Leitfaden zum Schutz personenbezogener Daten an der Universität Passau

Ziel des Leitfadens ist es, Sie in Ergänzung zu der durchgeführten Informationsveranstaltung am 06.12.2018 über die aktuell geltenden datenschutzrechtlichen Anforderungen zu informieren. Weiterhin möchten wir Ihnen mit diesem Leitfaden Handlungshilfen für Ihren täglichen Umgang mit personenbezogenen Daten zur Verfügung stellen.

→ **Hinweis:** Dieser Leitfaden unterliegt einer fortlaufenden Überarbeitung sowie Anpassung an die jeweils aktuellsten Entwicklungen im Zuge der Umsetzung der DSGVO. Insbesondere in Teil III. FAQ werden Neuerungen aus der gelebten datenschutzrechtlichen Praxis fortlaufend Eingang finden.

Für Fragen bei der Umsetzung datenschutzrechtlicher Anforderungen wenden Sie sich bitte an:

Datenschutzbeauftragter (extern)
Johannes Nehlsen
insidas GmbH & Co. KG
Tel.: +49 851 / 509 - 1126
datenschutz@uni-passau.de

Stellvertretung (intern)
Kathrin Bernecker
Raum N12 116
Tel.: +49 851/509-7124
datenschutz@uni-passau.de

Tel. extern: +49 871 / 20 54 94 – 0
Adresse extern: insidas GmbH & Co. KG, Wallerstraße 2 84032 Altdorf, Deutschland

Fragen oder Anregungen zum Leitfaden sowie zu den datenschutzrechtlichen Informationsveranstaltungen an der Universität richten Sie bitte an:

datenschutz@uni-passau.de

Stand: 15.03.2024

Inhaltsverzeichnis

Allgemeine Grundlagen zum Schutz personenbezogener Daten

Seit dem 25. Mai 2018 entfaltet die europäische Datenschutz-Grundverordnung **(DSGVO)** unmittelbare Wirkung in den europäischen Mitgliedsstaaten. Ab diesem Zeitpunkt müssen nun die Regelungen der DSGVO direkt und ohne weiteren Umsetzungsakt unseres nationalen Gesetzgebers angewendet werden.

I.

Daneben finden die nationalen Gesetze weiterhin in den Fällen Anwendung, in denen die DSGVO sogenannte „Öffnungsklauseln" vorsieht. Die Öffnungsklauseln geben den nationalen Gesetzgebern der Mitgliedsstaaten die Möglichkeit, Normen zu erlassen, welche die Vorschriften der DSGVO konkretisieren, ergänzen und modifizieren können. In Deutschland wurden entsprechende Konkretisierungen, Ergänzungen und Modifikationen insbesondere durch die Neuregelungen des Bundesdatenschutzgesetzes **(BDSG)** und des Bayerischen Datenschutzgesetzes **(BayDSG)** gesetzlich verankert. Im Hochschulkontext ist zudem auf das Zusammenspiel von DSGVO und hochschulrechtlichen Normen wie beispielsweise dem Bayerischen Hochschulinnovationsgesetz (**BayHIG**) oder aber auch dem Bayerischen Beamtengesetz (**BayBG**) zu achten.

→ **Grundsatz:** Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten. Sie ist nur dann zulässig, wenn für die konkrete Verarbeitung eine Rechtsgrundlage[1] gegeben ist.

1. Personenbezogenes Datum als das zentrale Schutzobjekt der DSGVO

Immer dann, wenn es sich um **personenbezogene Daten** handelt, sind datenschutzrechtliche Vorschriften zu beachten. Nach der Legaldefinition sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen[2].

Dem Begriff des personenbezogenen Datums liegt somit ein sehr weites Verständnis zugrunde. **Personenbezogene Daten** sind all jene Informationen, die sich auf eine lebende natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben.

Personenbezogene Daten sind also bspw. Name, Anschrift, Geburtsdatum, Foto, Beruf oder der Familienstand. Auf die Art und Weise der Darstellung der soeben genannten Informationen kommt es nicht an. Umfasst sind insoweit alle Informationen, egal ob diese in Form von Sprache, Schrift, Zeichen, Bild oder Ton, digital oder analog dargestellt werden.

→ Bei der Angabe des/der Leiters/in der Abteilung XY handelt es sich um eine bereits identifizierte Person.

Für das Vorliegen eines personenbezogenen Datums ist es aber nicht erforderlich, dass die Identität der betroffenen Person unmittelbar aus der Information selbst folgt. Alternativ genügt es, wenn die betroffene Person zumindest „identifizierbar" ist, d.h. wenn die Information jedenfalls mit Hilfe von Zusatzwissen genügt, um sie einer konkreten Person zuzuordnen.

[1] Art. 6 Abs. 1 S. 1 lit. a – f DSGVO
[2] Art. 4 Nr. 1 DSGVO

→ Eine Person ist identifizierbar, wenn Informationen sich durch Nutzung von (Hilfs-) Mitteln einer Person zuordnen lassen.
Beispiel: der/die Mitarbeiter/in mit der Personalnummer XY, der/die Studierende mit der Matrikelnummer XY.

Geschützt sind nur solche Daten, die sich auf eine **lebende, natürliche Person** beziehen. Die DSGVO nennt diese „betroffene Personen" oder „Betroffene". Bereits verstorbene Personen genießen zwar auch nach ihrem Ableben noch Persönlichkeitsschutz, nach den Vorschriften der DSGVO handelt es sich jedoch bei den Daten Verstorbener grundsätzlich nicht um personenbezogene Daten.

Auch juristische Personen (bspw. eine GmbH) werden grundsätzlich nicht vom Schutzbereich der DSGVO umfasst.

→ Eine Ausnahme besteht hier wiederum dann, wenn bspw. über die Angabe der Firma (des Firmennamens) der Bezug zu einer natürlichen Person hergestellt wird, Beispiel: „Max Mustermann-GmbH".

An den einzelnen Einrichtungen/Instituten/Lehrstühlen einer Universität werden eine Vielzahl personenbezogener Daten verarbeitet, Beispiele hierfür sind:

- Originalklausuren von Studierenden
- Andere Prüfungsleistungen wie bspw. Hausarbeiten
- Notenlisten
- Teilnehmerlisten von (Lehr-)Veranstaltungen
- Matrikelnummern
- Adresslisten
- Geburtstagslisten
- Urlaubs-/Abwesenheitskalender
- Dienstreisedokumente
- persönliche Briefe

→ **Vorsicht:** Matrikelnummern ermöglichen die Identifizierbarkeit Studierender! Daher stellt auch die Matrikelnummer ein personenbezogenes Datum dar und unterfällt datenschutzrechtlichen Anforderungen.

2.

Abgrenzung personenbezogener Daten von reinen Sachdaten

Sachdaten beziehen sich ausschließlich auf eine Sache, eine Identifizierbarkeit von Personen ist nicht gegeben. Sachdaten sind demnach keine personenbezogenen Daten und unterfallen somit auch nicht den datenschutzrechtlichen Regelungen.

→ Beispiele für Sachdaten sind die Angabe der Projektlaufzeit oder eines Veranstaltungstitels. Bei der Angabe eines Projekttitels (Akronyms) handelt es sich in der Regel ebenfalls um ein Sachdatum.
Vorsicht ist allerdings dann geboten, wenn für die Bildung des Akronyms Namenskürzel verwendet werden, da hierdurch wiederum ein Personenbezug hergestellt werden kann.

Auch wenn keine datenschutzrechtlichen Vorschriften im Bereich der Sachdaten zu berücksichtigen sind, sind dennoch etwaig getroffene Vertraulichkeitsregelungen (bspw. getroffene Geheimhaltungsklausel über Projektinhalte, Inhalte externer Abschlussarbeiten Studierender) unbedingt einzuhalten.

Besondere Kategorien personenbezogener Daten – sog. „sensible Daten"

3. Von dem Begriff der personenbezogenen Daten sind zudem besondere Kategorien personenbezogener Daten („sensible Daten") zu unterscheiden. Die sog. „sensiblen Daten" weisen eine im Vergleich zu den rein personenbezogenen Daten gesteigerte Schutzbedürftigkeit vor Missbrauch auf.

Die Verarbeitung personenbezogener 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 ist grundsätzlich untersagt[3].

→ Beispiel für genetische Daten: DNA-Analysen; Beispiele für biometrische Daten: Gesichtsbilder oder Fingerabdrücke; Beispiel für Gesundheitsdaten: ärztliches Attest.

An eine rechtmäßige Verarbeitung sensibler Daten stellt die DSGVO also nochmals strengere Anforderungen[4].

→ Eine Verarbeitung sensibler Daten ist ausnahmsweise dann zulässig, wenn deren Verarbeitung für die Erfüllung arbeitsrechtlicher Pflichten erforderlich ist.[5] Denkbar ist demnach eine Verarbeitung von Gesundheitsdaten (bspw. Erfassen von Krankheitstagen), damit der/die Verantwortliche die ihm/ihr aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte und Pflichten nachkommen kann.

