern.

2.4 ICH MÖCHTE EINE VERANSTALTUNG ABHALTEN UND DIE TEILNEHMER_INNENLISTE AUFBEWAHREN. DARF ICH DAS?

Auch hier gilt 2.1. Im Anmeldeformular ist darüber zu informieren, gegebenenfalls ist die Einwilligung einzuholen, dass die Teilnehmer_innen mit der Weitergabe der Kontaktdaten und Speicherung einverstanden sind.

Vorlagen für die Einwilligung zur Zusendung von Newsletter finden Sie im „Handbuch Datenschutz bei Veranstaltungen an der TU Wien“ auf Seite 23.

2.5 ICH MÖCHTE AUF MEINER VERANSTALTUNG FOTOS MACHEN. DARF ICH DAS?

Grundsätzlich darf auf Konferenzen fotografiert werden. Wir empfehlen folgendes Vorgehen:

Bei der Anmeldung vor Ort werden zwei verschiedenfarbige Schlüsselbänder (lanyards) ausgegeben: Blau = Fotografieren geht in Ordnung; Weiß = will grundsätzlich auf keinen Fotos zu sehen sein.

Was aber dennoch akzeptiert werden muss, sind Fotos in die Gruppe um die Veranstaltung an sich dokumentieren zu können.

Bei der Ausgabe der lanyards sollte folgende Information angebracht sein:

„Please select a blue lanyard if you have no objection to being photographed. During (*name of the conference*) the official photographer will be onsite and taking photographs of attendees at both working sessions and during social times. In addition, many participants engage in photography as a hobby and enjoy taking photos during the meeting.

Please note that we expect all photographers – official and amateur – to act respectfully when taking photographs of attendees. If you feel that someone is acting disrespectfully, please contact (*name of person to contact*)“

„If you do not want to be photographed during the meeting or at social events of this meeting, please wear a white lanyard.

The white lanyard indicates:

- You do not want to be individually photographed by either professional or amateur photographers
- You do not want to be included in small group photos taken by professional or amateur photographers

Please note that photos of large groups may contain incidential images of attendees in white lanyards which the (*name of the organisation*) will not attempt to redact. In addition, individuals wearing white lanyards will still be included in official video recordings."

Dies könnte beispielsweise folgendermaßen umgesetzt werden:

Vorlagen für die Einwilligung zur Zusendung von Newsletter und Details zum Thema Datenschutz und Veranstaltungen finden Sie im „Handbuch Datenschutz bei Veranstaltungen an der TU Wien" auf Seite 23.

2.6 DARF ICH STUDIERENDE/VORTRAGENDE FILMEN?

Wie bisher auch, nur mit Einwilligung der betroffenen Personen.

2.7 ICH ORGANISIERE EINE KONFERENZ UND MÖCHTE ZUSÄTZLICH ZU PERSONEN AUF MEINER DSGVO-KONFORMEN MAILINGLISTE PERSONEN ANSCHREIBEN VON DENEN ICH AUSGEHE, DASS SIE SICH FÜR DAS KONFERENZTHEMA INTERESSIEREN. DARF ICH DAS?

Artikel 9 (2) lit e DSGVO erlaubt die Verarbeitung von besonderen Kategorien personenbezogener Daten (vormals sensible Daten), wenn diese Daten von der betroffenen Person offensichtlich öffentlich

gemacht wurden. Da diese Art von personenbezogenen Daten als schützenswerter eingestuft werden müssen, als allgemeine personenbezogene Daten (wie Name, Anschrift, Arbeitgeber etc.), diese aber verarbeitet werden dürfen, sofern sie von der betroffenen Person offensichtlich öffentlich gemacht wurden, ist davon auszugehen, dass allgemeine personenbezogene Daten die offensichtlich öffentlich gemacht wurden ebenfalls verarbeitet werden dürfen (eine entsprechende Erwähnung im Gesetzestext gibt es allerdings nicht).

Des weiteren könnte hier mit dem Bestehen eines berechtigten Interesses argumentiert werden. So steht im ErwGr 47 „*…Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigen Interesse dienende Verarbeitung betrachtet werden.*“ Hier besteht zwar eine gewisse Rechtsunsicherheit, wenn Sie aber nur Adressen verwenden, die von den angeschriebenen Personen oder deren Arbeitgeber_innen öffentlich gemacht wurden und deren Forschungsgebiet bzw. Arbeitsfeld dezidiert in den Bereich des Konferenz-/Veranstaltungsthemas fällt, erscheint es legitim diese Personen zum Zweck der Einladung zur Konferenz anzuschreiben.

