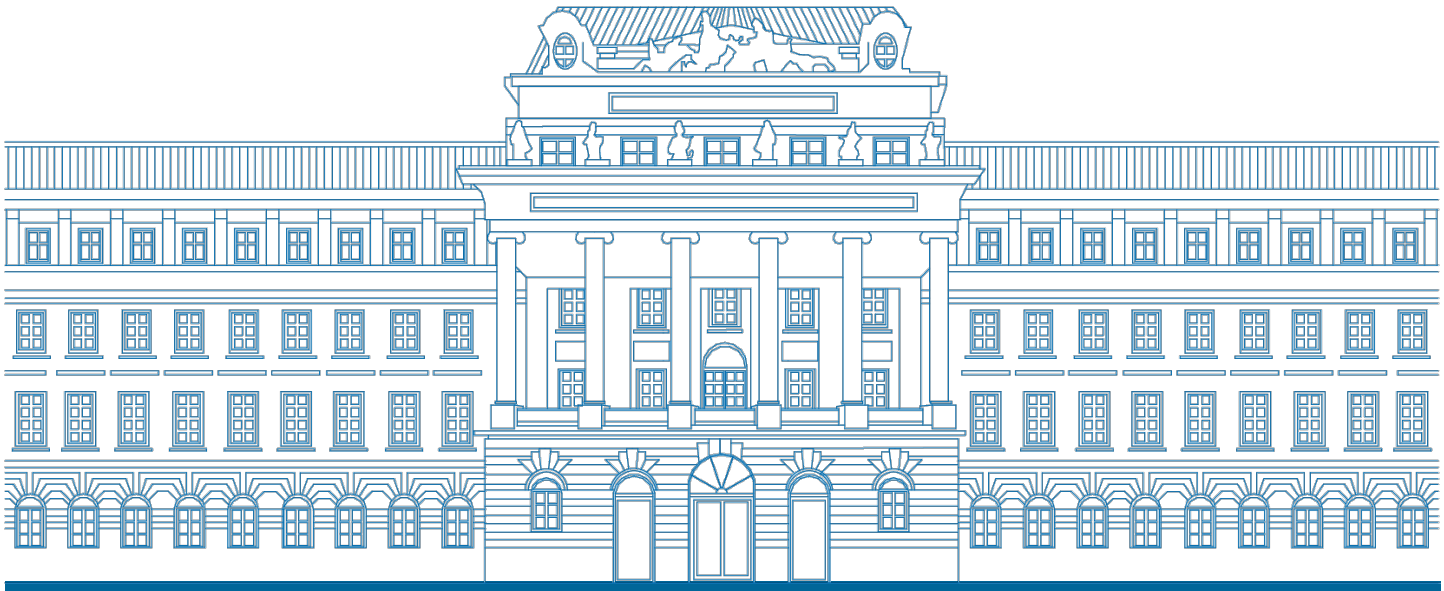
TECHNISCHE UNIVERSITÄT WIEN

Datenschutz-Handbuch



(online 31.08.201)

www.tuwien.at

DOKUMENTENINFORMATION

Beschluss des Rektorats am	-
Sachbearbeiter_innen	Mag[a] Marianne Rudigier
GZ:	30100.10/46/2020
Fassung vom:	26.06.2020

INHALT

Präambel

Dieses Dokument beschreibt die Datenschutz-Organisation und die Umsetzung des Datenschutzes an der TU Wien. Esadressiert alle Angehörigen der TU Wien gem. § 94 Universitätsgesetz (UG). Dritte sind über vertragliche und sonstige Vereinbarungen in den jeweils relevanten Punkten zu verpflichten. Darüber hinaus gelten die enthaltenen Regelungen ohne zeitliche und örtliche Einschränkungen.

Abkürzungen

Abs	Absatz
Art	Artikel
Avv	Auftragsverarbeitungsvertrag
BGBl	Bundesgesetzblatt
bPK	bereichssepzifisches Personenkennzeichen
bPK-BF-FO	bereichsspezifisches Personenkennzeichen für den Tätigkeitsbereich "Forschung"
BRZ	Bundesrechenzentrum
bzgl.	bezüglich
bzw.	beziehungsweise
CRM	Customer Relationship Management
DSA	Datenschutzansprechperson
DSDM	Abteilung für Datenschutz und Dokumentenmanagement
DSFA	Datenschutzfolgenabschätzung
DSG	Datenschutzgesetz
DSGVO	Datenschutzgrundverordnung
DSK	Datenschutzkoordinator_in
e.V	eingetragener Verein
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft(en)
ErwG	Erwägungsgrund
etc	et cetera
EU	Europäische Union
ev	eventuell
FAQ	Frequently Asked Questions
FOG	Forschungsorganisationsgesetz
GB	Gigabyte
gem	gemäß
ggf.	gegebenenfalls
GUT	Abteilung Gebäude und Technik

Hg	Herausgeber_in
idF	in der Fassung
idR	in der Regel
IP	Internetprotokoll
IT	Informations Technologie
iVm	in Verbindung mit
lit	litera(e)
RGBl	Reichsgesetzblatt
RL	Richtlinie
S.	Seite
sog.	sogenannt(e_r)
TKG	Telekommunikationsgesetz
TU	Technische Universität
TU.it	TU Information Technology Solutions
UG	Universitätsgesetz
USA	United States of America
USB	Universal Serial Bus
usw.	und so weiter
VdV	Verzeichnis der Verarbeitungstätigkeiten
Vgl	Vergleiche
WP	Working Paper
z.B.	zum Beispiel

1 Zielsetzung und Geltungsbereich des Dokuments

Die Technische Universität Wien, nachfolgend kurz TU Wien, verpflichtet sich im Rahmen ihrer gesellschaftlichen Ver-antwortung zur Einhaltung von Datenschutzrechten.

Dieses Datenschutz-Handbuch schafft eine Rahmenbedingung für Datenverarbeitung. Es gewährleistet das von der Eu-ropäischen Datenschutzgrundverordnung und den nationalen Gesetzen verlangte angemessene Datenschutzniveau fürdie Datenverarbeitung und den grenzüberschreitenden Datenverkehr auch in solche Länder, in denen kein angemesse-nes Datenschutzniveau gesetzlich gefordert wird.

Es beschreibt den Rahmen innerhalb dessen die organisationsweiten Datenschutzmaßnahmen zu planen und zu steuern, ihre Umsetzung zu bewerten und Verbesserungen abzuleiten sind. Die Konkretisierung und die damit verbundenentechnischen und organisatorischen Maßnahmen werden in spezifischen Richtlinien beschrieben, die den Handlungsrah-men darstellen. Die Rollen und Aufgaben sind in der Datenschutz-Organisation der TU Wien festgelegt.[1]

1.1 Geltungsbereich

Das Datenschutzhandbuch erstreckt sich auf sämtliche systematische Verarbeitungen personenbezogener Daten inner-halb der Geschäftsprozesse der TU Wien. Anonymisierte Daten, z.B. für statistische Auswertungen oder Untersuchun- gen, unterliegen nicht diesem Datenschutz-Handbuch.

1.2 Regelmäßige Überprüfung

Die Erfüllung der Aufgaben wird regelmäßig, aber auch anlassbezogen von dem_der Datenschutzbeauftragten überprüft. Die Datenschutzvorschriften samt Regelungen dieses Handbuchs sind zum Zweck der Gewährleistung des Datenschut- zes und zur Vermeidung von Rechtsansprüchen unbedingt einzuhalten. Für Folgen der bewussten Nichtumsetzung ist der_die Dateneigentümer_in[2] verantwortlich.

2 Regelungen

2.1 Gesetze, Richtlinien und Vorschriften

Das bestehende Datenschutz-Handbuch nimmt auf die Vorgaben der nachfolgenden Bestimmungen Bezug:

- Datenschutz-Grundverordnung („VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARL MENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“, DSGVO),
- Datenschutzgesetz (Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, DSG),
- Forschungsorganisationsgesetz (Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation, FOG).

[1] zu finden unter: https://www.tuwien.at/tu-wien/organisation/zentrale-bereiche/datenschutz-und-dokumentenmanagement/datenschutz/dokumente unter dem Punkt „Datenschutzrichtlinie“

[2] Dateneigentümer_innen sind jene Personen, die über die Verarbeitung von personenbezogenen Daten entscheiden

2.2 Datenschutzgrundsätze und ihre Umsetzung

Die DSGVO gibt Datenschutzgrundsätze und Erlaubnistatbestände vor, die bei der Verarbeitung von personenbezogenen Daten zu beachten sind. Werden diese Prinzipien eingehalten und liegt einer der Erlaubnistatbestände vor, dürfen personenbezogene Daten grundsätzlich verarbeitet werden. Demzufolge muss für jede Verarbeitungstätigkeit die durchgeführt wird, geprüft werden, ob die Verarbeitung zulässig ist.[3] Die Erlaubnistatbestände und die Datenschutzgrundsätze werden im Folgenden erläutert.

2.2.1 Die Erlaubnisbestände

Im Datenschutzrecht gilt das sogenannte Verbot mit Erlaubnisvorbehalt. Demnach ist die Verarbeitung von personenbezogenen Daten grundsätzlich verboten und nur in den Fällen zulässig, die im Gesetz ausdrücklich genannt sind. Eine Verarbeitung ist gemäß Art. 6 Abs. 1 DSGVO zulässig und damit rechtmäßig, wenn:

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

2.2.1.1 Die Einwilligung

Einwilligungen können schriftlich auf Papier, elektronisch oder mündlich erteilt werden. Der_die für die Datenverarbeitung Verantwortliche muss das Vorliegen der Einwilligung allerdings nachweisen können, weshalb empfohlen wird, die Einwilligung zu dokumentieren. Um sicherzustellen, dass eine Einwilligung vorliegt, sollte sie schriftlich eingeholt und aneinem vorher festgelegten Ort gespeichert werden. Die betroffenen Personen müssen außerdem auf ihr Widerrufsrecht hingewiesen werden und sie sind darüber zu informieren, wer der_die für die Verarbeitung der personenbezogenen Daten Verantwortliche ist und für welche Zwecke die Daten verarbeitet werden.

Bisher erhaltene Einwilligungen gelten weiter, sofern sie den Anforderungen der DSGVO entsprechen. Es ist also zu prüfen, ob der Zweck der Datenverarbeitung angegeben und ob eine Widerrufsrechtsbelehrung enthalten war und ob die Einwilligung nachweisbar ist. Andernfalls müssen Einwilligungen neu eingeholt werden. Da Einwilligungen zu jedem Zeitpunkt widerrufen werden können, sind diese nur dann als Erlaubnistatbestand heranzuziehen, wenn kein anderer Rechtfertigungsgrund zutrifft.[4] Einwilligungen sind daher nur in Ausnahmefällen einzuholen, wenn keine andere Rechtsgrundlage für die Datenverarbeitung besteht. Im Zweifelsfall ist das mit dem_der Datenschutzbeauftragten zu klären.

Beispiel: Das Institut xy hat im Jahr 2016 eine Konferenz abgehalten. Im Rahmen der Konferenzabwicklung ist eine E-Mail-Verteilerliste entstanden. Die Teilnehmer_innen haben bei der Anmeldung bestätigt, dass sie damit einverstanden sind, einen Newsletter zu erhalten, der sie über Themen zur Konferenz bzw. weitere Konferenzen in diesem Bereich informiert. Die Bestätigung liegt schriftlich vor und ist auf einem Institutsrechner / in der TUownCloud sicher abgespeichert

[3] Anmerkung: Dies ist nicht für jede singuläre Tätigkeit die durchgeführt wird zu prüfen, sondern es ist z.B. die Frage zu stellen, ob fürdie Verarbeitungstätigkeit „Personaldatenverwaltung“ ein Erlaubnistatbestand vorliegt. Liegt einer vor, ist zu prüfen, ob im Zusam-menhang mit dieser Verarbeitung die Datenschutzgrundsätze eingehalten werden.

[4] Vgl. RESMEDIA – Anwälte für IT-IP-Medien: FAQ zur Datenschutz-Grundverordnung (DSGVO). Was Unternehmen über das neue EU-Datenschutzrecht zum 25.05.2018 wissen müssen. Mainz/Berlin 2017. http://res- media.net/service/booklets/formular-download-booklet-faq-dsgvo/ (zuletzt abgerufen am 26.06.2020).

Nachdem bei der Anmeldung der Zweck angegeben wurde, muss keine erneute Einwilligung eingeholt werden. Beimnächsten Newsletter ist anzuführen, dass eine Abmeldung von der E-Mail-Verteilerliste jederzeit möglich ist.

Empfehlung: Die TU.it bietet unterschiedliche Mailinglisten an, in die auch TU-externe Adressen eingebunden werden und in die bestehenden Listen eingespielt werden können. Es bestehen vielfältige Einstellungsmöglichkeiten zur Abmeldung aus dem Verteiler, die Möglichkeit zur Selbstabmeldung ist gegeben. Informationen dazu finden sie hier: https://www.it.tuwien.ac.at/services/kooperation-und-kommunikation/e-mail-und-kalender/mailinglisten/.

Hinweis: Der Versand von Newslettern ist u.U. auch durch § 3 Z 7 UG (Unterstützung der nationalen und internationalen Zusammenarbeit im Bereich der Forschung und Lehre sowie der Kunst) gedeckt und fällt somit unter den Erlaubnistatbestand „öffentliches Interesse“ gem. Art. 6 Abs. 1 lit. e DSGVO. Dies ist im Einzelfall zu klären.

Sonderfall: Die Verarbeitung von besonderen Kategorien von personenbezogenen Daten.[5]

Unter diesen Begriff fällt gem. Art. 9 Z 1 DSGVO die Verarbeitung von personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Verarbeitung dieser Daten ist grundsätzlich untersagt, ausgenommen einer der Erlaubnistatbestände des Art. 9 Abs. 2 DSGVO liegt vor. Primär ist hier an eine Einwilligung, an ein Erfordernis aus dem Arbeitsrecht oder an einen Ausnahmetatbestand des FOG[6] zu denken.
Sämtliche Unterlagen sind sicher und entsprechend den Lösch- und Aufbewahrungsfristen[7] zu verwahren bzw. zu vernichten.

2.2.1.2 Datenverarbeitung zum Zweck der Vertragserfüllung

Alle personenbezogenen Daten, die im Zusammenhang mit einem Vertrag erhoben wurden / werden, dürfen weiter ohne Erlaubnis des_der Betroffenen verarbeitet werden, wenn das zur Begründung, Durchführung oder Beendigung der vertraglichen Beziehungen erforderlich ist.

Beispiel: Bestellung im Online-Shop: Kundendaten, die zur Abwicklung der Bestellung erforderlich sind (Name, Adresse, Bankverbindung, E-Mail-Adresse usw.) dürfen zu diesem Zweck gespeichert werden. Nicht erforderlich zur Zweckerreichung ist allerdings die dauerhafte Speicherung in einem Kundenkonto oder die Verwendung der E-Mail-Adresse für die Versendung von Mailings oder Newslettern. Dafür wäre eine Einwilligung erforderlich.[8]

Beispiel: Im Zuge einer Ausschreibung zur Beschaffung werden Daten von potentiellen Lieferanten gespeichert. Dies erfolgt zum einen im berechtigen Interesse (es liegt im wirtschaftlichen Interesse des Lieferanten, dass seine Daten an der TU Wien verarbeitet werden, damit er im Falle der Beauftragung kontaktiert werden kann) und in weiterer Folge zurErfüllung vorvertraglicher und später dann vertraglicher Verpflichtungen.