4.

Zentrale Grundsätze der DSGVO

„Datenschutz geht jeden an!"

Die DSGVO selbst benennt die bei der Verarbeitung personenbezogener Daten zu beachtenden Grundsätze[6]. Hiernach gilt Folgendes:

1) **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz**
   Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

[3] Art. 9 Abs. 1 DSGVO
[4] Art. 9 Abse. 2 und 3 DSGVO
[5] Art. 9 Abs. 2 lit. b DSGVO
[6] Art. 5 DSGVO

Rechtmäßigkeit bedeutet, dass für die konkrete Verarbeitung personenbezogener Daten immer eine entsprechende Rechtsgrundlage erforderlich ist. Kann die Verarbeitung nicht auf eine Rechtsgrundlage gestützt werden, liegt keine rechtmäßige Datenverarbeitung vor. Die Verarbeitung personenbezogener Daten ist in diesem Fall verboten und somit zu unterlassen.

Nähere Ausführungen, insbesondere einzelne Rechtsgrundlagen für eine rechtmäßige Datenverarbeitung, finden Sie ab Seite 8 sowie anhand von Einzelbeispielen in Teil III. FAQ.

Die Verarbeitung personenbezogener Daten nach Treu und Glauben fordert eine „faire" Datenverarbeitung. Hierdurch soll gewährleistet werden, dass dem/der Betroffenen durch die Verarbeitung seiner/ihrer personenbezogenen Daten keine Nachteile entstehen.

Die Verarbeitung personenbezogener Daten in transparenter Form verlangt, dass der/die Betroffene im konkreten Einzelfall über den Umstand und den Umfang der Verarbeitung Kenntnis hat. Die hierfür erforderlichen Informationen müssen leicht zugänglich, verständlich und in klarer und einfacher Sprache abgefasst sein.

2) Zweckbindung der Datenverarbeitung

Personenbezogene Daten müssen für (bereits zum Zeitpunkt der Erhebung) festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Tritt nachträglich eine Zweckänderung ein, also die Verarbeitung personenbezogener Daten zu anderen Zwecken als denjenigen, zu welchen die Daten ursprünglich erhoben wurden, ist eine Verarbeitung grundsätzlich unzulässig. Etwas anderes gilt nur dann, wenn gesetzlich normierte Ausnahmefälle vorliegen.[7]

3) Datenminimierung

Personenbezogene Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

4) Sachliche Richtigkeit der Daten

Personenbezogene Daten müssen sachlich richtig und (erforderlichenfalls) auf dem neuesten Stand sein. Unrichtige Daten sind unverzüglich zu löschen oder jedenfalls zu berichtigen.

5) Zeitliche Begrenzung der Speicherdauer

Personenbezogene Daten müssen in einer Form gespeichert werden, die eine Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Danach ist eine auf das unbedingt erforderliche Maß begrenzte Speicherfrist zu definieren. Des Weiteren müssen Fristen für die Löschung oder jedenfalls für die regelmäßige Überprüfung der personenbezogenen Daten festgelegt werden. Für die Festlegung von

[7] Art. 6 Abs. 4 DSGVO: Einwilligung; qualifizierte Rechtsvorschrift der Union oder der Mitgliedstaaten oder Vereinbarkeit mit dem ursprünglichen Zweck

Überprüfungs- sowie Löschfristen sind gesetzliche Aufbewahrungs- und/oder Archivierungspflichten zu beachten.

6) **Integrität und Vertraulichkeit – Schutz vor unberechtigter Verarbeitung**
Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Insbesondere müssen diese vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust geschützt werden. Dies ist durch entsprechende technische und organisatorische Maßnahmen sicherzustellen.

Rechtmäßigkeit der Verarbeitung personenbezogener Daten

5. Eine Verarbeitung personenbezogener Daten ohne Vorliegen der entsprechenden Rechtsgrundlage ist verboten. Nur wenn und soweit eine Rechtsgrundlage vorliegt, ist eine Verarbeitung personenbezogener Daten zulässig. Die DSGVO selbst nennt eine abschließende Liste von Rechtsgrundlagen für eine Datenverarbeitung[8].

Im universitären Kontext kommen dabei vor allem folgende Rechtsgrundlagen in Betracht:

- **Die Verarbeitung personenbezogener Daten zur Aufgabenerfüllung[9]**
Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Nach dem Bayerischen Hochschulgesetz obliegt den staatlichen Hochschulen (Universitäten) die Aufgabe, u.a. Wissenschaft, Forschung, Lehre und Studium durchzuführen und zu fördern. Soweit demnach personenbezogene Daten von z.B. Studierenden zum Zwecke der Lehre/des Studiums verarbeitet werden, kann die Rechtsgrundlage der Verarbeitung in der Erfüllung der den Hochschulen nach dem Bayerischen Hochschulgesetz zugewiesenen Aufgaben zu finden sein.

  Dabei kann das Tatbestandsmerkmal der „Aufgabe, die im öffentlichen Interesse liegt“ weit verstanden werden, so dass die Verarbeitung personenbezogener Daten zur Wahrnehmung einer Aufgabe im öffentlichen Interesse auch eine solche Datenverarbeitung mit einschließt, die für die Verwaltung und das Funktionieren der Organe und Einrichtungen und damit auch der Universitäten erforderlich ist[10]. Dieses weite Verständnis bedeutet, dass hiervon nicht nur die Erfüllung der eigentlichen Kernaufgabe erfasst ist, sondern auch die Erfüllung von den die Kernaufgaben unterstützenden, gewissermaßen vorgelagerten Aufgaben ebenfalls von dieser Rechtsgrundlage mitumfasst sein können.

  Im konkreten Fall hat eine sorgfältige Prüfung zu erfolgen, ob es sich 1. um eine Datenverarbeitung in Aufgabenerfüllung handelt, die im öffentlichen Interesse liegt und 2. die jeweils konkret zu erfüllende Aufgabe noch unter dieses Tatbestandsmerkmal subsumiert werden kann.

---

[8] Art. 6 (und 9) DSGVO
[9] Art. 6 Abs. 1 S.1 lit. e DSGVO
[10] Vgl. 844/14/EN WP 217, Artikel-29-Datenschutzgruppe, Stellungnahme 06/2014, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/WP217_Opinion62014LegitimateInterest.html

Darüber hinaus kommt das ebenfalls zu beachtende **Kriterium der Erforderlichkeit** hinzu[11]. Hiernach ist eine Verarbeitung personenbezogener Daten durch eine öffentliche Stelle (unbeschadet sonstiger Bestimmungen) zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist. Nicht jede Tätigkeit, die in Aufgabenerfüllung vorgenommen wird, ist auch erforderlich um diese Aufgabe tatsächlich zu erfüllen.

→ Beispiel: Berichterstattung über Personen von öffentlichem Interesse (bspw. Redner auf Veranstaltungen) durch Hochschulen, da hierdurch die Öffentlichkeitsarbeit als eine der weiteren, nach dem Bayerischen Hochschulgesetz zugewiesenen, Aufgaben der Universitäten erfüllt wird.

So umschreibt beispielsweise die Öffentlichkeitsarbeit ein weites, schier unbegrenztes Spektrum an Möglichkeiten zur Unterrichtung der Öffentlichkeit. Nicht jede dieser Möglichkeiten ist allerdings auch tatsächlich erforderlich um die Aufgabe der Öffentlichkeitsarbeit zu erfüllen. So kann es z.B. erforderlich zur Erfüllung der Aufgabe „Öffentlichkeitsarbeit" sein, Redner, hervorgehobene Funktionsträger oder Ehrengäste auf universitären Veranstaltungen zu fotografieren. Nicht erforderlich allerdings erscheint ein „systematisches Abfotografieren" aller anwesenden Veranstaltungsteilnehmer[12]. Denn das systematische Abfotografieren aller Veranstaltungsteilnehmer stellt zwar ein geeignetes Mittel zur Information der Öffentlichkeit dar, allerdings ist ein solches Vorgehen über das angemessene, d.h. gebotene, Maß hinaus gerade nicht erforderlich.

→ Im Rahmen der Erforderlichkeit ist zu prüfen, ob eine (Verarbeitungs-)Maßnahme zur Erfüllung der Aufgabe objektiv geeignet und angemessen ist.

- **Die Verarbeitung personenbezogener Daten zur Erfüllung eines Vertrages[13]**
  Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrages mit der betroffenen Person oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist.

→ Beispiel: Die Verarbeitung von Kontaktdaten und/oder Zahlungsdaten im Rahmen der Durchführung eines Werkvertrages aufgrund dieser Rechtsgrundlage ist zulässig.

- **Die Verarbeitung personenbezogener Daten aufgrund einer erteilten Einwilligung des/der Betroffenen[14]**
  Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere vorab bestimmte Zwecke gegeben hat.