Im Anschreiben sollten folgende Hinweise gemacht werden:

„Da Sie im Bereich xy arbeiten, gehen wir davon aus, dass die Konferenz xy für Sie von Interesse sein könnte. Sollten Sie keine weiteren Zusendungen zu dieser Konferenz erhalten wollten, bitten wir Sie um Rückmeldung bei xy@abckonferenz.at.“

3 STUDIUM, LEHRE UND FORSCHUNG

3.1 DARF ICH ALS LEHRBEAUFTRAGTE_R ANWESENHEITS- UND TEILNEHMER_INNENLISTEN FÜHREN?

Ja, dies ist rechtlich gedeckt durch das Universitätsgesetz 2002.

3.2 WELCHE FORMVORSCHRIFTEN MÜSSEN BEI DER FÜHRUNG VON ANWESENHEITSLISTEN IM RAHMEN VON LEHRVERANSTALTUNGEN BEACHTET WERDEN (DÜRFEN UNTERSCHRIFTSLISTEN OFFEN DURCH DEN HÖRSAAL GEREICHT WERDEN, ETC.)?

Anwesenheitslisten dürfen nach wie vor durch den Hörsaal gereicht werden, sollten aber so rasch wie möglich wieder zum_r Lehrenden zurückgebracht werden.

3.3 WIE IST MIT ZWISCHENERGEBNISSEN UMZUGEHEN? DARF ICH ERGEBNISSE/ZWISCHENERGEBNISSE AM INSTITUT AUSHÄNGEN?

Da es sich bei der Matrikelnummer sowie Name und Vorname um personenbezogene Daten handelt, ist eine Veröffentlichung jeglicher Ergebnisse am Institut nicht gestattet. Dies muss über TUWEL erfolgen.

Möchten Sie den Studierenden nur die Endnoten einer LVA bekanntgeben, so nutzen Sie direkt die TISS-Funktion »Studierende über Beurteilung benachrichtigen«. Um von den Studierenden einzelne Prüfungsergebnisse oder Teilergebnisse personenbezogen bekanntzugeben, nutzen Sie am besten TUWEL.

Link zum **Videotutorial** »Bewertungsaushang in TUWEL«: https://tuwel.tuwien.ac.at/mod/url/view.php?id=502363

3.4 DÜRFEN FÜR EXKURSIONEN TEILNEHMER_INNEN_LISTEN AN EXTERNE WEITERGEGEBEN WERDEN?

Wenn für eine Exkursion die Teilnehmer_innen dem externen Partner bekanntgegeben werden müssen (z.B. aus Sicherheitsgründen) dann ist diese Weitergabe zulässig. Allerdings dürfen nur die unbedingt notwendigen Daten weitergegeben werden, üblicherweise wird das der Name der Teilnehmer_innen sein. Eine Zustimmung ist in diesem Fall nicht erforderlich, die Studierenden sind jedoch im Zuge der Anmeldung zur Exkursion darüber zu informieren.

3.5 DARF ICH BEI EINER MÜNDLICHEN PRÜFUNG MIT MEHREREN PRÜFLINGEN, DAS PRÜFUNGSERGEBNIS LAUT VOR ALLEN ANWESENDEN BEKANNTGEBEN?

Bei der mündlichen Bekanntgabe von Noten, handelt es sich um keine strukturierte Verarbeitung von personenbezogenen Daten im Sinne der DSGVO. Noten dürfen daher mündlich verkündet werden. Auf Wünsche von Studierenden darf natürlich Rücksicht genommen werden.

3.6 DARF ICH AN DIE E-MAILADRESSE HANSIWÜRSTEL@GMX.AT PERSONENBEZOGENE DATEN ÜBERMITTELN?

Wenn die Identität des Absenders nicht geklärt ist, dürfen an die Adresse keine personenbezogenen Daten übermittelt werden. Da es vor allem im Lehrbetrieb nicht zumutbar ist, jede Identität zu überprüfen empfehlen wir, am Anfang einer Lehrveranstaltung klarzustellen, dass jegliche E-Mail-Kommunikation in der Lehrveranstaltung über die generische TU-E-Mailadresse der Studierenden abgewickelt wird. Dazu ist den Studierenden nahezulegen, die Weiterleitung der TU-E-Mailadresse an eine andere E-

Mailadresse zu deaktivieren. Sollte dies von Seiten der Studierenden als unzumutbar aufgefasst werden, muss jedenfalls eine vorname.nachname@g... Adresse verwendet werden.