Empfehlung: Überprüfen Sie bereits vor der Vertragsunterzeichnung, welche Datenschutzklauseln im Vertrag enthalten sind.

2.2.1.3 Datenverarbeitung aufgrund einer rechtlichen Verpflichtung

Gibt es für die Verarbeitung von personenbezogenen Daten eine rechtliche Verpflichtung (beispielsweise eine gesetzliche Bestimmung im UG oder aus dem Arbeitsrecht), so ist die Verarbeitung zum Zweck der Erfüllung derselben erlaubt.

Beispielsweise sind umfassende Dokumentations- und Aufbewahrungspflichten des Handels- und Steuerrechts oder der Abgabenordnung, sowie die Regelungen der Sozialgesetzbücher und des Arbeitsrechts durch den Verantwortlichen zu erfüllen und einzuhalten.

[5] Anmerkung: Den Begriff der „sensiblen Daten“ kennt die DSGVO nicht.
[6] siehe: Anhang Kapitel 2 Forschungsorganisationsgesetz.
[7] in Bearbeitung.
[8] Vgl. RESMEDIA – Anwälte für IT-IP-Medien. Mainz/Berlin 2017. http://res-media.net/service/booklets/formular-download-booklet-faq-dsgvo/ (zuletzt abgerufen am 06.05.2019).

Beispiel: Eine rechtliche Verpflichtung zur Verarbeitung von personenbezogenen Daten ergibt sich beispielsweise aus Vorschriften des Steuerrechts, des Abgabenrechts, des Gleichbehandlungsgesetztes oder des Arbeitsrechts.

So ist beispielsweise der Dienstgeber gem. dem Allgemeinen Sozialversicherungsgesetz dazu verpflichtet, die Sozialversicherungsbeiträge an die österreichischen Gesundheitskassen abzuführen. Zu diesem Zweck darf der Dienstgeber alle dafür notwendigen personenbezogenen Daten der Arbeitnehmer_innen verarbeiten. Hier besteht also eine gesetzliche Verpflichtung gem. Art 6 Abs. 1 lit. c DSGVO für die Verarbeitung von personenbezogenen Daten die die TU Wien im Zusammenhang mit der Begründung eines Arbeitsverhältnisses erhält und die im Laufe dieses Verhältnisses entstehen.

Empfehlung: Wenn es für die Verarbeitung von personenbezogenen Daten keine vertragliche Grundlage gibt, prüfen Sie, ob eine rechtliche Verpflichtung vorliegt. Des Weiteren könnte die Verarbeitung auch im öffentlichen Interesse liegen (Details siehe 2.1.4). Wenn Sie nicht sicher sind, welcher Rechtsgrund zutreffend ist, kontaktieren Sie die Abteilung Da- tenschutz und Dokumentenmanagement (datenschutz@tuwien.ac.at).

2.2.1.4 Datenverarbeitung zur Wahrung öffentlicher Interessen

Besteht für die Verarbeitung von personenbezogenen Daten ein öffentliches Interesse, so ist die Verarbeitung auf Basis der Rechtsgrundlage gem. Art 6 Abs. 1 lit. e DSGVO zulässig.

Der Begriff „öffentliches Interesse“ beschreibt dabei das Vorhandenseins bestimmter Rechtsordnungen (Gesetzestexte), auf deren Basis ein_e Verantwortliche_r personenbezogene Daten verarbeiten darf. Die Verarbeitung kann also gerechtfertigt sein, wenn sie notwendig ist, um bestimmte Aufgaben – deren Ausführung im öffentlichen Interesse liegen – auszuführen oder um Aufgaben auszuführen, die dem_der Verantwortlichen Institution von offizieller Stelle übertragen wurden.[9] Art 6 Abs. 1 lit. e DSGVO begründet für sich selbst aber noch keinen Erlaubnistatbestand, sondern erst in Verbindung mit entsprechenden nationalen Gesetzen.[10]

Die TU Wien stützt sich hierbei vor allem auf das Universitätsgesetz 2000, in dem die Hauptaufgaben einer Universität definiert sind.

Beispiel: Zur Eröffnungsfeier des Zentrums für Mikro- und Nanostrukturen (ZMNS) werden Personen aus der umliegenden Nachbarschaft des ZMNS eingeladen. Diese Personen dürfen auf Basis des Art 6 Abs. 1 lit. e DSGVO i.V.m. § 3 lit. 11 UG (Information der Öffentlichkeit über die Erfüllung der Aufgaben der Universitäten) angeschrieben werden.

Das Continuing Education Center (CEC) der TU Wien führt einen neuen Lehrgang ein. Zur Bewerbung dieses Lehrganges darf das CEC Absolvent_innen der TU anschreiben. Grundlage für die Datenverarbeitung ist Art 6 Abs. 1 lit. e DSGVO i.V.m. § 3 lit. 5 UG (Weiterbildung, insbesondere der Absolventinnen und Absolventen von Universitäten und von Pädagoginnen und Pädagogen).

Empfehlung: Wenn für die Verarbeitung von personenbezogenen Daten kein öffentliches Interesse besteht, prüfen Sie, ob es eine vertragliche Grundlage oder rechtliche Verpflichtung gibt. Wenn Sie nicht sicher sind, welcher Rechtsgrund zutreffend ist, kontaktieren Sie die Abteilung Datenschutz und Dokumentenmanagement (datenschutz@tuwien.ac.at).

2.2.1.5 Datenverarbeitung zur Wahrung berechtigter Interessen

Dieser Erlaubnistatbestand kann nur dann in Anspruch genommen werden, wenn der konkrete Zweck der Datenerhebung und -verarbeitung klar im Einzelfall definiert ist. Die Datenerhebung muss also z.B. für den konkreten Zweck notwendig sein. Allerdings sind die berechtigten Interessen des Unternehmens/ der Institution gegen die Interessen des_der Betroffenen abzuwägen. Dabei muss das Interesse des Unternehmens / der Institution das Interesse der betroffenen Person am Schutz ihrer personenbezogenen Daten überwiegen.[11]

Beispiel: Ein berechtigtes Interesse kann vorliegen, *wenn die betroffene Person Kunde des Verantwortlichen ist oder in seinen Diensten steht. […] Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt*

[9] Vgl. https://uk.practicallaw.thomsonreuters.com/Glossary/UKPracticalLaw/Ibcdae8145a0c11e89bf199c0ee06c731?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 (zuletzt abgerufen am 28.06.2020).
[10] Vgl. ErwGr 45 S. 1 DSGVO, sowie Schulz, in: Gola, DSGVO. 2018 in: J. Golla, L. Matthe: Das neue Datenschutzrecht und die Hoch-schullehre. In: Wissenschaftsrecht. Zeitschrift für deutsches und europäisches Wissenschaftsrecht. 51/2 (2018). S. 206 – 223.
[11] Vgl. RESMEDIA – Anwälte für IT-IP-Medien. Mainz/Berlin 2017. http://res-media.net/service/booklets/formular-download-booklet-faq-dsgvo/ (zuletzt abgerufen am 06.05.2019).

erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar.[12] Des Weiteren muss dabei die Erwartungshaltung der betroffenen Person geprüft werden, ob diese bei der Ersterhebung und deren Umständen vernünftigerweise absehen konnte, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.Es muss eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem_der Verantwortli- chen bestehen.[13]

Empfehlung: Angesichts dieser Formulierung besteht eine erhebliche Rechtsunsicherheit, für welche Anwendungsszenarien dieser Erlaubnistatbestand als Rechtsgrundlage herangezogen werden kann.[14] Daher wird empfohlen diesen Erlaubnistatbestand nicht als Rechtsgrundlage zu verwenden.[15]

2.2.2. Die Datenschutzgrundsätze

Unabhängig davon, dass eine Verarbeitung von personenbezogenen Daten nur zulässig ist, wenn einer der Erlaubnistatbestände greift, müssen **zusätzlich** auch die im Folgenden beschriebenen Datenschutzgrundsätze gemäß DSGVO eingehalten werden.

2.2.2.1. Rechtmäßigkeit

Dem Grundsatz der Rechtmäßigkeit wird nachgekommen, in dem nachgewiesen wird, dass einer der Erlaubnistatbestände erfüllt ist.

Beispiel: Zur Kundenkontaktpflege werden Kundendaten in einer Datenbank gespeichert. Es ist zu prüfen, ob dies per Gesetz erlaubt ist, ein öffentliches oder berechtigtes Interesse besteht, ob dafür eine vertragliche Grundlage vorliegt oder ob eine Einwilligung benötigt wird. Wenn einer der fünf Erlaubnistatbestände erfüllt ist, wird dem Grundsatz der Rechtmäßigkeit entsprochen.

2.2.2.2. Verarbeitung nach Treu und Glauben

Dieser Grundsatz wird erfüllt, wenn die personenbezogenen Daten nur so verarbeitet werden, wie es bei der Erhebung angegeben wurde und nicht anders. Die Verarbeitung darf nur in dem Umfang gemacht werden, auf welchen die Person, deren Daten verarbeitet werden, vertrauen durfte.

Beispiel: Im Zuge eines Forschungsprojektes erhalten Sie Zugang zu personenbezogenen Daten der Projektmitarbeiter_innen. Diese dürfen zum Zweck der Projektabrechnung und Projektabwicklung verarbeitet werden (vertragliche Grundlage ist der Fördervertrag). Es ist nicht erlaubt, diese Daten für die Weiterleitung von Jobinseraten der Firma abc zu verwenden, weil eine Bekannte in dem Bereich gerade jemanden sucht. Dies wäre ein Zuwiderhandeln gegen diesenGrundsatz. Die Projektmitarbeiter_innen müssen sich darauf verlassen können, dass Daten, die von ihrer Institution an die TU Wien übermittelt werden, nur im Rahmen und nur für den Zweck des Projekts verarbeitet werden.

2.2.2.3. Transparenz der Datenverarbeitung

Transparenz ist dann gewährleistet, wenn klar ist, wer für die Datenverarbeitung verantwortlich ist und für welchen Zweck die Daten verarbeitet werden. Es darf keine verdeckte oder geheime Verarbeitung von personenbezogenen Da- ten erfolgen, außer es ist im Gesetz geregelt. In diesem Grundsatz wird auf die Pflichten des_der Verantwortlichen in Art12 ff DSGVO Bezug genommen. Transparenz wird demgemäß unter anderem dadurch erreicht, indem Informationen zurVerarbeitung in präziser, leicht zugänglicher und verständlicher Form bereitgestellt werden. Zu informieren ist außerdem über den Umfang sowie den Zweck der Verarbeitung.[16]

Beispiel: Das Institut xy organisiert eine Konferenz. Die TU Wien ist für die Datenverarbeitung im Zusammenhang mit dieser Konferenz verantwortlich. Bei der Anmeldung ist allen Teilnehmer_innen offenzulegen, welche Daten, zu welchem Zweck, wie lange und wo verarbeitet werden. Es muss angeführt werden, ob Daten an Dritte (z.B. Hotels) übermittelt

[12] gl. zur Direktwerbung per E-Mail § 107 (3) TKG 2003, BGBl I 2003/70 idF sowie Art. 13 (2) E-Privacy-RL 2002/58/EG idF RL2009/136/EG.
[13] Vgl. Erwägungsgrund (ErwG) 47.
[14] Vgl. M. Kastelitz: Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten. In: R. Knyrim (Hg.): DatenschutzGrundverordnung. Praxishandbuch. Wien 2016. S. 106f.
[15] Anmerkung: Da die Erlaubnistatbestände 2.1. Z 4 und 2.1. Z 5 idR an der TU Wien nicht anzuwenden sind, werden sie hier nicht näher erläutert.
[16] Vgl. M. Kastelitz. In: R. Knyrim (Hg.). Wien 2016. S. 100f.

werden und ob sie an Drittstaaten gesendet und dort verarbeitet werden. Außerdem müssen die Teilnehmer_innen darauf hingewiesen werden, welche Rechte sie im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten haben.

Empfehlung: Vorlagen für die Informationspflichten bei Konferenzen erhalten Sie von Ihre_r Datenschutzkoordinator_in (DSK) und auf der Homepage unter dem Punkt „Datenschutzbrunch“: https://www.tuwien.at/tu-wien/organisation/zentrale-services/datenschutz-und-dokumentenmanagement/datenschutz/services/.

2.2.2.4. Zweckbindungsgrundsatz

Dieser Grundsatz besagt, dass die Datenverarbeitung nur zu vorher festgelegten, eindeutigen und legitimen Zwecken erfolgen darf und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise. Hierbei ist allerdings zu beachten, dass eine Datenverarbeitung für andere Zwecke als den ursprünglichen gem. Art. 5 Abs. 2 lit. b DSGVO i.V.m. Art. 6 Abs. 4 DSGVO dann zulässig ist, wenn

- die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erfolgt, oder
- eine Einwilligung der betroffenen Person vorliegt, oder
- dies auf Unionsrecht oder nationalem Recht der Mitgliedsstaaten beruht[17], oder
- der Kompatibilitätstest eine Vereinbarkeit ergibt.[18]

Beispiel: Von einem externen Konferenzteilnehmer liegt die schriftliche Zustimmung vor, dass seine E- Mail-Adresse gespeichert werden darf, um ihm Informationen für weitere Konferenzen zum Thema zukommen zu lassen. Diese Adresse darf nicht dazu verwendet werden, der Person Informationen zu Tätigkeiten des Alumni Clubs der TU Wien zuzusenden.

2.2.2.5. Grundsatz der Datensparsamkeit

Der Grundsatz der Datensparsamkeit wird erfüllt, wenn die Datenverarbeitung auf das zweckgebundene, notwendige Maß beschränkt wird. Es dürfen folglich keine Daten verarbeitet werden, die zur Erfüllung des angegebenen Verwendungszwecks nicht erforderlich sind. Personenbezogene Daten sollten nach Möglichkeit anonymisiert oder pseudonymisiert[19] werden.

Beispiel: Für eine zweitätige Exkursion im Rahmen einer Lehrveranstaltung innerhalb Österreichs wird ein Formular ausgefüllt, um die Teilnehmer_innen beim Hotel xy anzumelden. Auf dem Formular wird der Geburtsort abgefragt (weil z.B. ein altes Muster verwendet wird, wo dieser Punkt nie hinterfragt wurde). Der Geburtsort ist für die Hotelanmeldung nicht erforderlich und darf daher nicht erhoben werden.

2.2.2.6. Grundsatz der sachlichen Richtigkeit

Der_die für die Verarbeitung von personenbezogenen Daten Verantwortliche, hat sicherzustellen, dass die verarbeiteten Daten richtig sind. Das heißt die Daten müssen sachlich richtig und auf dem neuesten Stand sein. Außerdem sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

Beispiel: Im TISS wird der Student xy mit einer anderen Adresse angeführt als auf dem Formular zur Exkursionsanmeldung. Wenn man dies zufällig bemerkt, ist dem nachzugehen und die falsche Adresse zu korrigieren.

---

[17] siehe dazu: FOG. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009514 (zuletztabgerufen am 17.10.2018)

[18] Vgl. M. Kastelitz. In: R. Knyrim (Hg.). Wien 2016. S. 100f.

[19] Anmerkung: Unter Pseudonymisierung versteht man gem. Art. 4 Z 5 DSGVO die Verarbeitung von personenbezogenen Daten in einer Weise, dass diese Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Es handelt sich dabei aber nach wie vor um personenbezogene Daten, für die das Datenschutzgesetz gilt. Anony-misierte Daten sind Informationen, die auf keine Weise mehr Rückschlüsse auf eine Person zulassen. Es besteht also weder ein Personenbezug, noch kann ein solcher mittels „Schlüssel“ hergestellt werden, weshalb das Datenschutzgesetz hier keine Anwen- dung findet. Daten über Gruppen mit mehr als fünf Personen gelten nach Ansicht der Datenschutzbehörde als anonymisiert.