→ Beispiel: Einwilligung des/der Betroffenen in die Anfertigung von Ton- und Bildaufnahmen im Rahmen studentischer Pflichtveranstaltungen unter gleichzeitiger Bereitstellung eines aufnahmefreien Bereichs.

[11] Art. 6 Abs. 1 S. 1 lit. e DSGVO, Art. 4 Abs. 1 BayDSG
[12] https://www.datenschutz-bayern.de/datenschutzreform2018/aki16.html
[13] Art. 6 Abs. 1 S.1 lit. b DSGVO
[14] Art. 6 Abs. 1 S.1 lit. a DSGVO

Für das Verhältnis der Rechtsgrundlagen zueinander gilt allgemein:

→ Nur wenn **keine andere Rechtsgrundlage** für die Datenverarbeitung in Betracht kommt, kann eine Einwilligung des Betroffenen in die Verarbeitung seiner personenbezogenen Daten als Rechtsgrundlage dienen!

Nach der Legaldefinition ist eine Einwilligung der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.[15]

→ Eine wirksame Einwilligung des Betroffenen liegt also dann vor, wenn diese
- Freiwillig (freie Wahl ohne Nachteile befürchten zu müssen)
- Informiert (mindestens Kenntnis der Datenverarbeitung und deren Umfang)
- Bezogen auf einen bestimmten Zweck
- Bezogen auf eine bestimmte Verarbeitung (keine Blanko-Einwilligung)
- Und in unmissverständlicher Weise (eindeutige bestätigende Handlung)

erteilt worden ist.

Eine Einwilligung kann von der betroffenen Person jederzeit widerrufen werden. Ein erfolgter Widerruf der Einwilligung hat keine Auswirkung auf die bis zum Widerruf erfolgte Verarbeitung, sondern wirkt nur für die Zukunft.[16]

Als weitere Rechtsgrundlagen für eine rechtmäßige Datenverarbeitung kommen daneben grundsätzlich ebenfalls in Betracht:

- Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt[17]
- Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person [18]
- Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten.[19]

Eine rechtmäßige Datenverarbeitung durch Hochschulen zur Wahrung eigener, berechtigter Interessen hat von vorneherein auszuscheiden.

Eine Verarbeitung personenbezogener Daten zur Wahrung der berechtigten Interessen des Verantwortlichen (gemäß Art. 6 Absatz 1 Satz 1 lit. f DSGVO) gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung[20]. Der Anwendungsbereich dieser Rechtsgrundlage ist eng zu verstehen, sodass es den Behörden hiernach gänzlich verwehrt ist, sich auf ein berechtigtes Interesse als Grundlage für eine rechtmäßige Datenverarbeitung zu berufen. Es gilt der allgemeine Grundsatz, wonach Behörden personenbezogene Daten im Regelfall nur dann in Erfüllung ihrer Aufgaben verarbeiten sollen, wenn sie von Rechts wegen entsprechend befugt sind. Denn insoweit obliegt es dem Gesetzgeber durch Rechtsvorschrift

[15] Art. 4 Nr. 11 DSGVO
[16] https://www.datenschutz-bayern.de/datenschutzreform2018/einwilligung.pdf
[17] Art. 6 Abs. 1 S.1 lit. c DSGVO
[18] Art. 6 Abs. 1 S.1 lit. d DSGVO
[19] Art. 6 Abs. 1 S.1 lit. f DSGVO
[20] Art. 6 Abs. 1 S. 2 DSGVO

die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen[21].

Universitäten dürfen demnach nur dann rechtmäßiger Weise personenbezogene Daten verarbeiten, wenn dies in Erfüllung einer Aufgabe geschieht, die im öffentlichen Interesse liegt und die den Universitäten durch Rechtsvorschrift zugewiesen ist, wie dies beispielsweise durch Art. 2 Bayerisches Hochschulgesetz geregelt ist.

Datenverarbeitung

Die Verarbeitung erfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang, auf den Einsatz von EDV kommt es also nicht an. Ausreichend ist es, soweit von einem
6. geordneten Ablagesystem ausgegangen werden kann.

→ Ein geordnetes Ablagesystem liegt bereits dann vor, wenn Sie Unterlagen auch in Papierform bspw. alphabetisch oder nach Eingangsdatum vorsortieren.

Der Begriff der Verarbeitung personenbezogener Daten ist weit zu verstehen und umfasst u.a. das/die

- Erheben und Erfassen *(bspw. Einsammeln von Originalklausuren)*
- Organisation und Ordnen *(bspw. Alphabetische Vorsortierung)*
- Speichern *(bspw. Noteneintrag in HISQIS)*
- Anpassung oder Veränderung *(bspw. Notenkorrektur in HISQIS)*
- Auslesen und Abfragen
- Verwendung *(bspw. Nutzung von bestehenden Adressdaten)*
- Offenlegung durch Übermittlung, Verbreitung und sonstige Bereitstellung *(bspw. Ausspielen auf Internetseiten)*
- Abgleich und Verknüpfung
- Einschränkung
- Löschen und Vernichten *(Aufbewahrungs-, Archivierungspflichten beachten!)*

personenbezogener Daten.

[21] DSGVO, Erwägungsgrund 47

Datenschutzgerechter Arbeitsplatz

Die Gewährleistung des Schutzes personenbezogener Daten, insbesondere vor einer unberechtigten Kenntnisnahme durch Dritte, erfordert die Umsetzung datenschutzrechtlicher Anforderungen in der täglichen Arbeitspraxis.

II. Was Sie an Ihrem Arbeitsplatz beachten sollten

Oberstes Gebot ist der Schutz personenbezogener Daten vor einer unberechtigten Kenntnisnahme durch Dritte. Unter Berücksichtigung der vorstehenden Grundsätze gelten nachfolgende Handlungsgebote.

1. Umgang mit Dokumenten in Papierform

- 1.1 Unterlagen mit personenbezogenen Daten dürfen für Unberechtigte nicht zugänglich sein. Wenn Sie also mit Dokumenten in Papierform arbeiten, dürfen die darin enthaltenen personenbezogenen Daten nicht für Unberechtigte offen einsehbar sein. Beispielsweise Umlaufmappen aber auch Aktenordner dürfen nicht mit personenbezogenen Daten beschriftet sein. Vielmehr sind diese mit Aktenzeichen zu versehen.
- Insbesondere Akten zu Personal- oder Studierendenangelegenheiten sowie Prüfungsakten müssen in verschlossenen Schränken aufbewahrt werden. Nur Sie, ggf. weitere Zugriffsberechtigte wie Ihr/e Vorgesetzte/r, dürfen hierfür einen Schlüssel haben. Der Zugriff auf Papierakten muss kontrolliert sowie nachvollzogen werden können.
- Achten Sie bei Ausdrucken oder Faxempfängen darauf, den Ausdruck sofort an sich zu nehmen. Bei der Geräteauswahl ist insbesondere auf die Auswahl des richtigen Druckers zu achten. Dies gilt vor allem dann, wenn sich das Gerät nicht an Ihrem Arbeitsplatz befindet.
- Fordern Sie andere niemals dazu auf, Unterlagen mit personenbezogenen Daten an einem für Unberechtigte frei zugänglichen Ort abzulegen. Beispielsweise sollten Sie Studierende nicht dazu auffordern, Hausarbeiten in einer unverschlossenen Box vor dem Büro abzulegen. Der Schutz personenbezogener Daten vor dem Zugriff unberechtigter Dritter kann insoweit nicht gewährleistet werden.
- Gleiches gilt für das Versenden von Unterlagen, welche personenbezogenen Daten enthalten. Auch diese sind stets in verschlossenen Umschlägen zu versenden, da diese nur hierdurch vor dem Zugriff unberechtigter Dritter geschützt werden können.
- 1.2 Unterlagen in Papierform, insbesondere Klausuren und andere Prüfungsleistungen, sind der Registratur/dem Archivar zur Archivierung anzubieten, wenn deren Verarbeitung vor Ort nicht mehr erforderlich ist

Arbeiten am PC-Arbeitsplatz

- Stellen Sie Ihren PC-Bildschirm so auf, dass der Inhalt Ihres Bildschirms für Dritte/Besucher weder lesbar noch einsehbar ist.
- Dienstliche Arbeiten sind nicht lokal (d.h. nicht auf dem Desktop), sondern auf einem Netzlaufwerk abzuspeichern.
- Sichern Sie den Zugriff auf Ihren PC mittels der Verwendung einer Passwortabfrage ab und teilen Sie Ihre Passwörter nicht mit anderen. Insbesondere sollten Sie Ihre Log-In-Daten

nicht mit Dritten (auch nicht mit Kollegen/innen) teilen oder diese an einem für Dritte frei zugänglichen Ort aufbewahren.

