FAQs und Handlungs-anleitungen zum Datenschutz an der TU Wien

Stand: 21.6.2018

Die Zusammenstellung wird laufend ergänzt (betrifft auch Muster und Vorlagen für Informationen, erforderliche Zustimmungen etc.) und aktualisiert.
Neue Fragen sind gelb hinterlegt.

>FAQs und Handlungsanleitungen<

Inhalt

Die Datenschutz-Grundsätze

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; keine weitere Prüfung erforderlich.

→ Ja: DSGVO/DSG anwendbar; Prüfung, ob Verarbeitung erlaubt ist, ist notwendig.

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. **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);

[1] EU-Datenschutz-Grundverordnung

[2] Datenschutzgesetz

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 neuesten 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 die von Ihnen verarbeiteten personenbezogenen Daten, aktualisieren oder löschen sie diese, falls der Zweck der Verarbeitung erloschen ist: Achtung Löschfristen.[3]

[3] Liste ist in Arbeit

I. Allgemeines

1. Darf ich weiterhin internen und externen Personen meine Aussendungen zukommen lassen, 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).
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 muss darüber Informiert werden, welche Daten verarbeitet werden und zu welchem Zweck (dies muss vor der Einwilligung geschehen)
- die 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 erhalten Sie von Ihrer_m Datenschutzkoordinator_in (sobald es auf der TU Webseite einen internen Bereich gibt, werden sämtliche Unterlagen auch dort zur Verfügung stehen). https://www.tuwien.ac.at/dle/datenschutz_und_dokumentenmanagement/datenschutz/datenschutzorganisation/

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.

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.

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 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.

4. 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.

5. 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, wenden Sie sich bitte an die Abteilung für Datenschutz und Dokumentenmanagement oder an das Archiv der TU Wien.

6. Was muss ich tun, wenn ich personenbezogene Daten neu verarbeite (dh 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?
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“).

7. 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.

8. 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.[4] Was heißt das für die Seitenbetreiber_Innen? Welche personenbezogenen Daten werden hier wie verarbeitet?

Aus dem Urteil[5]:

„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 Facebook 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[6].
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?

---

[4] Siehe: https://derstandard.at/2000080989027/EuGH-Facebook-Fanpages-mitverantwortlich-fuer-Datenschutzverstoesse (zuletzt abgerufen am 20.06.2018)

[5] Presseaussendung zum Urteil: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081de.pdf (zuletzt abgerufen am 18.06.2018)

[6] Detaillierte Informationen finden Sie hier: https://allfacebook.de/policy/eugh-urteil (zuletzt abgerufen am 18.06.2018)

- 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/

II. Veranstaltungen

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 in Verwendung sind. 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 erhalten Sie von Ihrer_m Datenschutzkoordinator_in (sobald es auf der Webseite einen internen Bereich gibt, werden sämtliche Unterlagen auch dort zur Verfügung stehen). https://www.tuwien.ac.at/dle/datenschutz_und_dokumentenmanagement/datenschutz/datenschutzorganisation/

2. Wie gehe ich mit neuen Kontakten aus Veranstaltungen, Konferenzen, Messen etc. um, die ich aufbewahren / abspeichern möchte?

Auch hier gilt II 1. Betroffene Person sind über die Datenverarbeitung zu informieren (Datenschutzerklärung), gegebenenfalls sind Einwilligungserklärungen zu unterschreiben[7].

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.

Eine Vorlage für die Einwilligung für Fotos, für den Newsletterversand sowie eine Datenschutzinformation für Konferenzen erhalten Sie von Ihrem_r jeweiligen Datenschutzkoordinator_in. (sobald es auf der Webseite einen internen Bereich gibt, werden sämtliche Unterlagen auch dort zur Verfügung stehen) https://www.tuwien.ac.at/dle/datenschutz_und_dokumentenmanagement/datenschutz/datenschutzorganisation/

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.

4. Ich möchte eine Veranstaltung abhalten und die Teilnehmer_innenliste aufbewahren. Darf ich das?

Auch hier gilt II 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.