2.2.2.7. Begrenzte Speicherung

Die personenbezogenen Daten dürfen nur so lange gespeichert werden, wie dies für die Erfüllung des angegebenen Zweckes tatsächlich erforderlich ist. Eine Speicherung über diesen Zeitpunkt hinaus, bedarf einer separaten Einwilligungder Betroffenen[20]. Bei der Auswahl des konkreten Speicherorts der personenbezogenen Daten müssen außerdem stets datenschutzrechtliche Überlegungen mitbedacht werden.[21]

Beispiel: Für die Ausstellung von Visa für Konferenzteilnehmer_innen ist die Angabe der Reisepassnummer erforder-lich. Diese ist zum frühestmöglichen Zeitpunkt wieder zu löschen.

2.2.2.8. Integrität und Vertraulichkeit

Integrität im Sinne der DSGVO bedeutet, dass die Daten bei der Übermittlung von A nach B ihr Ziel unverändert errei-chen müssen. Vertraulichkeit bedeutet, dass der_die Verantwortliche sicherstellen muss, dass nur befugte Personen Zugriff auf die personenbezogenen Daten haben.

Zur Sicherstellung der Einhaltung des Grundsatzes der Vertraulichkeit werden alle Mitarbeiter_innen der TU Wien zur Geheimhaltung von personenbezogenen Daten, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, verpflichtet. Diese Verpflichtung zur Geheimhaltung bleibt auch nach Beendigung des Arbeitsverhältnisses aufrecht. Darüber hinaus sind auch etwaige Geschäftspartner_innen zur Einhal- tung der Vertraulichkeit zu verpflichten.

Die Verpflichtungserklärung zum Datengeheimnis[22] ist von Mitarbeiter_innen der TU Wien im Zuge des erstmaligen Logins im Single Sign-on Portal der TU.it zur Kenntnis zu nehmen.

Beispiel: Im Zuge eines Forschungsprojektes werden Daten aus dem Land xy an die TU Wien übermittelt, die für die Projektabrechnung benötigt werden. Die TU Wien ist dafür verantwortlich, dass die Daten korrekt gespeichert werdenund niemand Zugriff zu diesen Daten hat, der nicht in das Projekt involviert bzw. dazu berechtigt ist.

2.2.2.9. Rechenschaftspflicht

Dem Grundsatz der Rechenschaftspflicht kommt die TU Wien als Verantwortliche für die Verarbeitung von personenbezogenen Daten dann nach, wenn sie dazu in der Lage ist, die Einhaltung der Datenschutzgrundsätze nachzuweisen.

Dazu ist es notwendig, dass entsprechende Maßnahmen dokumentiert werden. Diese Aufgabe obliegt dem Rektorat der TU Wien.[23]

Die Verarbeitung von personenbezogenen Daten muss dokumentiert werden. Dies erfolgt über das Verzeichnis der Verarbeitungstätigkeiten[24] (VdV). Protokolldaten werden nach definierten Grundsätzen ausgewertet.[25] Etwaig notwendige Vertragswerke (z.B. Betriebsvereinbarung Datenschutz) zur Durchführung von Protokollierungsmaßnahmen werden durch die Personaladministration sichergestellt. Die Durchführung von Datenschutz-Audits erfolgt auf Initiative der Abtei-lung Interne Revision der TU Wien, in Abstimmung mit dem Rektorat und dem_der Datenschutzbeauftragten der TU Wien. Die Überprüfung durch einen externen Wirtschaftsprüfer erfolgt auf Initiative des Rektorats.

[20] Anmerkung: Zu beachten ist hier das FOG.
[21] Anmerkung: die Abteilung Datenschutz und Dokumentenmanagement (DSDM) arbeitet – in Abstimmung mit anderen österreichischen Universitäten – an einem einheitlichen Löschkonzept für die TU Wien.
[22] https://www.tuwien.at/index.php?eID=dms&s=4&path=Dokumente/Datenschutzerkl%C3%A4rungen%20Mitarbeiter_innen/Verpflichtungserklaerung_Datengeheimnis.pdf
[23] siehe: https://www.tuwien.at/tu-wien/organisation/zentrale-bereiche/datenschutz-und-dokumentenmanagement/datenschutz/datenschutzorganisation
[24] siehe: Kapitel 4.2.
[25] Die Logging-Richtlinie – als Teil der Richtlinie Datenschutz und Informationssicherheit – der TU Wien finden Sie hier unter dem Punkt „Datenschutzrichtlinien“: https://www.tuwien.at/tu-wien/organisation/zentrale-services/datenschutz-und-dokumentenmanage- ment/datenschutz/dokumente/

3 Informationspflichten, Betroffenenrechte und weitere Prozesse

Abgesehen von der Erfüllung eines Erlaubnistatbestandes und der Einhaltung der Datenschutzgrundsätze, gibt es gewisse Informationspflichten, die einzuhalten sind und Betroffenenrechte, denen auf Anfrage nachgekommen werden muss.

3.1 Informationspflichten bei der Datenerhebung

Die Erhebung der Daten erfolgt im Regelfall direkt bei der betroffenen Person. Nur in Ausnahmefällen und bei rechtlich zulässigen Fällen können die Daten von einer anderen Quelle bezogen / zugekauft werden.
Vor jeder Datenerhebung muss geprüft werden, ob eine Informationspflicht gegenüber der betroffenen Person besteht. Sofern dies zutreffend ist, sind der betroffenen Person alle gesetzlich geforderten Informationen in präziser, leicht zugänglicher und verständlicher Form zur Verfügung zu stellen (Anm.: in Form einer Datenschutzinformation[26]). Stammen die Daten von der betroffenen Person selbst, ist über folgende Punkte zu informieren:

- Namen und Kontaktdaten des_der Verantwortlichen,
- ggf. Kontaktdaten des_der Datenschutzbeauftragten,
- Verarbeitungszweck und Rechtsgrundlage der Verarbeitung,
- im Falle einer Datenverarbeitung aufgrund berechtigter Interessen des_der Verantwortlichen bzw. eines Dritten dieberechtigten Interessen, die von dem_der Verantwortlichen oder einem Dritten verfolgt werden,
- ggf. Empfänger der Daten,
- falls die Absicht besteht, die Daten in ein Drittland oder eine internationale Organisation zu übermitteln, muss über diesen Umstand informiert werden. In diesem Fall ist ebenso über das Vorhandensein oder das Fehlen eines Ange-messenheitsbeschlusses[27] der Europäischen Kommission zu informieren. Weiters ist ggf. über das Vorhandensein geeigneter Garantien zu informieren,
- über die Dauer der Speicherung bzw., wenn dies nicht möglich ist, die Kriterien für die Festlegung der Dauer derSpeicherung,
- die Betroffenenrechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch,
- auf die Möglichkeit des Widerrufs der Einwilligung, mit dem Hinweis darauf, dass die Datenverarbeitung bis zum Zeit-punkt des Widerrufs rechtmäßig war,
- über die Beschwerdemöglichkeit bei der Aufsichtsbehörde,
- darüber ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben bzw. für denAbschluss eines Vertrages erforderlich ist, einschließlich der Belehrung über die möglichen Folgen einer verweigerten Bereitstellung,
- ggf. ein Hinweis darauf, dass Profiling[28] betrieben wird, inkl. aussagekräftiger Informationen über die involvierte Logikund die Auswirkung der Entscheidung,
- ggf. Angaben über die Datenherkunft: werden die Daten nicht bei dem_der Betroffenen erhoben, sind die Quellenanzugeben, aus denen die Daten stammen (auch wenn es sich dabei um öffentlich zugängliche Quellen handelt),
- sollten die Daten für einen anderen als den ursprünglichen Zweck weiterverarbeitet werden, kommen auch Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen dazu.[29]

[26] = Datenschutzerklärung
[27] Anmerkung: ein Angemessenheitsbeschluss besagt, dass in diesem Land Datenschutzbestimmungen eingehalten werden, die den Anforderungen bzgl. Datenschutz der EU genügen. Die Liste der Länder für die ein Angemessenheitsbeschluss besteht finden Sie hier: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (zuletzt abgerufen am 30.06.2020).
[28] bzgl. Definition von Profiling, siehe Kapitel 3.6.
[29] Vgl. U. Illibauer: Informationsrecht und Modalitäten für die Ausübung der Betroffenenrechte. In.: R. Knyrim (Hg.). Wien 2016. S. 121f.

Beispiel: Für die Organisation einer Konferenz erhalten Sie von der Dachorganisation eine Liste von Teilnehmer_innen, damit Sie vor Ort die Anmeldung abwickeln können. Bereits bei der Anmeldung zur Konferenz sind die Teilnehmer_innen darüber zu informieren, welche Daten zu welchem Zweck verarbeitet werden.

Beispiel: Beim Besuch einer Webseite werden idR personenbezogene Daten (z.B. die IP-Adresse) verarbeitet und zum Teil auch an Dritte übermittelt (z.B. Google Analytics). Den Benützer_innen der Webseite ist die Information darüber, welche Daten über sie verarbeitet werden, in leicht zugänglicher Form zur Verfügung zu stellen.

Empfehlung: Wenn Sie eine eigene, nicht zentral verwaltete Webseite mit TU-Domain betreiben, prüfen Sie, ob eine solche Datenschutzerklärung auf Ihrer Seite zur Verfügung steht bzw. ergänzen Sie diese im Anlassfall.[30]

Alle Informationen, die beim Besuch der TU Wien Website verarbeitet werden, finden Sie hier: https://www.tuwien.at/index.php?eID=dms&s=4&path=Dokumente/Datenschutzerkl%C3%A4rungen%20Sonstige/Datenschutzerkl%C3%A4rung_Websites.pdf

Weitere Informationen bzgl. an der TU Wien verarbeiteter Daten finden Sie hier: https://www.tuwien.at/tu-wien/organisation/zentrale-bereiche/datenschutz-und-dokumentenmanagement/datenschutz/datenschutzorganisation

3.2 Betroffenenrechte

Gemäß Art. 15 DSGVO hat jede_r Betroffene das Recht, von dem_der Verantwortlichen eine Bestätigung darüber zu verlangen, ob und welche sie_ihn betreffende personenbezogenen Daten verarbeitet werden. Des Weiteren hat er_siedas Recht auf:

- **Auskunft:** Alle innerhalb der TU Wien verarbeiteten personenbezogenen Daten einer Person, sind dieser auf derenAnsuchen zur Verfügung zu stellen. Neben den personenbezogenen Daten müssen alle gesetzlich geforderten Zu- satzinformationen, wie beispielsweise die Zwecke der Datenverarbeitung, die Empfänger_innen oder die geplante Speicherdauer, mitgeteilt werden.
- **Berichtigung:** Stellt eine Person ein Ansuchen, dass ihre Daten berichtigt werden sollen und sind diese auch tat- sächlich unrichtig, müssen die Daten umgehend korrigiert werden. Soweit es nicht mit einem unverhältnismäßig ho-hen Aufwand verbunden ist, ist allen Empfänger_innen der fehlerhaften personenbezogenen Daten die Berichtigungmitzuteilen.
- **Löschung:** Stellt eine Person ein berechtigtes Ansuchen auf Löschung ihrer Daten (z.B. wenn die Daten für die Zwe-ckerreichung nicht mehr notwendig sind), müssen diese Daten unter Berücksichtigung des Wirtschaftlichkeitsgrund- satzes und etwaiger gesetzlicher Vorschriften unverzüglich gelöscht werden. Darüber hinaus muss sichergestellt sein, dass personenbezogene Daten, die durch einen externen Auftragsverarbeiter verarbeitet werden, von diesem ebenfalls gelöscht werden. Allen Empfänger_innen der betroffenen Daten ist die Löschung mitzuteilen, sofern dies nicht mit einem unverhältnismäßig hohen Aufwand verbunden ist.
- **Einschränkung:** Stellt eine Person ein berechtigtes Ansuchen, dass die Verarbeitung ihrer Daten eingeschränkt werden soll, muss durch technische Maßnahmen sichergestellt sein, dass die personenbezogenen Daten nicht mehrin die Datenverarbeitung integriert werden (die betroffenen Daten dürfen ausschließlich gespeichert bleiben). Soweites nicht mit einem unverhältnismäßig hohen Aufwand verbunden ist, ist allen Empfänger_innen der betroffenen Da- ten die Einschränkung der Verarbeitung der personenbezogenen Daten mitzuteilen.
- **Datenübertragbarkeit:** Erfolgt eine Datenverarbeitung in automatisierter Form und auf Basis der Einwilligung der betroffenen Person oder zur Erfüllung eines Vertrages, hat die Person ein Recht auf Datenübertragbarkeit der Daten,die durch den_die Betroffene_n zur Verfügung gestellt wurden bzw. durch dessen_deren Aktionen bei dem_der Ver- antwortlichen erstellt wurden. Das bedeutet, dass der Datensatz in einem strukturierten, gängigen und maschinenles-baren Format verarbeitet und im Falle eines berechtigten Ansuchens an die betroffene Person übermittelt werden muss. Auf Verlangen des_der Betroffenen muss der Datensatz auch an eine_n andere_n Verantwortliche_n übermit-telt werden.
- **Widerruf:** Eine Einwilligung zur Verarbeitung personenbezogener Daten kann jederzeit widerrufen werden. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der bisher erfolgten Verarbeitung nicht berührt.

[30] In diesem Fall kann die Datenschutzerklärung der TU Wien für Websites nicht verwendet werden.

- **Widerspruch:** Stellt eine Person einen begründeten Widerspruch gegen die Verarbeitung ihrer Datenn auf Grund von Art. 6 Abs. 1 lit. e oder f, muss die Datenverarbeitung in Bezug auf die konkret genannten Daten des_der Betroffenen umgehend eingestellt werden. Das Widerspruchsrecht ist gesetzlich genau umschrieben. Betroffenen wirdbeispielsweise ein Widerspruchsrecht gegen eine an sich rechtmäßige Verarbeitung personenbezogener Daten ein-geräumt, wenn bestimmte Voraussetzungen gegeben sind. Ein Widerspruchsrecht besteht auch dann, wenn Direkt-werbung betrieben oder Profiling eingesetzt wird.

Eine Anfrage müsste grundsätzlich nicht schriftlich gestellt werden, ebenso wenig wäre lt. DSGVO ein aktiver Nachweis der Identität erforderlich. Hat ein Unternehmen / eine Institution aber berechtigte Zweifel an der Identität des_der Betroffenen und um sicherzustellen, dass die Auskunft auch von der Person verlangt wird, der diese zusteht, wird empfohlen, zur Authentifizierung zusätzliche Informationen anzufordern. Ein Auskunftsbegehren ist unverzüglich, spätestens aber innerhalb eines Monats nach Einlangen, zu beantworten. In begründeten Fällen kann die Frist um bis zu zwei Monate verlängert werden.

Um sicherzustellen, dass eine Anfrage – unabhängig davon, ob es sich dabei um ein Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs-, Datenübertragbarkeits- oder Widerrufsbegehren handelt – dort eingeht, wo sie bearbeitet werden kann, um einen klar definierten Beantwortungsprozess und um die Beantwortungsfrist von einem Monat einhal-ten zu können, werden Betroffenenrechte an der TU Wien ausschließlich über das Ticket-System Assyst abgewickelt. Eswerden lediglich solche Anfragen als Datenschutzanfragen gewertet, die über das Webformular[31] eingelangt sind. Erhalten Sie Anfragen zu Betroffenenrechten via E-Mail, per Telefon, per Post etc. ist die anfragende Person auf dieses Web- formular zu verweisen. Die Anfrage wird ausschließlich von dem_der Datenschutzbeauftragten der TU Wien beantwortet.