3.7 ICH MÖCHTE MEINE LEHRVERANSTALTUNGEN AUF YOUTUBE ZUR VERFÜGUNG STELLEN. DARF ICH DAS? BZW. DARF ICH WEITERHIN DIE SERVICES VON GOOGLE IN ANSPRUCH NEHMEN?

Youtube ist Teil des Google-Konzerns. Google hat seinen Sitz in den USA und betreibt Rechnerzentren auf der ganzen Welt. Um ein möglichst hohes Sicherheitsniveau zu erreichen – so argumentiert Google – werden die Daten an unterschiedlichen Orten gespeichert. Nachdem weder Taiwan noch Singapur von der EU-Kommission als sichere Drittstaaten angeführt werden und nicht ausgeschlossen werden kann, dass dort Daten verarbeitet werden, ist mit Google eine Vereinbarung zum Datentransfer auf Basis von Standardvertragsklauseln abzuschließen. Andernfalls sollten keine personenbezogenen Daten über Google verarbeitet werden. Selbst wenn Sie personenbezogene Daten die beispielsweise in GoogleSheets eingegeben werden pseudonymisieren, werden mit Ihrer IP-Adresse personenbezogene Daten an Google übermittelt und dort verarbeitet.

Bzgl. des Streamens von Lehrveranstaltungen empfehlen wir die Nutzung von LectureTube. Diese, vom Teaching Support Center zur Verfügung gestellte Anwendung, ermöglicht es, Lehrveranstaltungen mit geringem Aufwand aufzuzeichnen, um diese Studierenden als multimediale Lernressource in TUWEL zur Verfügung zu stellen. Nähere Information dazu finden Sie hier: https://tsc.tuwien.ac.at/lecturetube

Als Alternative zur Google-Cloud, kann die OwnCloud der TU Wien verwendet werden.

Bzgl. der Veröffentlichung von Lehrveranstaltungen via Youtube ist unter anderem auch das Urheberrecht zu beachten. Details dazu finden Sie unter anderem hier: https://www.saferinternet.at/news-detail/urheberrecht-und-unterricht/

3.8 IST EINE EINWILLIGUNG VON MITARBEITER/INNEN ZUR VERÖFFENTLICHUNG VON PUBLIKATIONEN ODER FORSCHUNGSPROJEKTEN IM INTERNET ERFORDERLICH (FORSCHUNGSINFORMATIONS-DB)?

Nein. Gemäß § 2h Forschungsorganisationsgesetz (FOG) dürfen wissenschaftliche Einrichtungen zur Erhöhung der Transparenz wissenschaftliche Mitarbeiter_innen, die sich in einem aufrechten Arbeitsverhältnis mit der jeweiligen wissenschaftlichen Einrichtung befinden oder befunden haben, mit Foto und einer Liste ihrer Publikationen auf der Website der wissenschaftlichen Einrichtung oder im Rahmen öffentlich zugänglicher Berichte der wissenschaftlichen Einrichtung nennen.

3.9 WELCHE AUSNAHMEN/ERLEICHTERUNGEN BESTEHEN FÜR FORSCHUNGSDATEN? (FOG)

Generell finden sich die neu nominierten Ausnahmen und Erleichterungen bei Forschungsdaten im zweiten Abschnitt des FOG wieder. Beispielhaft werden nachfolgende Themen dazu genannt: Wissenschaftliche Einrichtungen im Sinne des FOG dürfen Forschungsmaterial im Sinne des § 2 FOG insbesondere sammeln, archivieren und systematisch erfassen und dazu sämtliche Daten verarbeiten, die erforderlich sind, um einen optimalen Zugang zu Daten und Forschungsmaterial für Zwecke gemäß Art 89 Abs 1 DSGVO zu gewährleisten. Die einzelnen Datenkategorien, welche in diesem Zusammenhang verarbeitet werden dürfen, sind in § 2f FOG angeführt. Das FOG normiert auch Erleichterungen für die – im Rahmen von Forschungstätigkeit durchgeführte – Verarbeitung personenbezogener Daten, indem etwa Rechte der betroffenen Person, z.B. auf Löschung der Daten, eingeschränkt werden.