- Personenbezogene Daten auf Notebooks oder anderen mobilen Datenträgern wie USB-Sticks sind zu verschlüsseln,
- Für den Versand von E-Mails gilt es, die eingegebenen E-Mail-Adressen vor dem Versand auf deren Korrektheit zu überprüfen. Dies ist notwendig, um Fehlauswahlen bedingt durch etwaige von dem verwendeten E-Mail-Programm vorgeschlagene Kontakte zu vermeiden.
- Für den Versand von Rundmails gilt es zu prüfen, ob es erforderlich ist, dass jede/r einzelne Empfänger/in sehen kann, an welchen Empfängerkreis die E-Mail adressiert ist. Soweit dies nicht erforderlich ist, sind die Empfänger/innen im Bcc-Feld einzutragen. Hintergrund ist, dass sich aus dem Empfängerkreis von Rundmails Rückschlüsse auf personenbezogene Daten ziehen lassen. Beachten Sie für den Versand von Rundmails an Beschäftigte folgende **Richtlinien zum Versand digitaler Rundschreiben an der Universität Passau**; verwenden Sie für den Versand von Rundmails folgenden **Antrag auf Versand einer Rund-Mail**.
- Personenbezogene Daten sind niemals per E-Mail an Dritte zu versenden. Dies gilt vor allem für besonders schützenswerte personenbezogene Daten („sensible Daten“) oder aber auch für den Versand großer Mengen personenbezogener Daten. So sollten keinesfalls Teilnehmerlisten zu Lehrveranstaltungen oder Notenlisten über Prüfungsleistungen per E-Mail versandt werden. Dies gilt grundsätzlich auch für den universitätsinternen E-Mail-Versand. Entsprechend sollten Sie andere niemals dazu auffordern, E-Mails mit personenbezogenen Daten an Sie zu übersenden. Grund hierfür ist, dass ein sicherer Umgang mit personenbezogenen Daten sowie deren Schutz vor Verlust oder einer unberechtigten Kenntnisnahme durch die Bereitstellung und Verwendung sicherer Kommunikationswege gewährleistet werden muss.
- Stellen Sie keine automatische Weiterleitung Ihrer Dienst-E-Mails auf ein privates E-Mail-Konto ein, wenn Sie den Empfang von personenbezogenen Daten nicht ausschließen können.

→ Stattdessen sind sichere Cloud-Dienste wie z.B. Filr, Vibe, Sync+Share zu nutzen. (**ZIM, Online-Zugriff auf Ihre Laufwerke**; **LRZ Sync+Share**)

1.3.

Umgang mit personenbezogenen Daten am Telefon

- Geben Sie am Telefon keine Auskünfte, wenn Sie den/die Anrufer/in nicht zweifelsfrei identifizieren können. Prüfen Sie vor der Weitergabe personenbezogener Daten, ob Sie zur Auskunft berechtigt sind, d.h. ob die für die Weitergabe personenbezogener Daten erforderliche Rechtsgrundlage vorliegt.
- Unberechtigte sollen keine Kenntnis von dem Inhalt des Telefonats nehmen können.
- Bei der Frage nach abwesenden Mitarbeitern/innen darf der Grund der Abwesenheit (Krankheit/ Urlaub) nicht genannt werden, lediglich wann diese/r voraussichtlich wieder zu erreichen sein wird.

1.4.

Was Sie beachten sollten, wenn Sie Ihr Büro verlassen

- Schließen Sie Ihr Büro auch dann ab, wenn Sie es nur kurz verlassen und lassen Sie fremde Personen nie alleine in Ihrem Büro.
- Verwenden Sie an Ihrem PC die Bildschirmsperre oder schalten Sie diesen ganz aus.

– Unterlagen mit personenbezogenen Daten (dies gilt auch für digitale Datenträger wie USB-Sticks) sind in einem verschlossenen Behältnis aufzubewahren. Der Zugang zu/Zugriff auf Datenträger mit personenbezogenen Daten ist zu sichern.

Verarbeitung personenbezogener Daten mittels privater EDV-Geräte

– Der Zugriff auf dienstliche Dokumente mittels privater EDV-Geräte (Laptop, Smartphone etc.) ist auf datenschutzrechtlich unbedenkliche Tätigkeiten und unter dem Aspekt der Geheimhaltung zu beschränken.

– Sämtliche Cloud-Dienste (z.B. Dropbox) sowie Messenger-Dienste (z.B. Skype) sind aus datenschutzrechtlicher Sicht hoch kritisch und daher für den Austausch personenbezogener Daten nicht zulässig.
Hintergrund hierfür ist, dass durch das Verwenden von bspw. Dropbox personenbezogene Daten in fremde Hände gegeben werden und somit die Einhaltung datenschutzrechtlicher Anforderungen nicht mehr gänzlich gewährleistet werden kann. Zudem liegt eine Auftragsdatenverarbeitung vor, welche ohne den Abschluss eines entsprechenden Vertrages zur Auftragsdatenverarbeitung nicht zulässig ist.

→ Stattdessen sind sichere Cloud-Dienste wie z.B. Filr, Vibe, Sync+Share zu nutzen (**ZIM, Online-Zugriff auf Ihre Laufwerke**; **LRZ Sync+Share**).
Als Alternative zu Skype kommt der **Webkonferenzdienst des DFN** in Betracht.

1.6. Datenschutzkonforme Entsorgung von Papier und Datenträgern

– Personenbezogene Daten sind nur solange aufzubewahren/zu speichern, wie diese zur Aufgabenerfüllung benötigt werden. Sobald der Zweck der Datenverarbeitung erfüllt ist und keine gesetzlichen Aufbewahrungs- und/oder Archivierungspflichten mehr greifen, sind die personenbezogenen Daten zu löschen/vernichten.

– Eine dauerhafte Speicherung personenbezogener Daten ist unzulässig. Dem steht der Grundsatz der zeitlichen Speicherbegrenzung entgegen.

– Vor einer Entsorgung bzw. Löschung sämtlicher Unterlagen, gleich ob in Papier- oder digitaler Form, sind also Aufbewahrungs- und Archivierungspflichten zu prüfen!

– Eine datenschutzgerechte Entsorgung von Papiergut hat gemäß der **Dienstanweisung für den Geschäftsgang** zu erfolgen (Stichwort: „Schreddern“); die Abholung des Entsorgungsguts erfolgt je nach Abgabemenge durch die Hauspost/Hausmeister.

– Für die Entsorgung sonstiger, digitaler Datenträger ist das Formular zur **Rückgabe und Verschrottung von Geräten** auszufüllen und direkt an den ZIM-Support zu versenden.

Zusammenfassung

- Nur wenn für den konkreten Fall der Datenverarbeitung eine Rechtsgrundlage gegeben ist, ist die Verarbeitung personenbezogener Daten rechtmäßig.
- Hochschulmitarbeiter/innen dürfen nur dann Zugriff auf personenbezogene Daten haben, **wenn, soweit und solange** sie diese Daten zur Erfüllung ihrer Aufgaben benötigen.

2.

- Die erforderlichen **Zugangs- und Zugriffskontrollen sind einzuhalten,** dies gilt grundsätzlich unabhängig davon, ob personenbezogene Daten auf Papier, auf dem PC oder anderen digitalen Medien gespeichert sind.
- Die **Dienstanweisung für den Geschäftsgang** an der Universität Passau ist zu beachten.
- Schriftgut zur Archivierung anbieten (Kontakt: **Referat IX/5 - Archiv, Dokumentation, Registratur**).
- Bei Auskunftsanfragen von Betroffenen oder etwaigen Datenpannen hat eine unverzügliche Meldung an die Datenschutzbeauftragte (**datenschutz@uni-passau.de**) zu erfolgen.

FAQ

Im universitären Kontext finden vielfältige Verarbeitungen personenbezogener Daten statt. Erfasst hiervon sind u. a. der Umgang mit personenbezogenen Daten Studierender sowie Beschäftigter, das Führen von Noten-, Teilnehmer- oder Adresslisten, die Planung und Durchführung von Veranstaltungen (Lehrveranstaltungen aber auch Veranstaltungen unter Teilnahme Externer) sowie die Erstellung von Foto- oder sonstigen Aufnahmen bei Veranstaltungen oder aber auch das Einladungsmanagement im Vorfeld von Veranstaltungen.

III.

Was ist bei der Verarbeitung personenbezogener Daten stets zu beachten?

Für die Verarbeitung personenbezogener Daten gilt es folgende allgemein gültige Grundlagen zu beachten:

1.

1.1. Auf welcher Rechtsgrundlage werden personenbezogene Daten verarbeitet?

Werden personenbezogene Daten erhoben oder anderweitig verarbeitet, ist stets das Vorliegen einer Rechtsgrundlage für die Datenverarbeitung zu prüfen. Als für den Hochschulkontext typische Rechtsgrundlagen für die Datenverarbeitung kommen dabei die Verarbeitung zur Aufgabenwahrnehmung[22], die Verarbeitung zur Vertragserfüllung[23], oder – wenn keine andere Rechtsgrundlage ersichtlich ist – die Verarbeitung aufgrund einer erteilten Einwilligung der betroffenen Person[24] in Betracht[25]. Die Verarbeitung personenbezogener Daten aufgrund einer Einwilligung ist somit nachrangig zu den soeben benannten Rechtsgrundlagen heranzuziehen. Im Rahmen der Einholung einer Einwilligung ist stets zu gewährleisten, dass die Voraussetzungen für eine wirksame Einwilligung tatsächlich vorliegen.[26]

→ Beachten Sie hierzu unbedingt die Ausführungen zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten auf den Seiten 8 bis 11 dieses Leitfadens!