Der_die Betroffene wird nach Ausfüllen des Webformulars inkl. Hochladen einer Ausweiskopie, welche der Authentifizierung dient, gebeten, eine Bestätigungs-E-Mail an das Ticket-System zu schicken. Mit Einlangen dieser Bestätigungsemail beginnt die Frist zu laufen. Es werden ausschließlich über das vollständig ausgefüllte Webformular eingehende Anfragen bearbeitet, da andernfalls eine gesetzeskonforme Abwicklung des Betroffenenrechts nicht gewährleistet werden kann.

Das Ticket ergeht an den_die Datenschutzbeauftragte_n und vier DSK. Der_die Datenschutzbeauftragte leitet die Anfrage an die DSK weiter. Diese prüfen – mit Unterstützung der Datenschutzansprechperson (DSA) – ob in ihrer / ihrem Fakultät / Rektoratsbereich personenbezogene Daten über die betroffene Person vorliegen. Daten, die in Abteilungen der Rektoratsbereiche (https://www.tuwien.at/tu-wien/organisation/zentrale-services/) verarbeitet werden, werden von den jeweils für die zentrale Einrichtung zuständige_n DSK_in abgefragt und müssen somit nicht von den Fakultäten ein- geholt werden. Ob und welche Daten über die betroffene Person vorliegen, ist mittels E-Mail an eine Sammeladresse zuübermitteln (Ticketnummer ist im Betreff in [R…] anzugeben). Dort werden sämtliche Daten gesammelt, von dem_der Datenschutzbeauftragten aufbereitet und von diese_r via passwortgeschütztem[32] Cloud-Ordner dem_der Betroffenen füreinen Monat zur Verfügung gestellt. Es wird lediglich Auskunft über die in Art. 15 DSGVO angeführten Informationen gegeben:

- die Verarbeitungszwecke,
- die Kategorien personenbezogener Daten, die verarbeitet werden,
- die Empfänger_innen oder Kategorien von Empfänger_innen, gegenüber denen die personenbezogenen Daten of-fengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfänger_innen in Drittländern oder bei internationalen Organisationen,
- falls möglich, die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nichtmöglich ist, die Kriterien für die Festlegung dieser Dauer,
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den_die Verantwortliche_n oder eines Widerspruchsrechts gegen dieseVerarbeitung,
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informatio-nen über die Herkunft der Daten,

[31] siehe: https://www.tuwien.at/tu-wien/organisation/zentrale-bereiche/datenschutz-und-dokumentenmanagement/datenschutz/auskunft.
[32] Anmerkung: Das Passwort wird von dem_der Betroffenen bei der Eingabe der Anfrage im Webformular generiert.

- über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik und die ange-strebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Anträge auf Löschung, Berichtigung etc. sind ebenfalls über das Webformular einzubringen und werden ausschließlich von dem_der Datenschutzbeauftragten beantwortet. Der_die Datenschutzbeauftragte erhält bei der Bearbeitung von Betroffenenrechten die Unterstützung von allen involvierten Abteilungen. Allgemeine Anfragen zum Thema Datenschutz sind an den_die Datenschutzbeauftragte der TU Wien über die E-Mailadresse datenschutz@tuwien.ac.at zu stellen.

3.3 Umgang mit Auftragsverarbeiten

Unter dem Begriff Auftragsverarbeitung versteht die DSGVO gem. Art. 4 Z 8 *eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet*. Entscheidend für die Qualifikation als Auftragsverarbeiter (bisher Dienstleister) ist, dass er die Daten im Auftrag des_der Verantwortlichen verarbeitet und nicht der Auftragsverarbeiter selbst über die Verarbeitungszwecke sowie -mittel entscheidet. Entscheidet der Auftragsverarbeiter selbst über einen Verarbeitungszweck oder die -mittel bzw. verstößt er gegen konkrete Weisungen des_der auftraggebenden Verantwortlichen oder gegen den zugrundeliegenden Auftragsverarbeitungsvertrag (Avv), wird er bezüglich dieser Verarbeitung zum_zur Verantwortlichen.[33]

Beispiel: Das BRZ betreibt im Auftrag der TU Wien die Software SAP zum Zweck der Personaldatenverwaltung. DasBRZ kann nicht über den Zweck der Datenverarbeitung bestimmen und ebenso wenig über die Mittel, die dazu einge-setzt werden und ist somit Auftragsverarbeiter der TU Wien.

Beispiel: Die Personaladministration der TU Wien übermittelt die Gehaltsdaten der Mitarbeiter_innen der TU Wien an das Finanzamt. Dieses verarbeitet die Daten aufgrund eigener Entscheidungen (bzw. auf Basis gesetzlicher Grundlagen)und bestimmt auch über die Mittel, die es für die Verarbeitung verwendet. Es handelt sich hierbei um keinen Auftragsverarbeiter, sondern um eine bloße Datenübermittlung auf Basis einer gesetzlichen Bestimmung.

Eine Datenverarbeitung durch einen Auftragsverarbeiter ist nur dann zulässig, wenn für die Verarbeitung eine Einwilligung vorliegt oder eine vertragliche oder gesetzliche Grundlage existiert. Außerdem ist sicherzustellen, dass für Datenverarbeitungen nur solche Auftragsverarbeiter herangezogen werden, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen (TOM) bei ihm getroffen werden, um eine Datenverarbeitung im Einklang mit der DSGVO zu gewährleisten.

Mit jedem Auftragsverarbeiter muss eine Vereinbarung zur Auftragsverarbeitung abgeschlossen werden (Avv), die zentral in der Abteilung Datenschutz und Dokumentenmanagement (DSDM) geprüft und abgelegt wird und gemäß Art. 28 DSGVO folgendes beinhaltet:

- den Gegenstand des Vertrages, sowie die Dauer der Verarbeitung,
- die Art und den Zweck der Datenverarbeitung,
- die Art der personenbezogenen Daten die verarbeitet werden (z.B. Name, Anschrift, Matrikelnummer etc.),
- die Kategorien der betroffenen Personen (z.B. Mitarbeiter_innen, Lieferanten etc.) sowie,
- die Pflichten und Rechte des_der Verantwortlichen.

Des Weiteren ist in diesem Vertrag unter anderem zu vereinbaren, dass die personenbezogenen Daten vom Auf-tragsverarbeiter nur auf dokumentierte Weisung des_der Verantwortlichen verarbeitet werden.[34] [35]

Beauftragt ein Auftragsverarbeiter weitere Auftragsverarbeiter für die Erfüllung seiner Aufgaben (sog. Subauftragsverarbeiter), muss vertraglich in der Vereinbarung zur Auftragsverarbeitung sichergestellt sein, dass alle Pflichten auch gleichermaßen für die Subauftragsverarbeiter gelten. Darüber hinaus ist sicherzustellen, dass jede Änderung der Subauf- tragsverarbeiter nur aufgrund einer gesonderten oder einer generell erteilten schriftlichen Genehmigung erfolgen darf.

[33] Vgl. R.J. Bogendorfer: Der Dienstleister wird zum Auftragsverarbeiter. In.: Knyrim (Hg.). Wien 2016. S. 170f.
[34] siehe: Art. 28 Abs. 3 DSGVO bzgl. weiterer verpflichtender Vertragsinhalte.
[35] Vgl. R.J. Bogendorfer. In.: R. Knyrim (Hg.). Wien 2016. S. 170f.

Zur Identifikation von Auftragsverarbeitern ist von jeder / m Abteilung / Institut zu prüfen, ob eine Auftragsverarbeitungvorliegt. Dazu sind folgende Fragen zu beantworten:
Zur Identifikation von Auftragsverarbeitern ist von jeder / m Abteilung / Institut zu prüfen, ob eine Auftragsverarbeitung vorliegt. Dazu sind folgende Fragen zu beantworten:

- Ist das wesentliche Element der Dienstleistung auf die Verarbeitung personenbezogener Daten für Zwecke des Auf-traggebers (der TU Wien) gerichtet und besteht kein eigenes Interesse des Dienstleisters / Auftragsverarbeiters an den Daten?
- Legt die TU Wien die Zwecke und Mittel der Verarbeitung im Wesentlichen selbst fest?
- Hat die datenverarbeitende Stelle ausschließlich eine (technische) Hilfs- oder Unterstützungsfunktion?

Werden diese drei Fragen positiv beantwortet, wird in der Regel eine Auftragsverarbeitung vorliegen.[36] Ist eine eindeu-tige Beantwortung dieser Fragen nicht möglich, wenden Sie sich bitte an den_die für Sie zuständige_n DSK oder an den_die Datenschutzbeauftragte_n.

In der Folge ist mit dem_der Auftragsverarbeiter ein Avv abzuschließen. Die Mustervorlage für einen Avv für die TU Wien erhalten Sie von ihrem_r DSK. Die Vorlage ist vom Auftragsverarbeiter auszufüllen, zu unterschreiben und an die TU Wien zu retournieren.

Von Seiten der TU Wien ist der Avv von derjenigen Person zu unterzeichnen, die den der Verarbeitung zugrundeliegenden Vertrag unterzeichnet hat. Eine unterzeichnete Version ist an den Auftragsverarbeiter zu übermitteln, eine Kopie verbleibt in Ihrer / m Abteilung / Institut und das Original ist der Abteilung DSDM zu übermitteln. Erhalten Sie Vertrags- vorlagen von Auftragsverarbeitern zur Unterzeichnung, sind diese vor der Unterzeichnung zur Prüfung an die Abteilung DSDM zu übermitteln. Manche Großunternehmen bieten vorunterzeichnete bzw. vorgefertigte Avv zum Download an. Diese Verträge müssen allerdings auch von der Abteilung DSDM geprüft werden. Unter Umständen kann es sein, dass dieser Avv nicht von der_dem Vertragspartner_in unterzeichnet werden muss. Zu Beweiszwecken muss dieser Vertrag jedoch von Seiten der TU Wien unterzeichnet werden und im Original in der Abteilung DSDM abgelegt werden.

3.4 Datenübermittlung an Dritte

Eine Datenübermittlung zu externen Unternehmen bzw. Stellen oder zwischen Gesellschaften der TU Wien darf nur erfolgen, wenn diese Übermittlung rechtlich zulässig ist. Sind Datenübermittlungen in ein Land außerhalb der Europäischen Union vorgesehen, ist zu prüfen, ob eine der folgenden Voraussetzungen erfüllt ist:

- die EU-Kommission hat ein angemessenes Schutzniveau für den Drittstaat festgestellt, wie etwa für Andorra, Argenti-nien, die Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Kanada, Neuseeland und die Schweiz,
- der Datentransfer basiert auf Standardvertragsklauseln, die die EU-Kommission genehmigt hat[37],
- der Datentransfer innerhalb eines Konzerns oder einer Unternehmensgruppe erfolgt aufgrund von „Binding CorporateRules“, die die zuständigen Aufsichtsbehörden genehmigt haben,
- der Datentransfer geht an ein Unternehmen / eine Institution, das / die sich europäischen Verhaltensregeln unterwor-fen hat oder über eine Zertifizierung verfügt,
- es liegt eine Einzelgenehmigung durch die zuständige Aufsichtsbehörde vor,
- es liegt eine Einwilligung des_der Betroffenen vor,
- es liegt ein Ausnahmetatbestand nach Art. 49 Abs. 1 Satz 1 b - g DSGVO (z. B. zur Vertragserfüllung),
- es handelt sich um einen überschaubaren Umfang des Datentransfers und es liegen zwingende berechtigte Interes-sen der Verantwortlichen vor.

Handelt es sich um eine Übermittlung in die USA, ist sie nur an „Privacy Shield“-zertifizierte Unternehmen zulässig.[38]

[36] Vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hg.): Begleitender Hinweis zu der Anlage Auftragsverarbeitung. Leitfaden. Berlin. 2017. S. 17. (https://www.bitkom.org/Bitkom/Publikationen/Begleitende-Hinweise-zu-der- Anlage-Auftragsverarbeitung.html (zuletzt abgerufen am 07.05.2019).
[37] siehe: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32010D0087 Achtung, der Wortlaut sollte keinesfalls geändertwerden! (zuletzt abgerufen am 07.05.2019).
[38] siehe: www.privacyshield.gov (zuletzt abgerufen am 07.05.2019).

Beispiel: Sie verwenden für die Abwicklung einer Konferenz Google Sheets. Das Unternehmen Google betreibt seine Rechenzentren auf der ganzen Welt.[39] Um ein möglichst hohes Sicherheitsniveau zu erreichen – so argumentiert Google – werden die Daten[40] an unterschiedlichen Orten gespeichert.[41]

Nachdem weder Taiwan noch Singapur von der EU-Kommission als sichere Drittstaaten angeführt werden und nichtausgeschlossen werden kann, dass dort Daten verarbeitet werden, sind Google-Services nicht zu verwenden.

Empfehlung: Die TU.it bietet die Services

- TUownCloud (https://www.it.tuwien.ac.at/owncloud/) und
- TUproCloud (https://www.it.tuwien.ac.at/services/kooperation-und-kommunikation/collaboration/tuprocloud-sync-und- share-fuer-projekte)

an. Dieses Service umfasst im Wesentlichen die auch von öffentlichen Cloudsystemen wie Dropbox bekannten Features, nur dass die Daten eben lokal auf einem Server der TU Wien liegen. Der Datenzugriff ist über Clients (Windows, Linux, Mac OS, iOS, Android), Web und WebDav möglich. Die Synchronisation mit beliebig vielen Geräten erfolgt automatisch oder entsprechend selbst getroffenen Einstellungen. Jede_r Mitarbeiter_in hat einen Speicherplatz von 20 GB zur eigenen Verfügung. Es wird allerdings aus Gründen des Datenschutzes und der Informationssicherheit empfohlen, die ownCloud auf so wenig Geräten wie nötig zu synchronisieren und per Einstellung nur jene Ordner zur synchronisieren, die für die jeweilige Aufgabenerfüllung erforderlich sind.

Über die TUproCloud ist es auch möglich, Inhalte mit Externen zu teilen und zu bearbeiten. TUproCloud stellt Mitarbeiter_innen für Projekte die Nutzung eines umfangreicheren, vom persönlichen TUown-Cloud-Speicher getrennten und unabhängigen Speicherplatzes zur Verfügung. Die TU-interne Projektkontaktperson der TUproCloud hat die Möglichkeit, sowohl die TU-internen wie auch die TU-externen Mitglieder ihrer Projektgruppe eigenständig zu verwalten.

Empfehlung: Für die Koordination von Terminen werden folgende Services empfohlen:

- Termino: https://www.termino.gv.at/meet/de
- DFN Terminplaner: https://terminplaner4.dfn.de/

Eine Übermittlung an Dritte ist rechtlich dann zulässig, wenn es dafür eine vertragliche oder gesetzliche Grundlage gibt oder wenn eine Einwilligung dafür vorliegt.

Beispiel: Zum Zweck der Anmeldung einer Mitarbeiterin werden Daten an die Sozialversicherung übermittelt. Basis dafür ist das Beamten-, Kranken- und Unfallversicherungsgesetz. Damit besteht eine gesetzliche Grundlage, auf Basis derer die Daten an den Sozialversicherungsträger übermittelt werden dürfen.