Sofern personenbezogene Daten pseudonymisiert werden, gelten generell entsprechende Erleichterungen bei der Verarbeitung. Pseudonymisierte Daten dürfen in der Regel für Forschungszwecke verarbeitet werden.

Darüber hinaus zählt die Forschung zu den Aufgaben einer Universität (§ 3 UG). Diese Rechtsgrundlage kann bei der Verarbeitung von personenbezogenen Daten in der Forschung in vielen Fällen herangezogen werden. Somit bedarf es keiner (zusätzlichen) Einwilligung der betroffenen Personen zur Verarbeitung ihrer personenbezogenen Daten.

3.10 WER HAFTET FÜR DATENSCHUTZVERLETZUNGEN BEI § 26-PROJEKTEN? PROJEKTLEITER/INNEN ODER DIE TU WIEN?

Eine Haftung für datenschutzrechtliche Verstöße bei Projekten gemäß Art 26 DSGVO ist im Sinne von Art 82 Abs 4 DSGVO solidarisch. Somit haften sämtliche gemeinsame Verantwortliche jeweils für den gesamten Schaden. Natürlich ist es denkbar, dass sich die jeweiligen gemeinsamen Verantwortlichen im Innenverhältnis regressieren. Unter bestimmten Voraussetzungen ist eine Haftungsbefreiung der/des Verantwortlichen oder der/des Auftragsverarbeiter_in möglich.

3.11 IST BEI FORSCHUNGSVERTRÄGEN DIE DSGVO ZU BERÜCKSICHTIGEN?

Sofern in Forschungsverträgen bzw. in den zugrundeliegenden Forschungen personenbezogene Daten verarbeitet werden, ist auch hier die DSGVO zu berücksichtigen ist. In diesen Fällen kontaktieren Sie bitte den_die Datenschutzbeauftragte_n der TU Wien.

3.12 WER IST FÜR DIE EINHALTUNG DES DATENSCHUTZES BEI ARBEITEN STUDIERENDER VERANTWORTLICH (DIE TU WIEN, DER_DIE BETREUER_IN)?

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

3.13 BETRIFFT DIE DSGVO AUCH DIE, AUS DRITTLÄNDERN ERHALTENEN PERSONENBEZOGENEN DATEN?

Die DSGVO gilt für alle in einem EU-Staat verarbeiteten personenbezogenen Daten, unabhängig von der Staatszugehörigkeit des_der Betroffenen.

4 PERSONAL

4.1 WAS PASSIERT MIT MEINEM DIENSTHANDY, PC, LAPTOP? MUSS ICH HIER VORKEHRUNGEN TREFFEN?

Bewahren Sie Ihre Geräte versperrt und gesichert mit Passwort/Code auf. Geben Sie keine Passwörter weiter, ändern Sie Ihre Passwörter regelmäßig und verwenden Sie sichere Passwörter. Nähere Informationen dazu finden Sie hier: https://www.it.tuwien.ac.at/rechte-und-rollen/accounts-an-der-tuw/faq-accounts-an-der-tuw

Festplatten von mobilen Geräten wie Laptops und Tabletts auf denen personenbezogene Daten gespeichert sind, **müssen** verschlüsselt sein. Da an der TU Wien eine Vielzahl von unterschiedlichen Geräten eingesetzt werden und diese zum Teil nicht von der TU.it ausgegeben und damit auch nicht von dieser serviciert werden, bitten wir Sie, sofern Sie die Verschlüsselung nicht selbst vornehmen können, sich dazu an den_die IT-Administrator_in ihrer/s Instituts/Abteilung zu wenden.

Alle von der TU.it neu ausgegebenen mobilen Geräte werden ab 1.6.2018 nur mehr mit verschlüsselten Festplatten ausgeliefert. Sollten Sie noch über ein von TU.it ausgegebenes Geräte verfügen, das keine Festplattenverschlüsselung aktiviert hat, können Sie sich diesbezüglich an den Helpdesk wenden.