Eine Vorlage für die Einwilligung für Fotos, für den Newsletterversand sowie eine Datenschutzinformation für Konferenzen erhalten Sie von Ihrem_r jeweiligen Datenschutzkoordinator_in. (sobald es auf der Webseite einen internen Bereich gibt, werden sämtliche Unterlagen auch dort zur Verfügung stehen) https://www.tuwien.ac.at/dle/datenschutz_und_dokumentenmanagement/datenschutz/datenschutzorganisation/

5. Ich möchte auf meiner Veranstaltung Fotos machen. Darf ich das?

Dafür ist eine Einwilligung der Teilnehmer_innen erforderlich. Falls es keine solche gibt, sind Fotos nicht zulässig. Bei akademischen Feiern sind Fotos grundsätzlich zulässig, jedoch ist bei Bedarf ein fotofreier

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

Bereich vorzusehen. Außerdem ist mittels GUT-Beschilderung zu informieren, dass auf der Veranstaltung fotografiert wird.

Eine Vorlage für die Einwilligung für Fotos, für den Newsletterversand sowie eine Datenschutzinformation für Konferenzen erhalten Sie von Ihrem_r jeweiligen Datenschutzkoordinator_in. (sobald es auf der Webseite einen internen Bereich gibt, werden sämtliche Unterlagen auch dort zur Verfügung stehen) https://www.tuwien.ac.at/dle/datenschutz_und_dokumentenmanagement/datenschutz/datenschutzorganisation/

6. Darf ich Studierende / Vortragende filmen?

Wie bisher auch, nur mit Einwilligung der betroffenen Personen.

III. Studium, Lehre und Forschung

1. Darf ich als Lehrbeauftragte_r Anwesenheits- und Teilnehmer_innenlisten führen?

Ja, dies ist rechtlich gedeckt durch das Universitätsgesetz 2002 (berechtigtes Interesse TU Wien).

2. 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. 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.

4. 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.

5. 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://teachingsupport.tuwien.ac.at/lecturetube/

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

Zur Erstellung von Online-Umfragen empfehlen wir limesurvey (https://www.limesurvey.org/de/).

IV. Personal

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.zid.tuwien.ac.at/tu_passwort/

Festplatten von mobilen Geräten wie Laptops und Tabletts auf denen personenbezogene Daten gespeichert sind, müssen verschlüsselt sein. Da an der TU 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, an dem keine Festplattenverschlüsselung aktiviert ist, 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. Eine Anleitung dazu finden Sie hier: https://www.zid.tuwien.ac.at/uptudate/anleitungen/lostphone_datadelete/

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.

3. Dürfen Mitarbeiter_innenfotos aus dem TISS auf der Homepage der TU Wien erscheinen?

Ja, da jede_r Mitarbeiter_in das Foto selber auf TISS hochladen kann und damit selbst darüber entscheiden kann, ob ein Foto erscheint oder nicht. Den Mitarbeiter_innen der TU Wien sollte bewusst sein, dass das Adressbuch der TU Wien öffentlich zugänglich ist.

4. Darf ich einem Fördergeber die Gehalts- und Krankenstandsdaten eines_r Mitarbeiters_in 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 Gehalts- und Krankenstandsdaten einholen.

5. 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.

6. Wie kann der Schutz vor unbefugter Einsichtnahme gewährleistet werden?

Personaldaten, unabhängig davon, ob sie in elektronischer oder in Papierform vorliegen, sind vor der Kenntnisnahme von Unberechtigte 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.

7. 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“ (Security).

8. 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.

V. Annex

Shortlist[8]

„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**[9] (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[10]. 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[11]). 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[12]. **Maßnahme: Entsorgung von Datenträgern (auch aus IT-Geräten am Ende ihrer Nutzungsdauer) nur im Wege des TU IT-Dienstes „TU Disk Shredder“!**

---

[8] 22.3.2018, Markus Haslinger.

[9] Beispiele für personenbezogene Daten: Namen, Matrikelnummern oder eMail-Adressen von Studierenden, Teilnahmelisten, Prüfungsergebnisse, Beurteilungsbögen usw.

[10] Nähere Informationen zB. hier: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html (22.3.2018).

[11] Siehe zB. https://futurezone.at/apps/die-besten-passwort-manager-im-ueberblick/249.643.370 (22.3.2018).

[12] Siehe https://www.zid.tuwien.ac.at/tudiskshredder/ (22.3.2018).