3.5 Umgang mit Datenschutzvorfällen („Data Breach“)

Bei einem Datenschutzvorfall handelt es sich um einen Verlust der vollständigen Kontrolle über Daten an sich und darüber, was mit personenbezogenen Daten passiert. Es ist dabei unerheblich, ob der Datenabfluss bewusst unbefugt und mit Vorsatz oder unbewusst durch einen Fehler erfolgt ist. Im ErwG 85 zur DSGVO wird ein solcher Vorfall folgendermaßen definiert:

Verletzungen des Schutzes personenbezogener Daten sind unbeabsichtigte oder unrechtmäßige Datenvernichtungen, -verluste, -veränderungen oder -offenlegungen („Datenschutzverletzung“). Sie können – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

[39] siehe: https://www.google.com/about/datacenters/inside/locations/ (zuletzt abgerufen am 30.06.2020).
[40] Anmerkung: Welche Daten von Google gespeichert werden, finden Sie hier: https://www.gstatic.com/policies/privacy/pdf/20180525/853e41a3/google_privacy_policy_de_eu.pdf (zuletzt abgerufen am 30.06.2020).
[41] Vgl. H. Denker: Interview mit Google-Direktor Michale Korbacher. Was macht Google mit unseren Daten? 22.07.2017. t-online.de. https://www.t-online.de/digital/internet/id_81639226/was-macht-google-mit-unseren- daten-.html (zuletzt abgerufen am 30.06.2020).

Beispiel: Einem Mitarbeiter der TU Wien wurde in der U-Bahn sein Handy gestohlen, welches er auch für dienstliche Zwecke (E-Mail) nutzt.

Beispiel: Eine Datenbank, in der personenbezogene Daten gespeichert werden, wurde durch Ransomware verschlüsselt. Das Institut / der_die Dateneigentümer_in hat die Kontrolle über die Daten verloren.

Beispiel: Ein Ordner mit ausgefüllten Prüfungen geht verloren.

Beispiel: Ein_e Mitarbeiter_in der TU Wien wurde Opfer eine Phishing Attacke. Da bei solchen Attacken nicht ausgeschlossen werden kann, dass unbefugte Personen Zugriff auf personenbezogene Daten erlangen, ist dies jedenfalls als Data Breach im Sinne der DSGVO zu werten.

Im Falle der Verletzung des Schutzes personenbezogener Daten beispielsweise aufgrund von Angriffen auf die IT-Infrastruktur eines Unternehmens / einer Institution, Hackerangriffen, Verlust externer Datenträger mit personenbezogenen Daten, sonstiger unberechtigter Zugriff auf Daten, etc. sind die internen sowie die nach der DSGVO und nationalen Gesetzen bestehenden Melde- und Informationspflichten zu beachten.

Darüber hinaus ist ein relevanter Datenschutzvorfall, der als „mit großer Wahrscheinlichkeit nicht risikolos für die Betroffenen“ einzustufen ist, umgehend nach Bekanntwerden an die Aufsichtsbehörde zu melden. Diese Meldung erfolgt möglichst innerhalb von 72 Stunden ausschließlich durch den_die Datenschutzbeauftragte_n. Erfolgt die Meldung nicht binnen 72 Stunden, so ist dies schriftlich zu begründen. Es ist zulässig, eine Benachrichtigung zu unterlassen, wenn der_die Verantwortliche durch Maßnahmen sichergestellt hat, dass mit hoher Wahrscheinlichkeit kein signifikantes Ri- siko für die Rechte und Freiheiten der betroffenen Personen mehr besteht.[42]

Von einem Datenschutzvorfall betroffene Personen müssen darüber hinaus benachrichtigt werden, wenn für den Schutz ihrer personenbezogenen Daten ein hohes Risiko besteht. Auftragsverarbeiter müssen im Rahmen der Auftragsverarbeitung vertraglich verpflichtet werden, dass diese im Falle von Datenschutzvorfällen umgehend alle relevanten Informationen an die TU Wien übermitteln.

Gemäß Art 33 Abs. 5 DSGVO ist jegliche Verletzung des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehender Fakten, von deren Auswirkun- gen und der ergriffenen Abhilfemaßnahmen zu dokumentieren. Dies unabhängig davon, ob ein Vorfall der Datenschutz- behörde gemeldet wurde oder nicht. Diese Dokumentation soll es der Aufsichtsbehörde ermöglichen, die Einhaltung die-ses Artikels zu prüfen.

Datenschutzvorfälle können in drei unterschiedliche Kategorien unterteilt werden (wobei alle drei Kategorien gleichzeitig zutreffen können):

- **Verletzung der Vertraulichkeit:** Daten werden nichtberechtigten Personen zugänglich oder generell öffentlich zu-gänglich, obwohl sie nicht für die Öffentlichkeit bestimmt sind.
- **Nicht-Verfügbarkeit:** personenbezogene Daten sind nicht mehr verfügbar; Verlust der Kontrolle über die Daten; per-sonenbezogene Daten wurden unbeabsichtigt gelöscht; der Zugangsschlüssel zu den Daten ist verloren gegangen.
- **Verlust der Integrität:** personenbezogene Daten werden von nicht dafür autorisierten Instanzen verändert.

Wurde einer dieser Grundsätze verletzt, gilt es zu beurteilen, ob tatsächlich ein Datenschutzvorfall vorliegt und ob und an wen dieser in weiterer Folge gemeldet werden muss. Steht beispielsweise ein Service, mittels dessen personenbezo- gene Daten verarbeitet werden, für gewisse Zeit nicht zur Verfügung, so kann dies jedenfalls als Sicherheitsvorfall ge- wertet werden und muss als solcher auch dokumentiert werden. Abhängig von den personenbezogenen Daten, die da- von betroffen sind und insbesondere, welche Auswirkung dieser Vorfall auf die betroffenen Personen hat, ist zu entschei-den, ob dieser Vorfall als Datenschutzvorfall deklariert und an die Behörde gemeldet werden muss. Besteht ein Risiko, dass den betroffenen Personen aus diesem Vorfall ein Schaden entsteht, ist die TU Wien als Verantwortliche dazu ver- pflichtet, die Datenschutzbehörde in Kenntnis zu setzen. Ob ein solches Risiko besteht, ist im Einzelfall zu beurteilen. Es sind jedenfalls alle möglichen Konsequenzen eines Datenschutzvorfalles in die Beurteilung miteinzubeziehen.

[42] Vgl. M. Oman: Daten weg – was nun? Data Breaches und ihre DSGVO-Folgen gem. Art. 33, 34 DSGVO. In: R. Knyrim (Hg.). Wien 2016. S. 209f.

Ein Vorfall ist dann an die Datenschutzbehörde zu melden, wenn eines der potentiellen Risiken für die Rechte und Freiheiten einer Person eintreten könnte, außer es ist sehr unwahrscheinlich, dass ein solches Szenario eintritt.[43] An den_die Datenschutzbeauftragte ist ein Datenschutzvorfall in jedem Fall zu melden.

Beispiel: Eine Mailingliste der TU.it ist für fünf Stunden nicht erreichbar. Es können in dieser Zeit keine Newsletter verschickt werden. Dies ist jedenfalls als IT-Sicherheitsvorfall zu vermerken. Sofern die Liste nicht an die Öffentlichkeit gelangt ist, ist keiner betroffenen Person ein Schaden entstanden. Das Datenschutzrecht ist in diesem Fall nicht relevant.
Beispiel: Die Konferenzdatenbank der Fakultät XY wurde durch Ransomware verschlüsselt und ist nicht mehr zugänglich. Der Vorfall ist jedenfalls als Sicherheitsvorfall zu vermerken. Da die Anmeldeliste für die geplante Konferenz nicht mehr zu Verfügung steht (und man auch kein Lösegeld bezahlen will), sind die Daten erneut zu erheben. Da nicht abgeschätzt werden kann, was mit den Daten passiert (es wurden z.B. Kreditkartendaten gespeichert), sind die Teilneh- mer_innen, sofern möglich, über diesen Vorfall zu informieren. Ist dies nicht auf direktem Weg möglich, muss dies über andere Kanäle erfolgen.
Beispiel: Ein unverschlüsselter USB-Stick, auf dem personenbezogene Daten gespeichert wurden, ist verloren gegangen. Da nicht ausgeschlossen werden kann, dass eine unbefugte Person Zugriff auf diese Daten erhält oder diese sogar veröffentlicht werden, ist dieser Vorfall jedenfalls intern als Datenschutzvorfall zu melden. Über das weitere Vorgehen entscheidet dann der_die Datenschutzbeauftragte.
Beispiel: Ein Handy, welches auch dienstlich genutzt wurde, wird gestohlen oder geht verloren. Das Telefon war nicht verschlüsselt, aber versperrt. Da nicht ausgeschlossen werden kann, dass eine unbefugte Person Zugriff auf diese Da-ten erhält oder diese sogar veröffentlicht werden, ist dieser Vorfall jedenfalls intern als Datenschutzvorfall zu melden. Über das weitere Vorgehen entscheidet dann der_die Datenschutzbeauftragte.

3.5.1 Verlauf des Datenschutzvorfalls und Prozessbeschreibung

1. Datenschutzvorfall ereignet sich.
2. Erkennen des Datenschutzvorfalls durch den_die Dateneigentümer_in.
3. Unverzügliche Meldung an den_die unmittelbar Vorgesetzte_n.
4. Meldung durch den_die unmittelbar Vorgesetzte_n oder durch den_die Dateneigentümer_in an den_die Datenschutzbeauftragte_n der TU Wien per E-Mail an datenschutz@tuwien.ac.at, mit dem Betreff „DS-Vorfall“.
5. Der_Die Datenschutzbeauftragte macht ohne unnötige Zeitverzögerung eine Ersteinschätzung des Vorfalls und kontaktiert die notwendigen Abteilungen innerhalb der TU Wien. Bei Schäden, die beispielsweise am Netzlaufwerk aufgetreten sind, ist die TU.it unverzüglich zu benachrichtigen. Bei Verlust eines Laptops, USB-Sticks oder ähnlichem, ist gemeinsam mit dem_der unmittelbaren Vorgesetzten, der_die den Vorfall gemeldet hat, dem_der zuständigen DSK, dem_der Datenschutzbeauftragten und dem Rektorat zu klären, wie damit umgegangen wird.
6. Verhinderung eines weiteren Abflusses. Bei Verlust eines Handys beispielsweise, ist dieses via Webmail auf die Werkseinstellungen zurückzusetzen.[44]
7. Beginn der Minimierung möglicher Folgeschäden durch dafür qualifizierte Personen.
8. Der_Die Datenschutzbeauftragte nimmt gemeinsam mit dafür qualifizierten Personen eine Einschätzung der Art und Schwere der nachteiligen Folgen für betroffene natürliche Personen vor.[45]
9. Beginn des Fristenlaufs der Meldefristen.
10. Falls erforderlich, unverzügliche Information der vermeintlich betroffenen natürlichen Personen, hinsichtlich der Verletzung des Schutzes ihrer personenbezogenen Daten durch den_die Datenschutzbeauftragte.
11. Falls erforderlich, Information über die Panne an die Aufsichtsbehörde innerhalb von 72 Stunden durch den_die Datenschutzbeauftragte.

[43] Vgl. Article 29 Data Protection Working Party: Guidelines on Personal data breach notification under Regulation 2016/679. Working Paper (WP) 250. 3.10.2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (zuletzt abgerufen am 30.06.2020).
[44] Anleitung siehe: https://www.it.tuwien.ac.at/services/kooperation-und-kommunikation/e-mail-und-kalender/uptudate-e-mail-u-kalender- f-mitarb/anleitungen/ (zuletzt abgerufen am 01.07.2020). Anmerkung: diese Anwendung funktioniert nur, wenn man den Exchange Server am Handy aktiviert hat. Ruft man E-Mails via IMAP am Handy ab, scheint das Gerät nicht im Webmail auf.
[45] Anmerkung: Entsprechende Bewertungskriterien werden ausgearbeitet.

12. Maßnahmen zur Schadensbeseitigung der betroffenen natürlichen Person, (ev. unter Auflagen der Aufsichtsbehörde)durch die entsprechenden Abteilungen.

13. Analyse und Dokumentation des Hergangs der Datenpanne durch den_die Datenschutzbeauftragte in Zusammenar-beit mit allen Beteiligten.

3.6 Einsatz von Profiling

Unter dem Begriff „Profiling“ versteht Art. 4 Z 4 DSGVO *„jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.“*

Beim Einsatz von Profiling ist darauf zu achten, dass es zu keinen negativen Auswirkungen für die betroffene Person kommt. Sofern das Profiling eine negative Auswirkung nach sich zieht (z.B. Kündigung eines Vertrages oder Ablehnung eines Vertragsabschlusses oder Abmeldung von einer Lehrveranstaltung oder Ablehnung eines Studienantrages), muss dies stets durch einen rechtlichen Grund gedeckt sein. Vor jedem Einsatz von Profilingmaßnahmen muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Arbeitsrechtliche Bestimmungen sind jedenfalls einzuhalten.

3.7 Abschluss einer Vereinbarung bei gemeinsam für die Verarbeitung Verantwortlichen

Im Fall, dass eine Verarbeitungstätigkeit gemeinsam und gleichberechtigt mit anderen Verantwortlichen durchgeführt wird, handelt es sich um eine gemeinsame Verantwortlichkeit im Sinne der DSGVO. Die Übermittlung personenbezogener Daten unter gemeinsam Verantwortlichen ist ein eigener Verarbeitungsvorgang im Sinne des Art. 4 Z 2 DSGVO undbedarf als solcher einer Rechtsgrundlage.

Die Möglichkeit der gemeinsamen Verantwortlichkeit in Bezug auf eine Datenverarbeitung dient unter anderem dazu, Haftungsfragen in Fällen zu regeln, bei denen eine Stelle gemeinsam mit mindestens einer anderen Stelle die Festle- gung der Zwecke und Mittel der Verarbeitung trifft.[46] So soll verhindert werden, dass sich der_die einzelne an einer Da- tenverarbeitung Beteiligte seiner_ihrer datenschutzrechtlichen Verantwortlichkeit und seiner_ihrer Haftung entledigt, wenn er_sie zwar nicht alleine über die Zwecke und Mittel einer Verarbeitung entscheidet, jedoch neben anderen Beteiligten einen tatsächlichen Einfluss auf die Zwecke und die wesentlichen Elemente der Mittel der Verarbeitung ausübt.

Eine „gemeinsame Entscheidung“ über die Zwecke und Mittel der Verarbeitung setzt voraus, dass jede_r der Beteiligten einen bestimmenden tatsächlichen Einfluss auf die Datenverarbeitung nimmt. Die bloße Zusammenarbeit mehrerer Stellen im Rahmen einer Kette führt als solche nicht zwingend zu einer gemeinsamen Verantwortlichkeit.

Gemeinsame Verantwortlichkeit kann außerdem vorliegen, wenn einzelne Beteiligte für bestimmte Teile bzw. Phasen einer Verarbeitung getrennt verantwortlich sind, jedoch die Daten über eine gemeinsame Plattform zusammengetragen werden[47]. Die gemeinsame Verarbeitung beschränkt sich dann allerdings auf den Betrieb der Plattform. Für die getrenn-ten Verantwortungsbereiche muss die Plattform selbst bereits zwischen den einzelnen dann nicht mehr gemeinsamen Verantwortlichen trennen.[48]

Bei Vorliegen einer gemeinsamen Verantwortung muss in einer transparenten Vereinbarung festgelegt werden, welche_r Verantwortliche welche Datenschutz-Aufgaben zu erfüllen hat. Insbesondere muss darin die Haftungs- und Aufgabenverteilung beim Umgang mit Betroffenenrechten genau geregelt werden. Diese Vereinbarung ist mit jedem_r gemeinsam Verantwortlichen gesondert zu treffen.