1.2. Erfüllung der Informationspflichten zum Zeitpunkt der Erhebung personenbezogener Daten

Bereits zum Zeitpunkt der Erhebung personenbezogener Daten ist der/die Betroffene über die konkrete Verarbeitung seiner/ihrer personenbezogenen Daten zu informieren. Eine Mitteilung pauschaler Informationen ohne konkreten Bezug zur jeweiligen Datenverarbeitung erfüllt nicht die datenschutzrechtlichen Anforderungen an die Einhaltung der Informationspflicht. Diese Informationspflicht ergibt sich unmittelbar aus den Vorschriften der DSGVO. Werden personenbezogene Daten direkt bei dem/der Betroffenen[27] erhoben, ist diese/r zu informieren über:

- die/den Verantwortliche/n für die Datenverarbeitung samt Kontaktdaten
- die/den Datenschutzbeauftragte/n des/der Verantwortlichen samt Kontaktdaten
- den Zweck und die Rechtsgrundlage der Datenverarbeitung
- ggf. die Empfänger der personenbezogenen Daten
- ggf. die Übermittlung personenbezogener Daten an ein Drittland

[22] Art. 6 Abs. 1 S.1 lit. e DSGVO
[23] Art. 6 Abs. 1 S.1 lit. b DSGVO
[24] Art. 6 Abs. 1 S.1 lit. a DSGVO
[25] Vgl. S. 8 – 11
[26] https://www.datenschutz-bayern.de/datenschutzreform2018/einwilligung.pdf
[27] Art. 13 Abs. 1 DSGVO

- die Dauer der Speicherung, oder jedenfalls die Kriterien für die Speicherdauer/ Überprüfungsfristen
- die Betroffenenrechte
- das Beschwerderecht bei einer Aufsichtsbehörde.

Zu den Betroffenenrechten zählen das Recht auf Auskunft, das Recht auf Berichtigung, das Recht auf Löschung, das Recht auf Einschränkung der Verarbeitung[28]. Basiert die Datenverarbeitung auf einer Einwilligung des/der Betroffenen steht diesem zudem ein Widerrufsrecht zu, d.h. der/die Betroffene kann seine/ihre erteilte Einwilligung in die Verarbeitung seiner/ihrer personenbezogener Daten widerrufen[29].

Werden personenbezogene Daten nicht direkt bei dem/der Betroffenen selbst erhoben, handelt es sich um eine Dritterhebung[30] (Erhebung der Daten bei einer dritten Stelle). Hierbei sind im Wesentlichen die gleichen Informationen wie im Fall einer Erhebung von Daten direkt bei der betroffenen Person zu erteilen. Darüber hinaus ist der/die Betroffene aber zudem darüber zu informieren, aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen.

→ Eine Datenerhebung findet „nicht bei der betroffenen Person" (Fall der Dritterhebung) statt, wenn die betroffene Person erkennbar weder körperlich noch mental an der Datenerhebung (aktiv oder passiv) beteiligt ist.

→ Abgrenzungsbeispiel: Bei einer Datenerhebung von einer Internetseite oder aus dem Telefonbuch, worin der/die Betroffene seine/ihre Informationen selbst eingegeben hat, handelt es sich um eine Erhebung personenbezogener Daten direkt bei der betroffenen Person, auch wenn diese an der eigentlichen Erhebung nicht (mehr) aktiv beteiligt ist.

Die DSGVO selbst nennt eine Beschränkung der Informationspflicht[31] für den Fall, dass die betroffene Person bereits über die entsprechenden Informationen verfügt. Kennt die betroffene Person die wesentlichen Informationen über die Datenverarbeitung also bereits, kann auf eine gesonderte Mitteilung der Informationen verzichtet werden. Wann ein solcher Fall vorliegt ist stets für den einzelnen Fall genauestens zu prüfen.

Gerade im universitären Kontext, wenn personenbezogene Daten bspw. zur Durchführung des Lehrbetriebs verarbeitet werden, wird den betroffenen Studierenden oftmals bereits bekannt sein, zu welchem Zweck ihre Daten verarbeitet werden. Dies ist bspw. dann der Fall, wenn Prüfungsergebnisse zum Nachweis des Bestehens oder Nichtbestehens verbucht werden, oder aber auch dann, wenn Klausuren, Hausarbeiten und andere Prüfungsleistungen mit Matrikelnummer, Namen, ggf. auch den Kontaktdaten der Studierenden versehen werden, um diese dem/der jeweiligen Studierenden zuordnen zu können.

1.3 Erfüllung der Dokumentationspflicht bei Verarbeitung personenbezogener Daten

[28] Art. 15 – 18 DSGVO
[29] Art. 7 Abs. 3 DSGVO
[30] Art. 14 Abs. 1 DSGVO
[31] Art. 13 Abs. 4 DSGVO; Art. 14 Abs. 5 lit. a) DSGVO

Findet eine Verarbeitung personenbezogener Daten statt, sind die zentralen Grundsätze der DSGVO (rechtmäßige Datenverarbeitung in transparenter Form, Zweckbindung der Datenverarbeitung, Datenminimierung, sachliche Richtigkeit der Daten, zeitliche Begrenzung der Speicherdauer, sowie Integrität und Vertraulichkeit zum Schutz der personenbezogenen Daten vor einer unberechtigten Verarbeitung[32]) zwingend einzuhalten. Die Einhaltung der zentralen Grundsätze muss nachgewiesen werden können. Insoweit folgt aus den Normen der DSGVO auch eine Dokumentationspflicht[33] über die Einhaltung der zentralen Grundsätze.

Basiert eine Datenverarbeitung bspw. auf einer erteilen Einwilligung des/der Betroffenen, so kann die Einwilligung auch mündlich erteilt werden, oder aber auch nur durch schlüssiges Verhalten, bspw. durch Überreichen einer Visitenkarte zur Kontaktaufnahme. Aus den Normen der DSGVO folgt also per se keine Pflicht, Einwilligungen in Schriftform einzuholen.

Zur Erfüllung der Dokumentationspflicht ist jedoch in schriftlicher Form festzuhalten,

- wann, wo und wie ein Kontakt hergestellt worden ist
- auf welcher Rechtsgrundlage sowie zu welchem Zweck personenbezogene Daten verarbeitet werden und
- dass dem/der Betroffenen die erforderlichen Informationen

erteilt wurden. Nur wenn eine schriftliche Dokumentation dieser Punkte vorliegt, kann die Nachweispflicht erfüllt werden.

→ Insoweit empfiehlt es sich bspw., Einwilligungen in die Datenverarbeitung in Schriftform einzuholen. Die Einhaltung der zentralen Grundsätze der DSGVO kann aber auch durch das Anfertigen eines eigenen Aktenvermerks oder mittels Fotoaufnahmen dokumentiert werden.

2. 2.1. Was ist beim Umgang mit personenbezogenen Daten von Studierenden zu beachten?

Wann liegen personenbezogene Daten Studierender vor?

Eine Verarbeitung personenbezogener Daten Studierender findet insbesondere statt bei/beim:

- Prüfungsleistungen
- Gutachten über Prüfungsleistungen
- Versand korrigierter Staatsprüfungen
- Übermittlung von Prüfungsleistungen innerhalb der Universität
- Ausstellen von Zertifikaten
- Führen von Notenlisten oder Teilnehmerlisten von Lehrveranstaltungen (dies betrifft auch Listen ehemaliger Studierender über vergangene Lehrveranstaltungen)
- Erstellen und Veröffentlichen von Foto-, Video- und sonstigen Aufnahmen von Studierenden während Lehrveranstaltungen/ Pflichtveranstaltungen

→ Zur Erinnerung: Matrikelnummern ermöglichen eine Identifizierbarkeit Studierender! Daher stellt auch die Matrikelnummer ein personenbezogenes Datum dar und somit sind bei deren Nutzung die Vorgaben der DSGVO zu beachten.

[32] Vgl. S. 6 – 8
[33] Art. 5 Abs. 2 DSGVO („Rechenschaftspflicht“)

Auf welcher Rechtsgrundlage findet eine Verarbeitung personenbezogener Daten Studierender statt?

Die Verarbeitung personenbezogener Daten Studierender bedarf einer Rechtsgrundlage. Als Rechtsgrundlage kommt insbesondere eine **Datenverarbeitung zur Aufgabenerfüllung**[34] in Betracht. Das Bayerische Hochschulgesetz weist den Universitäten u.a. die Durchführung von
25 Studium und Lehre als zentrale Aufgaben der staatlichen Hochschulen zu[35].