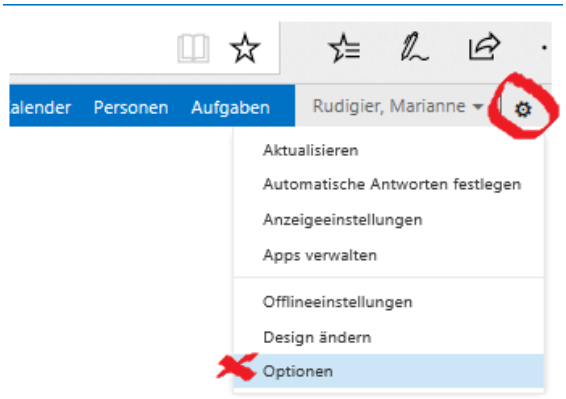
Aktuelle Smart-Phone Betriebssysteme laufen in der Regel mit verschlüsselten Dateisystemen. Bitte prüfen Sie, ob das für Ihr Smart-Phone zutreffend ist und veranlassen Sie gegebenenfalls eine Verschlüsselung. Dazu gehen Sie unter Einstellungen auf den Menüpunkt „Sicherheit“, wo es die Möglichkeit geben sollte, Ihr Gerät zu verschlüsseln (dauert idR eine Stunde).

Der Zugriff von Apps (WhatsApp, Skype, Messanger etc.) auf personenbezogene Daten die Sie auf Ihrem Gerät gespeichert haben, ist zu unterbinden (durch Konfigurationseinstellung oder Löschung der jeweiligen App).

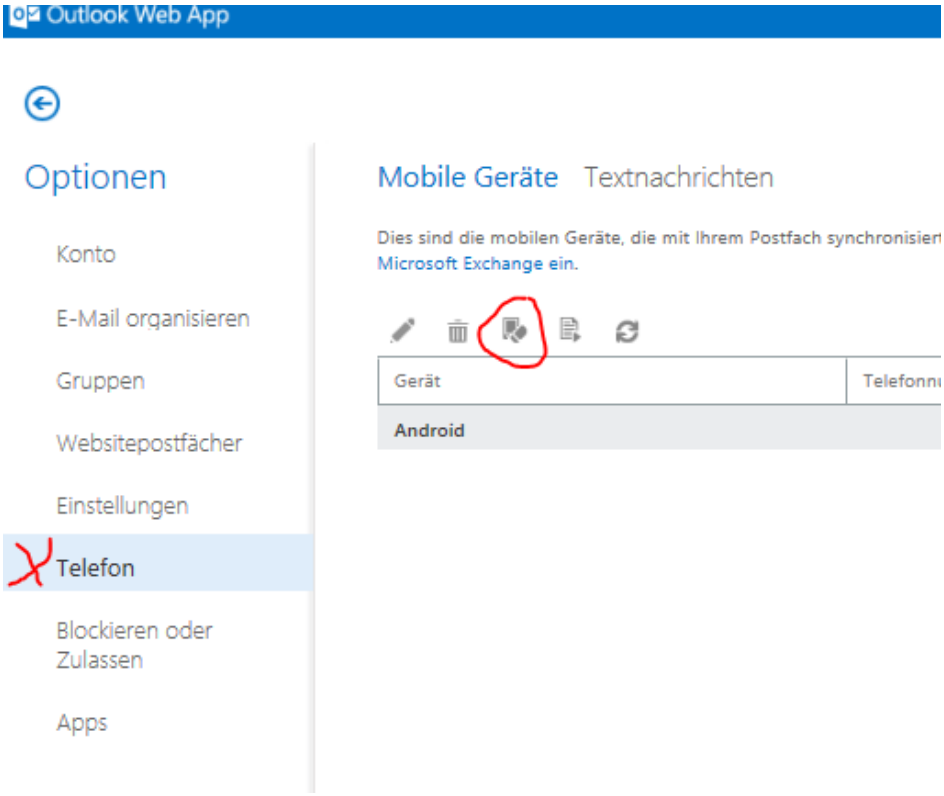
Bei Verwendung der TUOwnCloud ist sicherzustellen, dass diese nicht auf Ihrem Diensthandy synchronisiert wird.