[46] siehe: Working Paper (WP) 169 der Art.-29-Gruppe, S. 17ff: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf# (zuletzt abgerufen am 01.07.2020).
[47] siehe: Working Paper (WP) 169 der Art.-29-Gruppe, S. 17ff: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (zuletzt abgerufen am 01.07.2020).
[48] Vgl. https://www.datenschutzzentrum.de/artikel/1215-Kurzpapier-Nr.-16-Gemeinsam-fuer-die-Verarbeitung-Verantwortliche,-Art.-26- DS-GVO.html (zuletzt abgerufen am 01.07.2020).

Für die Beurteilung, ob eine gemeinsame Verantwortung vorliegt und bei der Erstellung einer entsprechenden Vereinbarung, ist der_die Datenschutzbeauftragte der TU Wien vor der Vertragserstellung jedenfalls einzubeziehen. Diese_r prüft, im Einzelfall welche Verantwortung die TU Wien trägt.

Beispiel: Im Rahmen einer Forschungsplattform, gegründet von den Universitäten A, B und C und einem Industrieunternehmen, wird eine gemeinsame Website betrieben. Die Webseite nutzt Google-Analytics und verwendet Social-Media-Plug-Ins (z.B. Twitter, LinkedIn und Facebook), wodurch jedenfalls personenbezogene Daten in Form der IP-Adresse jedes Seitenbesuchers verarbeitet werden. Im Rahmen der Erstellung des Konsortialvertrages kann es erforderlich sein,eine Vereinbarung darüber zu treffen, wer für die Verarbeitung der personenbezogenen Daten und die Umsetzung der Betroffenenrechte lt. DSGVO verantwortlich ist, insbesondere was die Wahrnehmung der Betroffenenrechte betrifft. Bei der Vertragsgestaltung sind die für die Ausgestaltung von Konsortialverträgen zuständigen Jurist_innen der TU Wien jedenfalls miteinzubeziehen.

4 Datenschutzorganisation- und Dokumentation an der TUW

Für die Umsetzung und die Einhaltung aller Vorgaben aus dem Datenschutz ist das Rektorat der TU Wien verantwort-lich. Für die strategische Entwicklung und die Vorlage von Konzepten zur Umsetzung des Datenschutzes an der TU Wien ist das lt. Geschäftsordnung zuständige Rektoratsmitglied verantwortlich.

Dazu werden durch das Rektorat Rollen und Verantwortlichkeiten im Bereich Datenschutz festgelegt und über den_die Datenschutzbeauftragte an die betroffenen Mitarbeiter_innen kommuniziert. Durch klare Regelungen von Aufgaben, Pflichten und Befugnissen wird die Vermeidung von Rollen- und Funktionskonflikten sichergestellt und die Umsetzung von Datenschutzprozessen optimiert. Die Prozessverantwortlichkeit, -abwicklung und -kontrollen werden vom Rektorat inAbstimmung mit dem_der Datenschutzbeauftragten festgelegt und an die Mitarbeiter_innen kommuniziert.

Die Datenschutzorganisation ist für die systematische Identifizierung, Analyse, Bewertung, Dokumentation und Kommunikation von Datenschutz- und Datensicherheitsrisiken verantwortlich und leitet angemessene Präventions- und Beseitigungsmaßnahmen ab.

Zum Aufbau der DS-Organisation an der TU Wien siehe: https://www.tuwien.at/tu-wien/organisation/zentrale-ser-vices/datenschutz-und-dokumentenmanagement/datenschutz/datenschutzorganisation/

4.1 Die Datenschutzorganisation der TU Wien

4.1.1 Datenschutzkommunikation und Berichtswesen

Der_die Datenschutzbeauftragte kommuniziert Datenschutzinhalte und -maßnahmen bedarfs- und anlassorientiert innerhalb der TU Wien (etwa an Mitarbeiter_innen und / oder Studierende), aber auch extern (etwa an Geschäftspartner_innen) insbesondere über die Datenschutzseite der TU Wien unter: https://www.tuwien.at/datenschutz/.

Der_die Datenschutzbeauftragte berichtet unmittelbar an das lt. Geschäftsordnung zuständige Rektoratsmitglied und verfasst darüber hinaus einmal jährlich (sowie anlassbezogen) einen Bericht an das gesamte Rektorat, zu den daten- schutzrechtlichen Themen aus dem vorangegangenen Geschäftsjahr sowie über die geplanten Aktivitäten zum ThemaDatenschutz für das nachfolgende Geschäftsjahr.

Die Erstellung von Richtlinien im Zusammenhang mit Datenschutz und Informationssicherheit obliegt der jeweiligenFachabteilung und erfolgt u.a. auf Anregung und unter Einbeziehung des_der Datenschutzbeauftragten.

Folgende Richtlinien werden im Rahmen der Datenschutz- und Informationssicherheitsorganisation in Zusammenarbeit mit den für den jeweiligen Prozess verantwortlichen Mitgliedern der Datenschutzorganisation entwickelt:

- IT Security / Acceptable Use Policy
- Logging-Richtlinie
- Cloud-Richtlinie
- CRM-Richtlinie
- Passwortrichtlinie
- Storage-Richtlinie

Die Erstellung und Weiterentwicklung des Datenschutzhandbuchs, sowie der FAQs obliegt dem_der Datenschutzbeauftragten in Abstimmung mit den für den jeweiligen Prozess verantwortlichen Mitgliedern der Datenschutzorganisation.
Die Richtlinien sind vom Rektorat zu verabschieden.

3.1.2. Datenschutzschulung

Durch die Datenschutzorganisation der TU Wien wird ein zentrales und bedarfsorientiertes Schulungsprogramm entwickelt. Dabei sind Mitarbeiter_innen aller Hierarchieebenen im Bedarfs- und Anlassfall zu schulen. Das Rektorat ist für die Entwicklung, die Durchführung und die Nachweisbarkeit der abgehaltenen Schulungen verantwortlich. Schulungsbedarf kann beim lt. Geschäftsordnung zuständigen Rektoratsmitglied, bei dem_der Datenschutzbeauftragten, sowie bei der Abteilung für Personalentwicklung angemeldet werden. Für die Konzipierung und Umsetzung der Schulungen ist das Rektorat gemeinsam mit dem_der Datenschutzbeauftragten zuständig.

3.1.3. Datenschutzberatung

Die Abteilung DSDM ist die zentrale Anlaufstelle für datenschutzrechtliche Anfragen der Angehörigen der TU Wien. Beratung steht nicht nur für konkrete Anfragen oder Verdachtsmomente zur Verfügung, viel mehr wird die frühzeitige Einbindung in Projekte der TU Wien empfohlen. Die Abteilung ist bei konkreten Fragestellungen zum Thema Datenschutz direkt über deren E-Mail-Adressen (datenschutz@tuwien.ac.at) zu kontaktieren.

3.1.4. Datenschutzdokumentation

Das Rektorat muss jederzeit, etwa gegenüber Aufsichtsbehörden, die Umsetzung, die Kontrolle, die Überwachung und den Status des Datenschutzes innerhalb der TU Wien sowie die getroffenen Maßnahmen nachweisen können. Zu diesen Nachweiszwecken sind sämtliche relevante Sachverhalte, Maßnahmen, Ergebnisse, Analysen etc. zu dokumentieren. Insbesondere sind vom Rektorat folgende Bereiche derart zu dokumentieren, dass sie jederzeit nachgewiesen wer-den können:

- Verzeichnis von Verarbeitungstätigkeiten,
- Bearbeitung von Datenschutzvorfällen,
- durchgeführte bzw. geplante Schulungsmaßnahmen,
- Erfüllung der Betroffenenrechte,
- Korrespondenz mit Aufsichtsbehörden,
- Durchführung von Datenschutzfolgen-Abschätzungen,
- Maßnahmen zur Sicherheit der Verarbeitung (Pseudonymisierung, Verschlüsselung, Datenzugriff, usw.),
- Auftragsverarbeitung und zugehörige Vereinbarungen,
- Vereinbarungen bei gemeinsamen Verantwortlichen,
- Nachweis über die Zulässigkeit von Datenübermittlungen in Drittländer,
- Nachweis über Rechtfertigungsgründe für die Datenverarbeitung,
- Überprüfungen (Audits),
- Berichterstattung und Unterweisung an das oberste Management.

4.2 Führung und Verwaltung des Verzeichnisses der Verarbeitungstätigkeiten

4.2.1 Neue Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten (VdV) ist zum Zweck des Nachweises der Einhaltung der DSGVO zu führen und ist auf Anfrage der Datenschutzbehörde derselben vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Unterlagen kontrolliert werden können.[49] Des Weiteren dient es als Grundlage für die Dokumentation von technischen und organisatorischen Maßnahmen, die zur Erhöhung der Datensicherheit gesetzt wurden. Die IT-technische Administration des VdV der TU Wien obliegt der TU.it.

Vor Beginn der erstmaligen Verarbeitung von personenbezogenen Daten ist von der für die Verarbeitung der Daten verantwortlichen Person (der_die Dateneigentümer_in) zu überprüfen, ob es für diese Tätigkeit bereits einen Eintrag im VdV der TU Wien gibt. Auskunft darüber gibt der_die für die / den Fakultät / Rektoratsbereich jeweils zuständige DSK, der_die über einen Zugang zum VdV verfügt.

Ist die Verarbeitungstätigkeit noch nicht eingetragen, ist von dem_der Dateneigentümer_in (wenn erforderlich mit der Unterstützung des_der DSK) zu prüfen, ob für diese Tätigkeit einer der Erlaubnistatbestände erfüllt ist. Fällt die Prüfung positiv aus, ist die Tätigkeit im VdV zu erfassen. Die personenbezogenen Daten dürfen in weiterer Folge erhoben und für den angegebenen Zweck verarbeitet werden. Es muss dabei sichergestellt sein, dass die Datenschutzgrundsätze eingehalten werden.

Beispiel: Sie werden von ihre_r Institutsleiter_in damit beauftragt eine Konferenz zu organisieren. Dafür wollen Sie unter anderem eine Liste aller angemeldeten Teilnehmer_innen erstellen in der Sie Name, Adresse, Staatsbürgerschaft, Reisepassnummer und E-Mail-Adresse erfassen. Bevor Sie diese Liste erstellen, stellen Sie sicher, dass einer der Erlaubnistatbestände erfüllt ist (das Anschreiben möglicher Interessent_innen kann mit einem bestehenden öffentlichen Interesse gerechtfertigt werden. Die Verarbeitung nach der erfolgten Anmeldung basiert auf einer vertraglichen Grundlage, da die Teilnehmer_innen einen Vertrag mit Ihnen abgeschlossen haben). Besprechen Sie mit Ihrer Datenschutzan- sprechperson bzw. direkt mit ihre_r DSK, ob es diese Verarbeitungstätigkeit bereits gibt. Wenn noch keine angelegt wurde, ist dies von dem_der DSK vorzunehmen.

Empfehlung / Hinweis: Für Verarbeitungsprozesse die standardmäßig an der TU Wien durchgeführt werden, wie etwa die Abwicklung von Konferenzen oder die Anmeldung zur Sponsion, wird eine Tätigkeit im VdV angelegt, zu der sich diejenigen Fakultäten, an denen die Verarbeitungstätigkeit ebenfalls vorgenommen wird, eintragen können.

Die Überprüfung der Inhalte des VdV obliegt dem_der Datenschutzbeauftragten. Dazu erfolgt einmal jährlich, falls erforderlich gemeinsam mit den jeweils für die Verarbeitungstätigkeiten zuständigen DSK, eine Qualitätskontrolle hinsichtlich der Aktualität und Vollständigkeit der Eintragungen im VdV. Die Überprüfung ist zu dokumentieren und im jährlichen Bericht an das Rektorat zu erwähnen.

4.2.2 IT-Services

Ebenfalls ins VdV einzutragen sind sämtliche IT-Systeme mittels derer personenbezogene Daten verarbeitet werden. Dazu sind Name, Beschreibung des Services und der Name des_der Service-Eigentümer_in an die Fachgruppe Securityund Monitoring der TU.it zu übermitteln, die als Administratorin der VdV-Software die Services in das VdV einträgt. Eine Überprüfung auf Vollständigkeit und Aktualität erfolgt einmal jährlich im Rahmen der oben genannten Überprüfung der Verarbeitungstätigkeiten durch den_die Datenschutzbeauftragte_n.

Beispiel: Sie betreiben am Institut einen eigenen E-Mail-Server. Es werden personenbezogene Daten verarbeitet. Der E-Mail-Server ist als IT-System an die Fachgruppe Security und Monitoring zu melden und als Verarbeitungstätigkeit imVdV anzuführen.

[49] siehe: Erwägungsgrund (ErwGr) 82 zur DSGVO: https://dsgvo-gesetz.de/erwaegungsgruende/nr-82/ (zuletzt abgerufen am 01.07.2020).

4.2.3 Änderungen bei bestehenden Verarbeitungstätigkeiten

Gibt es bei einer bestehenden Verarbeitungstätigkeit eine Änderung, ist diese Änderung im VdV einzutragen und zu dokumentieren. Ändert sich beispielsweise der Zweck oder die rechtliche Grundlage einer im VdV eingetragenen Verarbei tung, weil es eine Vertrags- oder Gesetzesänderung gab, so ist dies dem_der jeweils zuständigen DSK bekanntzugeben. Diese_r trägt die Änderung im VdV ein und informiert den_die Datenschutzbeauftragte_n. Wird eine Verarbeitungstätigkeit nicht mehr durchgeführt, so ist dies dem_der jeweils zuständigen DSK bekanntzugeben und von diese_r im VdV zu löschen. Der_die Datenschutzbeauftragte ist darüber in Kenntnis zu setzen.

Beispiel: In der GUT gibt es die Verarbeitungstätigkeit „Verarbeitung von Parkplatzgenehmigungen“ um die Vergabe von vergünstigten Parkplätzen an TU-Mitarbeiter_innen abzuwickeln. Ändern sich beispielsweise die Vertragsbedingungen des Garagenbetreibers dahingehend, dass für die Abwicklung eine zusätzliche Kategorie perso- nenbezogener Daten erforderlich ist (z.B. Ausweisdaten eines amtlichen Lichtbildausweises, die bisher nicht erforderlichwaren), so ist dies im VdV zu ergänzen. Wird das Angebot z.B. gänzlich gestrichen, ist die Verarbeitungstätigkeit zu lö- schen.

4.3 Technische und organisatorische Maßnahmen

Der Datenschutz wird durch die Implementierung von flankierenden Maßnahmen sichergestellt. Diese Maßnahmen umfassen insbesondere die Sicherstellung von Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Geschäftsprozesse (Technologie, Prozesse, Personen) und basieren auf den Grundsätzen „privacy by design“ sowie „privacy by default“. Für die Erarbeitung und Umsetzung von technischen Maßnahmen ist die TU.it unter Einbeziehung des_der Datenschutzbeauftragten zuständig. Für die Erarbeitung und Umsetzung von organisatorischen Maßnahmen ist das laut Geschäftsordnung zuständige Rektoratsmitglied unter Einbeziehung des_der Datenschutzbeauftragten verantwortlich.

4.3.1 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Bereits im Entwicklungsprozess einer neuen Datenverarbeitung muss sichergestellt sein, dass personenbezogene Daten entsprechend den datenschutzrechtlichen Vorgaben geschützt werden (Datenschutz durch Technikgestaltung).

Bestehende Datenverarbeitungen sind auf die datenschutzfreundlichste Weise voreinzustellen. Bei der Auswahl einer externen Software ist vertraglich sicherzustellen, dass die Softwareentwickler_innen diesen Verpflichtungen entspre- chen. Der_die Datenschutzbeauftragte, ist von Seiten des Auftraggebers bei der Vertragserstellung zu informieren undeinzubeziehen.