→ **Beachten Sie hierzu unbedingt die Ausführungen zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten auf den Seiten 8 bis 11 dieses Leitfadens!**

Nach der Regelung des Bayerischen Datenschutzgesetzes[36] ist eine Verarbeitung personenbezogener Daten durch öffentliche Stellen dann zulässig, wenn sie zur Erfüllung einer ihr obliegenden, d.h. durch Rechtsvorschriften zugewiesenen, Aufgabe erforderlich ist.

→ Die Verarbeitung personenbezogener Daten Studierender durch die Universität und deren Mitglieder ist demnach zulässig, wenn diese **zur Erfüllung einer universitären Aufgabe** auch **erforderlich** ist.

Das Bayerische Hochschulgesetz[37] weist den Universitäten im Rahmen der Betreuung Studierender insbesondere folgende Aufgaben zu:

- Die Universitäten dienen vornehmlich der Forschung und Lehre und verbinden diese zu einer vorwiegend wissenschaftsbezogenen Ausbildung
- Die Förderung besonders leistungsfähiger Studierender und des wissenschaftlichen und künstlerischen Nachwuchs
- Die wissenschaftliche Betreuung Promovierender
- Die soziale Förderung Studierender
- Zusammenwirken mit Wirtschaft und beruflicher Praxis und Förderung des Wissens- und Technologietransfer sowie der akademischen Weiterbildung
- In Zusammenarbeit mit der Wirtschaft und der Arbeitsverwaltung die Förderung des Erwerbs von Zusatzqualifikationen, die den Übergang in das Berufsleben erleichtern
- Unterrichtung der Öffentlichkeit über die Erfüllung ihrer Aufgaben.

Werden personenbezogene Daten zur Erfüllung einer der vorbenannten universitären Aufgaben verarbeitet, handelt es sich dann um eine zulässige Datenverarbeitung, wenn diese zur Aufgabenerfüllung auch erforderlich ist. Durch das Kriterium der Erforderlichkeit erfolgt also wiederum eine Begrenzung der zulässigen Datenverarbeitungstätigkeit. Nicht jede Datenverarbeitung zur Erfüllung einer öffentlichen Aufgabe ist demnach per se zulässig. Eine Erforderlichkeit wird dann ausscheiden müssen, wenn die durch Rechtsvorschrift zugewiesene Aufgabe auch ohne die Verarbeitung personenbezogener Daten zu erfüllen ist.

[34] Vgl. S. 8 – 11
[35] Art. 4 Abs. 1 BayDSG, Art. 6 Abs. 1 bis 3 DSGVO, Art. 2 Abs. 1 BayHIG
[36] Art. 4 Abs. 1 BayDSG
[37] Art. 2 BayHIG

Nachrangig zu einer Datenverarbeitung zur Erfüllung einer Aufgabe kommt als weitere Rechtsgrundlage für die Verarbeitung personenbezogener Daten Studierender die **Einwilligung des/der Betroffenen** in Betracht.

Vor allem bei studentischen Pflichtveranstaltungen, bei welchen bspw. Foto- oder Videoaufnahmen erstellt werden sollen, ist eine Einwilligung der Studierenden in die Datenverarbeitung erforderlich. Grund hierfür ist, dass den Studierenden ein Besuch von Pflichtveranstaltungen auch ohne eine gleichzeitig aufgezwungene Datenverarbeitung möglich sein muss. Insoweit ist bei der Veranstaltung ein „aufnahmefreier Bereich" bereitzustellen für den Fall, dass einzelne Studierende nicht in die Aufnahme von Fotografien und somit nicht in die Erhebung personenbezogener Daten einwilligen.

Weitere Hinweise zur Durchführung von Veranstaltungen, insbesondere zum Umgang mit Fotoaufnahmen finden Sie unter Punkt III. 4 „Was ist bei Vorbereitung und Durchführung von Veranstaltungen zu beachten?"[38]

2.3. Was ist bei der Verwendung personenbezogener Daten Studierender aus Stud.IP oder HISQIS/ HISinOne zu beachten?

Werden personenbezogene Daten Studierender aus bspw. Stud.IP verwendet, ist dies nur soweit zulässig, als diese Verarbeitung **zur Aufgabenerfüllung** auch **erforderlich** ist.

→ Beispiele: Verwenden personenbezogener Daten Studierender aus Stud.IP zur Durchführung von Lehrveranstaltungen oder für das Erstellen von Teilnehmerlisten.

2.4. Was ist bei einer Übermittlung von Prüfungsleistungen an andere Einrichtungen der Universität zu beachten?

Bei der Übermittlung von Prüfungsleistungen bspw. an das Studierendensekretariat handelt es sich ebenfalls um eine Verarbeitung personenbezogener Daten, da diese an das Studierendensekretariat weitergegeben werden. Dies ist nur soweit zulässig, als dies **zur Erfüllung** der jeweiligen Aufgaben **erforderlich** ist, bspw. also zur weiteren Bearbeitung der erzielten Prüfungsleistungen.

Das Studierendensekretariat ist dabei „Empfänger" der Daten. Denn als Empfänger von personenbezogenen Daten kommen auch Stellen innerhalb eines/r Verantwortlichen in Betracht und zwar immer dann, soweit voneinander abgrenzbare Bereiche von gewisser Eigenständigkeit vorliegen.

→ Lehrstuhlsekretariate sind vom Studierendensekretariat oder der Finanzabteilung klar abgrenzbare Einheiten. Die Mitarbeiter/innen der einzelnen Abteilungen/Einrichtungen erfüllen ihre jeweiligen Aufgaben selbständig und in kooperativer Zusammenarbeit mit den anderen Abteilungen/Einrichtungen.

[38] Vgl. S. 25 – 27

→ Insbesondere bei der Übermittlung personenbezogener Daten innerhalb der Universität ist auf deren Schutz vor einer unberechtigten Kenntnisnahme zu achten! Hierfür sind sichere Kommunikationswege zu nutzen.

Was gilt für die Bekanntgabe von Prüfungsleistungen an Studierende?

2.5.

Eine Bekanntgabe von Prüfungsleistungen mittels eines öffentlichen, d.h. frei zugänglichen, Aushangs von Notenlisten ist unzulässig. Selbst wenn die Bekanntgabe der einzelnen Prüfungsleistungen unter Zuweisung zu einer Matrikelnummer stattfindet, handelt es sich dennoch um eine Veröffentlichung personenbezogener Daten der Studierenden. Stattdessen sind hierfür wiederum sichere Kommunikationswege zu nutzen.

Was gilt für die Aufbewahrungs-/Speicherdauer gesammelter Datensätze?

2.6.

Sämtliche gesammelten Datensätze (hierzu zählt auch der Schriftverkehr via E-Mail) sowie Schriftgut in Papierform (bspw. Prüfungsakten) sind nur solange zu speichern/aufzubewahren, als dies **erforderlich** ist. Eine unbegrenzte Speicherung/Aufbewahrung personenbezogener Daten ist unzulässig, deshalb sind für den jeweiligen Fall Fristen für eine Löschung der personenbezogenen Daten zu definieren, falls dies nicht möglich ist sind jedenfalls Kriterien für eine regelmäßige Überprüfung der vorhandenen Datensätze zu definieren und einzuhalten.

Sämtliches Schriftgut ist nach Ablauf der gesetzlichen Aufbewahrungsfristen am Lehrstuhl dem Archiv über die Registratur zur Aufbewahrung anzubieten.

2.7.

Erfüllung von Informations- und Dokumentationspflichten

Wie bei allen Fällen einer Datenverarbeitung sind auch bei der Verarbeitung personenbezogener Daten Studierender die entsprechenden Informations- und Dokumentationspflichten zu erfüllen[39].

Gerade im Bereich der Verarbeitung personenbezogener Daten Studierender im Rahmen der Durchführung von Lehre und Studium zeigt sich die Herausforderung, für die Einhaltung der datenschutzrechtlichen Informationspflicht eine praktikable Lösung zu finden. In diesem Bereich findet nicht nur eine Vielzahl von Verarbeitungsvorgängen statt, gleichzeitig ist hier auch eine Großzahl an betroffenen Personen hiervon berührt. Problematisch ist insbesondere, dass vorab erteilte, pauschale Informationen nicht den Informationspflichten nach der DSGVO genügen. Die Betroffenen müssen über den konkreten Zweck der Verarbeitung ihrer personenbezogenen Daten Kenntnis haben. Wenn und soweit den betroffenen Studierenden allerdings Zweck und Inhalt einzelner Datenverarbeitungsvorgänge bereits bekannt sind, kann auf eine sonst erforderliche Mitteilung der Informationen verzichtet werden[40]. Dies gilt bspw. für das

[39] Vgl. S. 16 – 18
[40] Art. 13 Abs. 4 DSGVO

Verbuchen von Prüfungsleistungen der Studierenden zum Nachweise des Bestehens oder Nichtbestehens einzelner Lehrveranstaltungen.