Bei Verlust des Diensthandys gibt es die Möglichkeit via WebMail das Gerät auf Werkseinstellungen zurückzusetzen und so den Zugriff auf Ihre E-Mails zu verhindern:

Unter TUWebMail (https://mail.intern.tuwien.ac.at) im Menüpunkt „Einstellungen“, auf „Optionen“ klicken:



Unter dem Menüpunkt „Telefon“ werden Ihre Geräte angeführt. Das Gerät, welches sie zurücksetzen wollen auswählen und dieses Symbol  anklicken. Damit ist Ihr Gerät zurücksetzt.



4.2 DÜRFEN MITARBEITER_INNENKARTEN MIT FOTO VERWENDET WERDEN?

Ja, hier überwiegt das Interesse der TU Wien an der Identifizierbarkeit der betreffenden Personen das Geheimhaltungsinteresse der Mitarbeiter_innen.

4.3 DARF ICH EINEM FÖRDERGEBER DIE GEHALTS- UND KRANKENSTANDSDATEN EINES MITARBEITERS/EINER MITARBEITERIN WEITERLEITEN?

Ja, wenn dies durch den Arbeitsvertrag gedeckt ist (Zusatz zum Arbeitsvertrag erforderlich). Gibt es keinen Passus im Arbeitsvertrag, müssen Sie die Einwilligung der Forscher_innen zur Weitergabe von Gehaltsdaten und Krankenstandsdaten einholen.

4.4 WIE IST MIT ABWESENHEITEN IN TEAMKALENDERN UMZUGEHEN?

Bsp.: Die Mitarbeiter_innen geben ihre Abwesenheiten in einen Teamkalender ein, auf den alle Mitarbeiter_innen Zugriff haben. Im Fall einer Erkrankung wird dies so im Terminkalender vermerkt. In diesem Fall muss für alle Abwesenheitsgründe ein einheitlicher neutraler Begriff gewählt werden (zB.: „abwesend“). Denn der Austausch von besonderen personenbezogenen Daten (= „krank") ist für Zwecke des Beschäftigtenverhältnisses nicht erforderlich.

4.5 SCHUTZ VOR UNBEFUGTER EINSICHTNAHME:

Personaldaten, unabhängig davon, ob sie in elektronischer oder in Papierform vorliegen, sind vor der Kenntnisnahme von Unberechtigten zu schützen (z. B. keine offenen Akten am Schreibtisch). Papierakten sind in einem verschlossenen Schrank aufzubewahren und das Büro ist bei Verlassen desselben abzusperren. Sollten Sie verschließbare Schränke benötigen, wenden Sie sich bitte an die GUT.

Datenversand:
Werden personenbezogene Daten von Mitarbeiter_innen verschickt, sind die Daten so zu transportieren, dass sie nicht einsehbar sind (z.B. Akte in verschlossenem Umschlag, verschlüsselte und passwortgesicherte Datenträger). Innerhalb der TU Wien ist der Versand per E-Mail zulässig.

Dokumente mit personenbezogenen Daten sind an Empfänger_innen außerhalb der TU Wien gesichert zu verschicken, beispielsweise verschlüsselt oder passwortgeschützt per E-Mail oder über einen passwortgeschützten Link. Unverschlüsselte USB-Sticks sind zur Bearbeitung, Speicherung und Übertragung von personenbezogenen Daten gänzlich zu meiden.

In der TUOwnCloud können Sie Ordner für jede_n Mitarbeiter_in freischalten. In der TUproCloud ist auch die Integration externer Projektpartner möglich.

4.6 WIE KANN ICH SICHER SEIN, DASS DIE AN DER TU WIEN INSTALLIERTE KAMERA/ZUTRITTSYSTEM/BIOMETR. LESER DER DSGVO ENTSPRICHT?

In Zweifelsfällen wenden Sie sich bitte an die Abteilung „TU GUT“ (Fachgruppe Objektschutz und Brandschutz).