4.3.2 Datenflüsse zwischen Datenverarbeitungen

Beim Einsatz von Datenverarbeitungen müssen mögliche Datenflüsse zu anderen Datenverarbeitungen bedacht werden. Der Datenfluss zu anderen Datenverarbeitungen wird nur dort zugelassen, wo dieser tatsächlich für die Erfüllung des Verarbeitungszwecks notwendig ist. Auf Basis dieser Dokumentation muss klar ersichtlich sein, welche Daten aus einer Anwendung (z.B. Zeiterfassungssoftware) in ein anderes Programm (etwa elektronischer Personalakt) einfließen und gegebenenfalls in eine weitere Software (etwa Lohnverrechnungsprogramm) weiterfließen.

4.3.3 Sicherheit der Datenverarbeitung

Durch das Setzen von geeigneten technischen und organisatorischen Maßnahmen muss die Sicherheit der Datenverarbeitung zu jedem Zeitpunkt gewährleistet sein. Personenbezogene Daten müssen insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung geschützt werden. Dabei sind sowohl physische Maßnahmen wie Zutrittsbeschränkungen zu den verschiedensten Bereichen, als auch IT-bezogene Maßnahmen, wie etwa Zugriffsrechte auf Laufwerke und Datenbanken, zu berücksichtigen.

Wenn dies mit dem konkreten Verarbeitungszweck vereinbar ist, müssen personenbezogene Daten in pseudonymisier-ter oder anonymisierter Form verarbeitet werden. Die Auswahl der konkreten Maßnahmen erfolgt auf Basis eines risiko-basierten Ansatzes. Dabei müssen insbesondere die Ursache, Art, Eintrittswahrscheinlichkeit und Schwere des potenti-ellen Risikos aus Sicht der Betroffenen (nicht aus Sicht der TU Wien) sowie Kriterien der Wirtschaftlichkeit sowie das FOG berücksichtigt werden.

4.3.4 Lösch- und Aufbewahrungsfristen

Ist der Zweck der Datenverarbeitung erfüllt und liegen keine gesetzlichen Vorschriften vor, die eine längere Aufbewahrung der Daten erfordern, müssen die Daten grundsätzlich gelöscht oder anonymisiert werden. Einheitliche Lösch- und Aufbewahrungsfristen werden von der Abteilung Datenschutz- und Dokumentenmanagement erarbeitet.

Für Bereiche, für welche die Formulierung von einheitlichen Lösch- und Aufbewahrungsfristen nicht möglich ist, wird ein umfassendes Rollen- und Berechtigungskonzept erarbeitet, welches den Anforderungen der DSGVO entspricht.

Sind Sie nicht sicher, ob Sie gewisse Daten löschen dürfen oder müssen, wenden Sie sich bitte an das Archiv der TUWien (archiv@zv.tuwien.ac.at) oder an den_die Datenschutzbeauftragte_n der TU Wien (datenschutz@tuwien.ac.at).

Bei der Löschung / Vernichtung von personenbezogenen Daten ist sicherzustellen, dass dies datenschutzkonform pas-siert.[50]

4.3.5 Initiierung, Durchführung und Dokumentation von technischen und organisatorischen Maßnahmen

Ob eine technische und / oder organisatorische Maßnahme initiiert werden muss ergibt sich aus dem Anlegen und der Überprüfung der im VdV gemeldeten Verarbeitungstätigkeiten, sowie aus den Prüfberichten der Abteilung Interne Revision. Initiiert werden sie sowohl vom Rektorat als auch von dem_der Datenschutzbeauftragten der TU Wien. Für die ordnungsgemäße Durchführung ist der / die jeweils damit beauftragte Rektoratsbereich / Abteilung verantwortlich.

Die Dokumentation von technischen und organisatorischen Maßnahmen erfolgt durch den_die jeweils zuständige DSKim VdV.

[50] Zur Entsorgung von personenbezogenen Daten in Papierform siehe: https://www.tuwien.at/index.php?eID=dms&s=4&path=Dokumente/Handlungsanleitungen%2520und%2520FAQs/Entsorgung_personenbezogener_Daten_in_Papierform.pdf (zuletzt abgerufen am 01.07.2020). Zur Entsorgung von Festplatten siehe: https://www.it.tuwien.ac.at/tudiskshredder/ (zuletzt abgerufen am 01.07.2020).

4.4 Prozessverantwortliche und Prozesskontrolle

Datenschutzprozesse an der TU Wien:

- Umsetzung der Betroffenenrechte:
  - Prozessablauf: Kapitel 3.2.
  - Prozessverantwortliche: Datenschutzbeauftragte_r, TU.it, Dateneigentümer_in, Betreiber_in von IT-Services
  - Prozesskontrolle: Interne Revision
- Datenschutzauskunft:
  - Prozessablauf: Kapitel 3.2.
  - Prozessverantwortliche: Datenschutzbeauftragte_r, DSK
  - Prozesskontrolle: Interne Revision
- Datenschutzvorfall:
  - Prozessablauf: Kapitel 3.5.
  - Prozessverantwortliche: Dateneigentümer_in, unmittelbar Vorgesetzte_r in dessen_deren Bereich der Daten-schutzvorfall aufgetreten ist, DSB, Auftragsverarbeiter, Betreiber_in des betroffenen IT-Services
  - Prozesskontrolle: Interne Revision
- Datenschutz-Folgenabschätzung:
    - Prozessablauf siehe Anhang: 1. Datenschutzfolgenabschätzung.
    - Prozessverantwortliche: Datenschutzbeauftragte_r, DSK
    - Prozesskontrolle: Interne Revision
- Anlegen neuer oder Erfassung von Änderungen einer Verarbeitungstätigkeit:
  - Prozessablauf siehe Kapitel 4.2.
  - Prozessverantwortliche: Daten Eigentümer_in, DSA, DSK, Datenschutzbeauftragte_r, Betreiber_in des IT-Ser-vices
  - Prozesskontrolle: Interne Revision
- Aufbewahrung und Löschung von Daten:
  - Prozessablauf: Kapitel 4.3.4. und 2.2.7.
  - Prozessverantwortliche: Dateneigentümer_in, Betreiber_in des IT-Services, Datenschutzbeauftragte_r
  - Prozesskontrolle: Interne Revision
- Datenübermittlung an Dritte:
  - Prozessablauf siehe Kapitel 3.4.
  - Prozessverantwortliche: Dateneigentümer_in, Betreiber_in des IT-Services, Datenschutzbeauftragte_r
  - Prozesskontrolle: Interne Revision
- Umgang mit Auftragsverarbeitern und gemeinsam für die Verarbeitung Verantwortlichen:
  - Prozessablauf siehe Kapitel 3.3. und 3.7.
  - Prozessverantwortliche: Datenschutzbeauftragte_r , Dateneigentümer_in
  - Prozesskontrolle: Interne Revision
- Datenschutzberichtswesen:

- Prozessablauf: siehe Kapitel 4.1.1.
- Prozessverantwortliche: Datenschutzbeauftragte_r , DSK
- Prozesskontrolle: Interne Revision

- Datenschutzschulungen:
  - Prozessablauf: siehe Kapitel 4.1.2.
  - Prozessverantwortliche: Rektorat, Datenschutzbeauftragte_r
  - Prozesskontrolle: Interne Revision
- Technische und organisatorische Maßnahmen:
  - Prozessablauf: siehe Kapitel 4.3.
  - Prozessverantwortliche: die gesamte Datenschutzorganisation der TU Wien
  - Prozesskontrolle: Interne Revision
- Datenschutzaudits:
  - Prozessablauf: siehe Kapitel 2.2.9.
  - Prozessverantwortliche: Interne Revision
  - Prozesskontrolle: Rektorat

4.5 Umgang mit Aufsichtsbehörden

Den Aufsichtsbehörden müssen alle auf ihr Verlangen angefragten Informationen zur Verfügung gestellt werden, die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sind. Die Kommunikation findet ausschließlich über den_die Datenschutzbeauftragte_n der TU Wien statt.

5 ANHANG

5.1 Datenschutzfolgenabschätzung (DSFA)

Gemäß Art. 35 Abs. 1 DSGVO ist eine DSFA immer dann durchzuführen, *wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfanges, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.* Jedes einzelne dieser Kriterien kann dabei für sich die Pflicht zur Durchführung einer DSFA auslösen. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Alle Datenverarbeitungen, von denen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen ausgeht, müssen verpflichtend einer DSFA unterzogen werden. Bei neu geplanten Datenverarbeitungen muss die DSFA stets vor der Inbetriebnahme der Datenverarbeitung durchgeführt werden. Bereits bestehende Datenverarbeitungen sind bei entsprechender Risikoeinstufung ebenfalls einer DSFA zu unterziehen. Bei der Risikoeinschätzung gemäß den zentralen Vorgaben müssen stets auch Orientierungshilfen der nationalen Aufsichtsbehörden (z.B. eigene Listen) berücksichtigt werden.

Sie hat folgende Punkte zu enthalten:

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. ein-schließlich der von Verantwortlichen verfolgten berechtigten Interessen,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gem. Art. 37 Abs. 1 DSGVO und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird,dass diese VO eingehalten wird.

Gemäß Art. 35 Abs. 5 DSGVO kann die Aufsichtsbehörde eine Liste an Verarbeitungstätigkeiten veröffentlichen, für die keine DSFA notwendig ist. Die Österreichische Datenschutzbehörde hat eine Verordnung[51] veröffentlicht, indem fol- gende Verarbeitungstätigkeiten angeführt werden:

- Kundenverwaltung, Rechnungswesen, Logistik, Buchführung,
- Personalverwaltung für privatrechtliche und öffentlich-rechtliche Dienstverhältnisse,
- Mitgliederverwaltung,
- Kundenbetreuung und Marketing für eigene Zwecke,
- Sach- und Inventarverwaltung,
- Register, Evidenzen, Bücher,
- Zugriffsverwaltung für EDV-Systeme,
- Zutrittskontrollsysteme,
- Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung),
- Bild- und Akustikdatenverarbeitung in Echtzeit,
- Bild- und Akustikverarbeitungen zu Dokumentationszwecken,
- Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter undApotheker,

[51] siehe: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.pdfsig (zuletzt abgerufen am 01.07.2020).

- Rechts- und Beratungsberufe,
- Archivierung, Wissenschaftliche Forschung und Statistik,
- Unterstützungsbekundungen,
- Haushaltsführung der Gebietskörperschaften und sonstigen juristischen Personen öffentlichen Rechts,
- Öffentliche Abgabenverwaltung,
- Förderverwaltung,
- Öffentlichkeitsarbeit und Informationstätigkeit durch öffentliche Funktionsträger und deren Geschäftsapparate,
- Aktenverwaltung (Büroautomation) und Verfahrensführung,
- Organisation von Veranstaltungen,
- Preise und Ehrungen.[52]

Zusätzlich gibt es eine Verordnung der Datenschutzbehörde in der angeführt wird, für welche Verarbeitungsvorgänge zwingend eine DSFA durchzuführen ist[53].

Des Weiteren wurden vom Bundesministerium für Bildung, Wissenschaft und Forschung bei der Erstellung des FOG DSFAs für diverse Verarbeitungstätigkeiten im Bereich der Forschung durchgeführt (siehe dazu Anhang 2 Forschungsorganisationsgesetz).

Vor der Aufnahme einer Verarbeitungstätigkeit prüft der_die Datenschutzbeauftragte der TU Wien im Zuge der Erfas- sung im Verarbeitungsverzeichnis gemeinsam mit dem_der zuständigen DSK_in, ob für diese Tätigkeit eine DSFA durchzuführen ist. Dazu ist neben den oben genannten Bedingungen zu prüfen, ob es sich dabei um eine auf der White-List der österreichischen Datenschutzbehörde genannte Tätigkeit handelt oder ob für diese Tätigkeit bereits eine DSFA im FOG durchgeführt wurde. Trifft dies nicht zu, ist der_die Datenschutzbeauftragte zu kontaktieren, der_die beurteilt, obeine DSFA erforderlich ist und diese ggf. gemeinsam mit dem_der zuständigen DSK_in und weiteren qualifizierten Mitar-beiter_innen durchführt.

Die Durchführung der DSFA erfolgt gemäß einem festgelegten Prozess. Nähere Informationen dazu erhalten Sie von dem_der Datenschutzbeauftragten der TU Wien. Beachten Sie, dass insbesondere bei Big Data Anwendungen eine DSFA durchzuführen ist. Dies unabhängig davon, ob diese im Rahmen eines Forschungsprojekts oder im Bereich derVerwaltung der TU Wien durchgeführt wird.

5.2 Forschungsorganisationsgesetz

Dem Bereich Wissenschaft und Forschung kommt innerhalb der DSGVO eine besondere Rolle zu, was sich unter anderem daran zeigt, dass beispielsweise

- die Weiterverarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke oder wis-senschaftliche oder historische Forschungszwecke sowie statistische Zwecke keine Verletzung des Zweckbindungs-grundsatzes darstellt (Art. 5 Abs. 1 lit. e DSGVO),
- die Weiterverarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke oder wis-senschaftliche oder historische Forschungszwecke sowie statistische Zwecke keine Verletzung des Grundsatzes derSpeicherbegrenzung darstellt (Art. 5 Abs. 1 lit. e DSGVO),
- aufgrund unionsrechtlicher oder nationaler Rechtsvorschriften und unter Wahrung angemessener und spezifischer Maßnahmen sogar die Verarbeitung aller Arten von besonderen Kategorien von Daten für im öffentlichen Interesse liegende Archivzwecke oder Zwecke der wissenschaftlichen oder historischen Forschung sowie statistischer Zweckezulässig ist (Art. 9 Abs. 2 lit. j DSGVO),

[52] siehe dazu: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.pdfsig (zuletzt abgerufen am01.07.2020).
[53] siehe dazu: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.pdfsig (zuletzt abgerufen am07.05.2021).

- das Löschungsrecht bei im öffentlichen Interesse liegenden Archivzwecken oder der wissenschaftlichen und histori-schen Forschung oder für statistische Zwecke beschränkt werden kann (Art. 17 Abs. 3 lit. d DSGVO).

Eine EU-Verordnung ist grundsätzlich in allen Mitgliedsländern unmittelbar anwendbar. Es gibt aber in der DSGVO 69 Öffnungsklauseln. Das heißt, diese Bereiche können oder müssen von den Mitgliedsstaaten separat geregelt werden. Mit dem Datenschutzgesetz[54], dem Forschungsorganisationsgesetz – FOG[55] sowie einiger anderer Gesetze wurde diese Anpassung für Österreich vorgenommen.

Mit dem FOG wurde unter anderem Klarheit darüber geschaffen, was als „öffentliche Stelle“ im Sinne der DSGVO zu verstehen ist.[56] Demzufolge ist die TU Wien eine öffentliche Stelle und fällt damit unter die Strafbefreiungen des § 30Abs. 5 DSG (keine Geldstrafe).

Weitere Begriffsbestimmungen, wie etwa zu den Begriffen „Open Access“, „Open Data, „Big data“, „Forschungsmaterial“ etc. finden sich in § 2b Z1 bis 13 FOG.

Mit dem § 2c wurde die Möglichkeit der Verwendung von bereichsspezifischen Personenkennzeichen (bPK) für Zwecke der Wissenschaft und Forschung geöffnet. Die Verwendung dieser bPK stellt eine Pseudonymisierung im Sinne des Art. 4 Z 5 DSGVO dar und kann daher für die Verarbeitung von besonderen Kategorien von personenbezogenen Daten im Bereich der Wissenschaft und Forschung herangezogen werden.