Beruht eine Verarbeitung personenbezogener Daten Studierender auf deren Einwilligung, so sind diesen spätestens zum Zeitpunkt der Einwilligung die nach der DSGVO erforderlichen Informationen mitzuteilen. Liegt der Datenverarbeitung eine Einwilligung zugrunde, können die Informationen bspw. mittels eines Informationsschreibens (in digitaler und/oder analoger Form) mitgeteilt werden. Des Weiteren kommt die Möglichkeit in Betracht, den Betroffenen im Zeitpunkt der Datenerhebung lediglich die wesentlichen Grundinformationen über die Datenverarbeitung mitzuteilen und auf weiterführende Informationen zur eigenständigen Kenntnisnahme durch die Betroffenen zu verweisen (bspw. durch Verwendung eines Links auf im Internet bereitgestellte Informationen zur Datenverarbeitung).

Was gilt für die Verwaltung von Kontaktdaten?

3. Für eine zulässige Verarbeitung personenbezogener Daten in Form von Kontaktdaten mittels Kontakt-/Adresslisten oder für das Versenden von Einladungen bedarf es nach den allgemein dargelegten Grundsätzen ebenfalls einer **Rechtsgrundlage**. Darüber hinaus ist auch hier die **Informationspflicht** zu erfüllen und sämtliche Verarbeitungsvorgänge sind zu **dokumentieren**.[41]

→ Beachten Sie hierzu unbedingt die Ausführungen zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten auf den Seiten 8 bis 11 dieses Leitfadens!

3.1. Auf welcher Rechtsgrundlage findet eine Verarbeitung personenbezogener Daten mittels Kontakt- und/oder Adresslisten statt?

Als Rechtsgrundlage für eine zulässige Datenverarbeitung kommt auch hier eine Datenverarbeitung zur **Aufgabenerfüllung** in Betracht, soweit die Verarbeitung von Kontaktdaten zur Erfüllung einer universitären Aufgabe erforderlich ist[42].

Für Planung, Organisation und Durchführung von Lehrveranstaltungen kann es demnach erforderlich sein, personenbezogene Daten der Teilnehmenden in Listen zu führen, sodass diese Verarbeitungstätigkeit auf die Rechtsgrundlage der Aufgabenerfüllung gestützt werden kann.

Werden Kontaktdaten in Adresslisten für Veranstaltungen geführt, welche sich auch an externe Teilnehmende, d.h. nicht Universitätsmitglieder richtet, kommt ebenfalls die Aufgabenerfüllung als Grundlage für eine rechtmäßige und erforderliche Datenverarbeitung in Betracht. Richten sich universitäre Veranstaltungen an Akteure aus Wirtschaft und/oder Gesellschaft, so kann dies in Erfüllung der Aufgabe der Förderung des Wissens- und Technologietransfers, als

[41] Vgl. S. 8 – 11 sowie auf S. 16 – 18
[42] Art. 6 Abs. 1 S.1 lit. e DSGVO, Art. 4 Abs. 1 BayDSG

weitere den Universitäten durch das Bayerische Hochschulgesetz zugewiesene Aufgabe[43], geschehen.

Der aus DSGVO und Bayerischem Datenschutzgesetz folgende Erforderlichkeitsmaßstab[44] begrenzt wiederum den Anwendungsbereich einer rechtmäßigen Datenverarbeitung zur Aufgabenerfüllung. Eine Verarbeitung der Kontaktdaten ist demnach nur dann zulässig, wenn und soweit diese auch zur Erfüllung der (jeweiligen) Aufgabe erforderlich, d.h. objektiv geeignet und angemessen ist.

Eine Verarbeitung von Kontaktdaten kann auch dann rechtmäßig sein, wenn diese zur **Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen**[45] erforderlich ist. Hiervon umfasst ist das Erfassen von Kontaktdaten in Verträgen zu Gastvorträgen, Dozentenverträgen aber bspw. auch zur Korrekturtätigkeit, Übersetzungstätigkeit oder zur Erstellung von Gutachten.

Auch eine Datenverarbeitung im Vorfeld eines Vertragsabschlusses kann dann rechtmäßig sein, wenn diese zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, welche auf Anfrage der betroffenen Person erfolgen. Hiervon umfasst ist insbesondere die Verarbeitung personenbezogener Daten im Rahmen von Vertragsverhandlungen, nicht erforderlich ist es, dass es im Nachgang auch tatsächlich zu einem Vertragsabschluss kommt.

Kommt eine Datenverarbeitung weder unter dem Gesichtspunkt der Aufgabenerfüllung, noch zur Vertragserfüllung in Betracht, so bleibt in den meisten Fällen nur der Weg, eine **Einwilligung** der betroffenen Personen für eine rechtmäßige Datenverarbeitung einzuholen.

3.2. Auswirkungen der DSGVO auf die Verwaltung von Adresslisten, insbesondere im Hinblick auf „Altkontakte“

Für Kontakte und Kontaktdaten, die bereits vor der unmittelbaren Anwendbarkeit der DSGVO in Adresslisten geführt wurden, muss ebenfalls die Einhaltung der Dokumentationspflicht gewährleistet werden können. In vielen Fällen wird ein Nachweis darüber, auf welcher Rechtsgrundlage personenbezogene Daten verarbeitet wurden, oder auch darüber, dass die Informationspflichten bei Erhebung der Daten erfüllt wurden, mangels schriftlicher Dokumentation nicht gelingen.

Beruht die Datenverarbeitung bspw. auf einer Einwilligung des/der Betroffenen, ist zu prüfen, ob die ggf. erforderliche Einwilligung auch tatsächlich gegeben wurde.

Die Bestätigung einer bereits erteilten Einwilligung ist zwar grundsätzlich nicht erforderlich, da eine bereits erteilte Einwilligung auch weiterhin fort gilt, soweit die bereits erteilte Einwilligung den Anforderungen der DSGVO genügte. Für den Umgang mit „Altkontakten“

[43] Art. 2 Abs. 2 BayHIG
[44] Art. 4 Abs. 1 BayDSG
[45] Art. 6 Abs. 1 lit. b DSGVO

empfiehlt es sich aber dennoch, diese mit dem nächsten Anschreiben über die gespeicherten personenbezogenen Daten sowie über deren Rechte nach der DSGVO (Auskunft, Löschung etc.) zu informieren.

Was ist bei dem Versand von Einladungen und Grußkarten zu beachten?

Der Versand von Einladungen und Grußkarten, beispielsweise von Weihnachtsgrußkarten, ist ein ebenso gängiges wie beliebtes Mittel zur Pflege von bestehenden Kontakten.

3.3. Aus datenschutzrechtlicher Sicht handelt es sich bei dem Versand von (Weihnachts-) Grußkarten in der Regel jedoch um eine Verwendung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu welchem die Daten ursprünglich erhoben wurden[46]. Denn in der Regel werden personenbezogene Daten nicht ausdrücklich für den Zweck erhoben, der betroffenen Person zur Weihnachtszeit Grußkarten zuzusenden.

Somit beruht die Verwendung der personenbezogenen Daten auf einer Zweckänderung, welche nach den Normen der DSGVO[47] grundsätzlich nur dann zulässig ist, wenn diese auf einer Einwilligung der betroffenen Person, auf einer qualifizierten Rechtsvorschrift der Union oder der Mitgliedstaaten beruht, oder mit den ursprünglichen Zwecken vereinbar ist. Dieser enge Ausnahmebereich für eine dennoch zulässige Verarbeitung personenbezogener Daten trotz vorliegender Zweckänderung wird durch die Vorschriften des BayDSG[48] erweitert.

Hiernach ist eine Verarbeitung zu anderen Zwecken als zu denjenigen, zu denen die Daten erhoben wurden zulässig, wenn offensichtlich ist, dass die Verarbeitung im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung hierzu verweigern würde.

Es handelt sich also bei dem Versand von Einladungen und Grußkarten um ein gängiges, sozialadäquates Mittel der Kontaktpflege. Es ist nicht per se davon auszugehen, dass Betroffene ihre Einwilligung verweigert hätten, hätten Sie bereits bei der ersten Kontaktaufnahme gewusst, dass ihre personenbezogenen Daten auch für den Versand von Weihnachtsgrüßen verwendet werden.

Aufgrund der Verwendung personenbezogener Daten für einen anderen Zweck als für den ursprünglichen, sind den betroffenen Personen vor dieser Weiterverarbeitung Informationen über eben diesen geänderten/hinzugetretenen Zweck sowie alle sonst auch maßgeblichen Informationen zur Verfügung zu stellen[49].

> → **Beispielformulierung für den Versand von Einladungen und Grußkarten:** Ihre Adressdaten sind uns aus vorherigen Kontakten mit Ihnen bekannt. Sie werden von uns auch dazu verwendet, um Sie zu Veranstaltungen einzuladen oder Sie aus besonderem Anlass anzusprechen. Wenn Sie zukünftig keine dieser Anschreiben mehr von uns erhalten möchten, genügt eine kurze Rückmeldung (Angabe der Kontaktdaten).