4.7 MEIN/E SERVER/WEBSEITE ETC. WIRD NICHT VON DER TU.IT BETRIEBEN. WER IST VERANTWORTLICH FÜR DIE SICHERHEIT DER DATEN?

Das Rektorat ist nur für jene Bereiche verantwortlich, die auch in ihrem Einflussbereich stehen. Das ist jedenfalls für die Services zutreffend, die von der TU.it angeboten werden. Bitte prüfen Sie, ob das Betreiben eigener Services in ihrem Bereich nach wie vor wirtschaftlich und zweckmäßig ist oder ob ein Wechsel zu den konsolidierten Services der TU.it eine sinnvolle Alternative wäre. Bitte beachten Sie außerdem, dass von Ihnen betriebene Services, die personenbezogen Daten verarbeiten, im Verarbeitungsverzeichnis der TU-Wien angeführt werden müssen. Diesbezügliche Informationen geben Sie bitte an ihre_n jeweiligen_n Datenschutzkoordinator_in weiter, die_der die Eintragung dann vornimmt.

5 ANNEX

Shortlist[10]

„Wichtige Maßnahmen Datenschutz und -sicherheit“ (Teil 1)

Sämtliche nachstehenden Maßnahmen beziehen sich auf Papierdokumente oder elektronische Files bzw. Datenträger (zB. CDs, USB-Sticks) **mit personenbezogenen Daten**[11] (im Folgenden bezeichnet als „einschlägige Dokumente“ oder „einschlägige Daten“ bzw. „einschlägige Datenträger“).

1. **„Sauberer Schreibtisch“**: Einschlägige Dokumente und Datenträger dürfen nicht offen im Büro, Labor etc. „herumliegen“, sondern sind **für Dritte unzugänglich (zB. versperrbarer Schrank) aufzubewahren**. **Maßnahme: Einschlägige Dokumente und Datenträger immer versperrt aufbewahren!**

2. **Sichere Entsorgung:** Sollen einschlägige Dokumente entsorgt werden, darf das nicht im Wege des „normalen“ Altpapiers erfolgen: **Entsorgung nur via Shredder oder „blauen Sack“** (erhältlich bei der GUT - bis zur Übergabe an die GUT ist auch der „blaue Sack“ versperrt aufzubewahren!). **Maßnahme: Einschlägige Dokumente shreddern oder via „blauen Sack“ sicher entsorgen!**

3. **Passwort für IT-Geräte**: IT-Geräte, auf denen sich einschlägige Daten befinden (PC, Notebook, Smartphone etc.) sind mit einem **möglichst guten Passwort gegen Zugriff Dritter** abzusichern[12]. Das **Passwort darf für Dritte nicht zugänglich sein** (also zB. kein Post-it am Bildschirm oder auf der Schreibunterlage!). **Maßnahme: IT-Geräte mit sicherem Passwort versehen, welches Dritten nicht zugänglich sein darf!**

4. **Sichere Verwaltung von Passwörtern**: Um eine möglichst unkomplizierte Verwaltung von Passwörtern zu unterstützen, gibt es sichere und gut bedienbare Passwort-Manager (zB. als App für das Smartphone, aber auch als Software für den PC oder das Notebook[13]). Alternativ können Passwortaufzeichnungen auch sicher (versperrt) aufbewahrt werden. **Maßnahme: Passwortaufzeichnungen sind entweder versperrt aufzubewahren oder Passwörter mit einem sicheren Passwort-Manager (Software oder App) zu verwalten!**

5. **Entsorgung von Datenträgern (auch aus IT-Geräten):** Datenträger (CDs, USB-Sticks etc.) bzw. Festplatten aus IT-Geräten (PC, Notebook, Server etc.) am Ende ihrer Nutzungsdauer, auf denen sich einschlägige Daten befinden, sind sicher zu entsorgen. Dafür ist das Service „TU Disk Shredder“ der TU IT Services (vormals ZID) zu nutzen[14]. **Maßnahme: Entsorgung von Datenträgern (auch aus IT-Geräten am Ende ihrer Nutzungsdauer) nur im Wege des TU IT-Dienstes „TU Disk Shredder“!**

[10] 22.3.2018, Markus Haslinger.
[11] Beispiele für personenbezogene Daten: Namen, Matrikelnummern oder eMail-Adressen von Studierenden, Teilnahmelisten, Prüfungsergebnisse, Beurteilungsbögen usw.
[12] Nähere Informationen zB. hier: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html (07.05.2021).
[13] Siehe zB. https://futurezone.at/apps/die-besten-passwort-manager-im-ueberblick/249.643.370 (07.05.2021).
[14] Siehe https://www.it.tuwien.ac.at/services/beratung-und-servicedesk/servicedesk/tudiskshredder (07.05.2021).