In § 2d finden sich die grundlegenden Bestimmungen zum Schutz von personenbezogenen Daten. Demzufolge sind folgende Maßnahmen zu setzen:

1. Zugriffe auf personenbezogene Daten, die auf Grundlage des 1. Abschnitts des FOG automationsunterstützt verar-beitet werden, sind lückenlos zu protokollieren.
2. Verantwortliche und Auftragsverarbeiter, die personenbezogene Daten auf Grundlage des 1. Abschnitts des FOG verarbeiten und ihre Mitarbeiter_innen haben personenbezogene Daten, die ihnen ausschließlich auf Grundlage die-ses Abschnitts anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwie- genheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).
3. und
4. Personenbezogene Daten, die auf Grundlage des 1. Abschnitts des FOG automationsunterstützt verarbeitet werden, dürfen ausschließlich für Zwecke des FOG verarbeitet werden. Natürliche Personen, deren personenbezogene Da- ten auf Grundlage dieses Abschnitts verarbeitet werden, dürfen keine Nachteile aus der Verarbeitung erleiden, wobeidie Verarbeitung in Übereinstimmung mit diesem Abschnitt keinen Nachteil darstellt.
5. Verantwortliche, die Verarbeitungen auf Grundlage des § 2d Abs. 2 durchführen, also bereichsspezifische Personenkennzeichen verwenden, haben

    a) im Internet öffentlich einsehbar auf die Inanspruchnahme dieser Rechtsgrundlage hinzuweisen,

    b) bei Ausstattung ihrer Daten mit bereichsspezifischen Personenkennzeichen die Namensangaben jedenfalls zulöschen,

    c) vor Heranziehung von Registern gemäß Abs. 2 Z 3 jedenfalls einen Datenschutzbeauftragten (Art. 37 DSGVO) zubestellen,

    d) die Aufgabenverteilung bei der Verarbeitung der Daten (§ 2b Z 5) zwischen den Organisationseinheiten und zwi-schen den Mitarbeiter_innen ausdrücklich festzulegen,

    e) die Verarbeitung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheitenund Mitarbeiter_innen zu binden,

    f) jede_r Mitarbeiter_in über ihre / seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutz-vorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,

[54] siehe: BGBL I Nr. 24/2018.
[55] siehe: BGBL I Nr. 31/2018.
[56] siehe: § 2b Z 8 FOG.

g) die Zutrittsberechtigung zu den Räumlichkeiten, in denen die Verarbeitung der Daten (§ 2b Z 5) tatsächlich er-folgt, zu regeln,
h) die Zugriffsberechtigung auf Daten (§ 2b Z 5) und Programme und den Schutz der Datenträger vor der Einsichtund Verwendung durch Unbefugte zu regeln,
i) die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungenbei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
j) eine Dokumentation über die nach den lit. d bis i getroffenen Maßnahmen zu führen, um die Kontrolle und Be-weissicherung zu erleichtern,
k) ihrem Antrag auf Bereitstellung von Daten gemäß Abs. 2 Z 3 eine von der oder dem Verfügungsbefugten über dieDatenbestände aus denen die personenbezogenen Daten ermittelt werden sollen, unterfertigte Erklärung anzu- schließen, dass sie oder er dem Verantwortlichen die Datenbestände für die Untersuchung zur Verfügung stellt, wobei anstelle dieser Erklärung auch ein diese Erklärung ersetzender Exekutionstitel (§ 367 Abs. 1 der Exekuti- onsordnung, RGBl. Nr. 79/1896) vorgelegt werden kann,
l) bei Verarbeitung von gemäß Abs. 2 Z 3 bereitgestellten Daten (§ 2b Z 5) vorzusehen, dass nur die im Antrag ge-nannten natürlichen Personen auf die gemäß Abs. 2 Z 3 bereitgestellten Daten zugreifen dürfen sowie
m) bei Übermittlung von Namensangaben gemäß Abs. 2 Z 3 sind diese nach Erreichung der Zwecke gemäß Art. 89Abs. 1 DSGVO zu löschen.

Gemäß § 2d (2) Z 1 lit a bis d dürfen Forschungseinrichtungen sämtliche personenbezogene Daten jedenfalls verarbeiten, insbesondere im Rahmen von Big Data, personalisierter Medizin, biomedizinischer Forschung, Biobanken und der Übermittlung an andere wissenschaftliche Einrichtungen und Auftragsverarbeiter, wenn

a) anstelle des Namens, bereichsspezifische Personenkennzeichen für den Tätigkeitsbereich „Forschung“ (bPK-BF-FO)oder andere eindeutige Identifikatoren zur Zuordnung herangezogen werden oder
b) die Verarbeitung in pseudonymisierter Form (Art. 4 Z 5 DSGVO) erfolgt oder
c) Veröffentlichungen
    a) nicht oder
    b) nur in anonymisierter oder pseudonymisierter Form oder
    c) ohne Namen, Adressen oder Foto erfolgen oder
d) die Verarbeitung ausschließlich zum Zweck der Anonymisierung oder Pseudonymisierung erfolgt und keine Offenle-gung direkt personenbezogener Daten an Dritte (Art. 4 Z 10 DSGVO) damit verbunden ist.

Es ist folglich sicherzustellen, dass direkt personenbezogene Daten unter keinen Umständen veröffentlicht werden.

Durch § 2d Abs. 2 Z 3 soll die registerbasierte Forschung, die in ErwG 157 zur DSGVO ausdrücklich angeführt wird, auch innerstaatlich auf eine gesicherte Rechtsgrundlage gestellt werden. Durch die Verwendung von Registern können bessere Forschungsergebnisse erzielt werden, da sie auf einen größeren Bevölkerungsteil gestützt sind. Mit dieser Be- stimmung sollen möglichst alle bei öffentlichen Stellen und Behörden eingerichteten oder betriebenen Register zukünftig den wissenschaftlichen Einrichtungen offenstehen. Dabei sind unter Registern nicht nur öffentlich einsehbare Register imSinne des § 3 Z 18 des Bundesstatistikgesetzes 2000 gemeint, sondern sämtliche Verzeichnisse, Datenbanken oder ähnliche Anwendungen oder Verarbeitungsplattformen, die bundesgesetzlich vorgesehen sind. Staatsanwaltliche und strafgerichtliche Register sowie Register im Bereich der Gerichte, Rechtsanwälte und Notare sind von dieser Regelung ausgenommen. Für die Bereitstellung von Registerdaten ist ein Kostenersatz zu leisten (der öffentlichen Hand werden diese Kosten ersetzt). Das Recht auf Registerforschung besteht unabhängig davon, ob das betreffende Register perso- nenbezogene Daten enthält oder nicht.[57] Forschungseinrichtungen dürfen in Anwendung des FOG besondere Katego- rien von personenbezogenen Daten verarbeiten, wenn die betroffene Person freiwillig, in informierter Weise und unmiss- verständlich ihren Willen in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung bekundet, mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden zu sein, wobei die Angabe eines Zweckes durch die Angabe

[57] Vgl. Erläuterungen zum FOG. https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00068/fname_686447.pdf (zuletzt abgerufen am08.05.2019)

- eines Forschungsbereiches oder
- mehrerer Forschungsbereiche oder
- von Forschungsprojekten oder
- von Teilen von Forschungsprojektenerfolgen darf („broad consent“).

Gemäß Art. 5 Abs. 1 lit. e DSGVO dürfen personenbezogene Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken Art. 89 Abs. 1 DSGVO unbeschränkt gespeichert und gegebenenfalls sonst verarbeitet werden, soweit gesetzlich keine zeitlichen Begrenzungen vorgesehen sind. Dies ist allerdings nur als Zweifelsregelung zu verstehen, falls keine ausdrückliche Regelung getroffen wurde. Einschränkende Spezialbestimmungen gehen dieser Bestimmung vor (z.B. § 2f Abs. 3 FOG).
Die folgenden Rechte finden insoweit keine Anwendung, als dadurch die Erreichung von Zwecken gemäß Art. 89 Abs. 1 DSGVO voraussichtlich unmöglich gemacht oder ernsthaft beeinträchtigt wird:

- Auskunftsrecht der betroffenen Person (Art. 15 DSGVO),
- Recht auf Berichtigung (Art. 16 DSGVO),
- Recht auf Löschung bzw. Recht auf Vergessenwerden (Art. 17 DSGVO),
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO),
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO) sowie
- Widerspruchsrecht (Art. 21 DSGVO).

Die Erreichung von Zwecken gem. Art. 89 Abs. 1 DSGVO wird voraussichtlich dann unmöglich gemacht, wenn durch dieAusübung dieser Rechte Forschungsergebnisse nachträglich verändert würden. Eine ernsthafte Beeinträchtigung liegt vor, wenn die Erfüllung der Verpflichtungen für die oder den Verantwortlichen mit einem unverhältnismäßigen Aufwand verbunden wäre (§ 2e FOG).

Zum Zweck des Qualitätsmanagements von Forschungseinrichtungen dürfen diese insbesondere die folgenden Daten direkt personenbezogen verarbeiten, jedoch nur in pseudonymisierter oder anonymisierter Form veröffentlichen:

- hinsichtlich der Personen, die im Rahmen von Lehre bzw. Forschung tätig waren bzw. sind:

a) sämtliche Daten gemäß § 2g Abs. 1 bis 4 (alle Daten, die für die Abwicklung von Förderungen relevant sind),

b) soziobiografische und sozioökonomische Angaben,

c) qualitative Daten, wie insbesondere betreffend

- Relevanz des Studiums für die Beschäftigung,
- berufliches Fortkommen und Zufriedenheit,
- Wahrnehmung der Qualität und Relevanz ihrer Bildungs- und Ausbildungserfahrung sowie
- quantitative Daten, wie insbesondere betreffend

d) Einstieg ins Berufsleben und weitere (Aus-)Bildung,

a) Einkommen

b) Art des Vertrags,

c) Beschäftigungsstatus,

d) Beruf, Berufsstatus und Tätigkeit (im Verlauf),

e) Angaben zu geografischen und sektoralen Mobilitäten (§ 2b Z 7) sowie

f) sämtliche akademische Funktionen, Publikationen, Drittmitteleinwerbungen und Aktivitäten betreffend Technologietransfer sowie

- hinsichtlich der Personen, die im Rahmen der Lehre betreut wurden bzw. werden, die unter Z 1 genannten Angaben sowie quantitativen Daten, wie insbesondere betreffend

  a) Studienintensität,

  b) Studienmethode,

  c) Qualifikation(en),

  d) erhaltene Leistungspunkte sowie

  e) Studienfach.

Zur **Erhöhung der Transparenz bei Verarbeitungen** gem. Art. 89 DSGVO dürfen wissenschaftliche Einrichtungen (§2b Z 12)

1. wissenschaftliche Mitarbeiter_innen, die sich in einem aufrechten Arbeitsverhältnis zur jeweiligen wissenschaftlichenEinrichtung befinden, namentlich mit Foto und einer Liste ihrer Publikationen

- auf einer Website der wissenschaftlichen Einrichtung oder
- im Rahmen öffentlich zugänglicher Berichte der wissenschaftlichen Einrichtung

anführen, es sei denn, die Veröffentlichung ist geeignet, die öffentliche Sicherheit, die Strafrechtspflege, die umfassende Landesverteidigung, die auswärtigen Beziehungen oder ein berechtigtes privates oder geschäftliches Interesse zu verletzen, wobei der Veröffentlichung eines Fotos gemäß lit. a jederzeit widersprochen werden kann, oder

2. wissenschaftliche Mitarbeiter_innen, die sich nicht mehr in einem aufrechten Arbeitsverhältnis zur jeweiligen wissen schaftlichen Einrichtung befinden, sowie Studierende namentlich

- auf einer Website der wissenschaftlichen Einrichtung oder
- im Rahmen öffentlich zugänglicher Berichte der wissenschaftlichen Einrichtung anführen, es sei denn, die Veröffentlichung ist geeignet, die öffentliche Sicherheit, die Strafrechtspflege, die umfassende Landesverteidigung, die auswärtigen Beziehungen oder ein berechtigtes privates oder geschäftliches Inte- resse zu verletzen, oder

3. von Empfänger_innen von Förderungen aus Bundesmitteln, Forschungsaufträgen und Ähnlichem können zwecks Kontaktaufnahme für mindestens 10 Jahre Namensangaben, Personenmerkmale, Adress- und Kontaktdaten, Anga-ben zu Projektpartner_innen, Angaben zur Ausbildung sowie Angaben zu erhaltenen Mitteln und zu Mobilitäten ge- speichert werden.[58] Zusätzlich dürfen von ehemaligen wissenschaftlichen Mitarbeiter_innen und Studierenden Forschungsschwerpunkte und Angaben zu Publikationen verarbeitet werden.

4. von Wissenschafter_innen sowie ihnen nahestehenden Personen dürfen Namensangaben, Personenmerkmale undAngaben zum Lebenslauf verarbeitet werden.

Bezüglich **Wissens- und Technologietransfer** bestimmt § 2i: Ungeachtet allfälliger patentrechtlicher Bestimmungen ist die Verarbeitung, insbesondere im Sinne des § 2d Abs. 8 oder der Übermittlung personenbezogener Daten, für Technologietransfer zulässig, wenn

1. diese Verarbeitung erforderlich ist, um die Funktionalität der zu transferierenden Technologie zu erhalten, und

2. insbesondere durch Technikgestaltung gemäß Art. 25 DSGVO sichergestellt ist, dass Dritte (Art. 4 Z 10 DSGVO) keine tatsächliche Kenntnis der übermittelten Daten erlangen.

Unter diesen Voraussetzungen finden die Betroffenenrechte keine Anwendung.

Wissenstransfer ist unter den Voraussetzungen zulässig, dass an Stelle des Namens bereichsspezifische Personen- kennzeichen verwendet werden oder die Verarbeitung in pseudonymisierter Form erfolgt oder Veröffentlichungen nicht /nur in anonymisierter oder pseudonymisierter Form / ohne Name, Adresse, Foto erfolgen oder die Verarbeitung aus- schließlich zum Zweck der Anonymisierung oder Pseudonymisierung erfolgt und damit keine Offenlegung direkt personenbezogener Daten an Dritte verbunden ist.

[58] siehe: § 2g Abs. 1 Z 3 FOG.

Werden im Rahmen von Open-Science- und Citizen-Science-Projekten eigene personenbezogene Daten freiwillig zur Verfügung gestellt, ist ihre Verarbeitung für die zu Beginn des Projekts ausdrücklich kommunizierte Art, Umfang und Dauer zulässig. Die Löschung ist nur zulässig, wenn dadurch

1. die Projektziele und
2. die methodischen, insbesondere statistischen, Anforderungen an wissenschaftliches Arbeitennicht beeinträchtigt werden.

Werden im Rahmen von Open-Science- und Citizen-Science-Projekten personenbezogene Daten Dritter (Art. 4 lit. 10 DSGVO) zur Verfügung gestellt, ist ihre Verarbeitung für die zu Beginn des Projekts ausdrücklich kommunizierte Art, Umfang und Dauer jedenfalls zulässig, wenn

1. die Daten auf Beobachtungen oder Messungen im öffentlichen Raum beruhen oder
2. die Daten im Sinne des Art. 4 Z 5 DSGVO pseudonymisiert werden.

Die Löschung ist nur zulässig, wenn dadurch die Projektziele und die methodischen, insbesondere statistischen Anforderungen an wissenschaftlichen Arbeiten nicht beeinträchtigt werden.