[46] Art. 6 Abs. 2 BayDSG, Art. 6 Abs. 4 DSGVO
[47] Art. 6 Abs. 4 DSGVO
[48] Art. 6 Abs. 2 Nr. 1 BayDSG
[49] Art. 13 Abs. 3 DSGVO für die Direkterhebung; Art. 14 Abs. 4 DSGVO im Falle der Dritterhebung

Was ist für den Umgang mit neuen Kontakten zu beachten?

Gerade bei der Durchführung von Veranstaltungen mit externen Teilnehmern/innen (bspw. Unternehmen der Region) ist es nach wie vor üblich, Kontaktdaten für die weitere Kontaktaufnahme miteinander auszutauschen **(Überreichen von Visitenkarten).** Hierfür ist keine gesonderte schriftliche Einwilligung des/der Betroffenen erforderlich. Denn bei der Übergabe von Visitenkarten handelt es sich bereits um eine Einwilligung des/der Betroffen, da diese/r durch sein/ihr Verhalten zum Ausdruck bringt, dass er/sie eine Kontaktaufnahme im Nachgang der Veranstaltung wünscht, auch wenn dies nicht ausdrücklich so kommuniziert wird.

3.

Da es sich bei der Entgegennahme von Visitenkarten um eine Verarbeitung personenbezogener Daten handelt (Speicherung im Sinne einer Aufbewahrung sowie zumindest eine beabsichtigte Verwendung der Kontaktdaten) empfiehlt es sich, Informationen zur konkreten Verarbeitung, insbesondere über den Zweck der Datenverarbeitung, jedenfalls vorzuhalten. Dies kann durch einfache Mitteilung in mündlicher Form geschehen oder unter Verwendung eines für diesen Fall vorgefertigten Informationsblattes, welches der betroffenen Person überreicht wird. In beiden Fällen kann auf weiterführende Informationen bspw. auf dem Internetauftritt unter Bekanntgabe des entsprechenden Links verwiesen werden.

Im Anschluss an die Veranstaltung ist dieser Vorgang zu dokumentieren. Dies kann schriftlich mittels z.B. eines eigenen Aktenvermerks oder einer Eintragung in eine Datenbank/Liste darüber, wie der Kontakt im Einzelfall zustande gekommen ist, geschehen.

Für den Fall, dass man auf Veranstaltungen neue Kontakte knüpfen möchte, empfiehlt es sich eine **„Kontaktbox“** für den Einwurf bspw. von ausgefüllten Kontaktformularen oder aber auch von Visitenkarten zu verwenden. Dieser Vorgang kann bspw. durch ein Foto dokumentiert werden.

4.

Was ist bei Vorbereitung und Durchführung von Veranstaltungen zu beachten?

Sowohl im Vorfeld von Veranstaltungen als auch bei deren Durchführung werden personenbezogene Daten verarbeitet. Eine Datenverarbeitung findet bspw. bereits statt bei dem Versenden von Einladungen[50], bei der Anmeldung zu einer Veranstaltung, aber auch bei der Aufnahme von Fotografien oder von Videomaterial während Veranstaltungen handelt es sich um eine Verarbeitung personenbezogener Daten.

Eine Datenverarbeitung zur Vorbereitung und bei der Durchführung von Veranstaltungen ist nur dann zulässig, wenn hierfür eine **Rechtsgrundlage** (Verarbeitung bspw. zur Aufgabenerfüllung, zur Erfüllung eines Vertrages oder aufgrund einer Einwilligung) gegeben ist. Zudem sind wiederum die **Informationspflichten** zu erfüllen und der Vorgang der Datenverarbeitung ist zu **dokumentieren**.[51]

→ Beachten Sie hierzu unbedingt die Ausführungen zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten auf den Seiten 8 bis 11 dieses Leitfadens!

[50] Vgl. S. 22
[51] Vgl. S. 8 – 11 sowie S. 16 – 18

4.1. Vorbereitung von Veranstaltungen

Bereits im Zuge der Vorbereitung von Veranstaltungen ist vorab zu klären, um welches Veranstaltungsformat es sich handelt und vor allem, an welchen Adressatenkreis sich die jeweilige Veranstaltung richtet. Nicht nur aus datenschutzrechtlicher Sicht kommt es bei der Vorbereitung, aber auch bei der Durchführung von Veranstaltungen maßgeblich auf die soeben benannten Punkte an, d.h.: „Veranstaltung ist nicht gleich Veranstaltung".

So gelten bspw. für die Vorbereitung und Durchführung von öffentlichen Veranstaltungen, welche auch Nicht-Universitätsmitgliedern ohne oder mit vorheriger Anmeldung offen stehen und bei welchen eine Teilnahme ausschließlich freiwillig erfolgt, andere Anforderungen als für die Vorbereitung und Durchführung von studentischen Pflichtveranstaltungen.

Als Rechtsgrundlage für eine Datenverarbeitung für die Vorbereitung **studentischer Pflichtveranstaltungen** kommt wiederum die Erfüllung der aus dem BayHIG folgenden universitären Kernaufgaben (Durchführung von Studium und Lehre) in Betracht.

Richten sich **öffentliche Veranstaltungen** auch an externe Teilnehmer/innen, insbesondere an Unternehmen, so kommt eine Datenverarbeitung bspw. auf Grundlage der Förderung des Wissens- und Technologietransfers als weitere universitäre Aufgabe nach dem BayHIG[52] in Betracht.

4.2. Durchführung von Veranstaltungen – Fotoaufnahmen

Sollen bei/während einer Veranstaltung Foto-, Video- oder sonstige Aufnahmen erstellt werden, bedarf es hierfür einer Rechtsgrundlage, da hierdurch personenbezogene Daten erhoben und somit verarbeitet werden.

Insbesondere bei **studentischen Pflichtveranstaltungen** bedarf es für die Erstellung von Aufnahmen einer Einwilligung der betroffenen Studierenden, um deren personenbezogenen Daten (Abbildungen auf Foto- oder sonstigen Aufnahmen) zulässigerweise verarbeiten zu dürfen. Aus der Anwesenheitspflicht bei Lehrveranstaltungen darf nicht gleichzeitig die Pflicht folgen, Datenverarbeitungen hinnehmen zu müssen[53]. Vielmehr darf eine Verarbeitung personenbezogener Daten Studierender nur aufgrund einer freiwillig erteilten Einwilligung erfolgen. Teilnehmenden Studierenden, welche keine Aufnahmen möchten, ist ein aufnahmefreier Bereich bereitzustellen.

Aber auch bei **öffentlichen Veranstaltungen** bedarf es für die Abbildung der Teilnehmer/innen auf Foto-/Videoaufnahmen einer Rechtsgrundlage. Als mögliche Rechtsgrundlage kommt dabei die Erfüllung der Öffentlichkeitsarbeit[54], als weitere den staatlichen Hochschulen durch das BayHIG zugewiesene Aufgabe, soweit diese in Form von Bildberichterstattung auch erforderlich ist, in Betracht.[55] Dies gilt entsprechend für eine Veröffentlichung der Fotoaufnahmen im Nachgang der Veranstaltungen zur Bildberichterstattung.

Zwingend zu berücksichtigen ist insoweit, dass eine Verarbeitung personenbezogener Daten zur Öffentlichkeitsarbeit nur soweit erfolgen darf, als dies auch zur Erfüllung der

[52] Gesamtschau Art. 2 BayHIG, Art. 4 Abs. 1 BayDSG, Art. 6 Abs. 1 S.1 lit. e DSGVO
[53] oberstes Gebot ist die Freiwilligkeit einer erteilten Einwilligung, Art. 4 Nr. 11 DSGVO
[54] Gesamtschau Art. 2 BayHIG, Art. 4 Abs. 1 BayDSG, Art. 6 Abs. 1 S.1 lit. e DSGVO
[55] Weiterführende Informationen unter https://nordbild.com/info-tafeln-eventfotografie-dsgvo/

Öffentlichkeitsarbeit **erforderlich** ist. So ist es beispielsweise evtl. nicht erforderlich, eine weltweite Öffentlichkeit durch Veröffentlichung der Aufnahmen im Internet herzustellen.[56]

Soweit die Datenverarbeitung auf keine andere Rechtsgrundlage gestützt werden kann, bedarf es für Fotoaufnahmen sowie für deren anschließende Veröffentlichung einer **Einwilligung** des/der Betroffenen.

→ Bereits bei Einladung/Anmeldung zu Veranstaltungen ist auf die Erstellung sowie ggf. anschließende Veröffentlichung von bspw. Fotoaufnahmen hinzuweisen. Den Betroffenen sind die erforderlichen Informationen mitzuteilen.

→ Bei studentischen Pflichtveranstaltungen ist eine Einwilligung des/r betroffenen Studierenden in die Aufnahme von Fotografien oder Videomaterial erforderlich. Die Teilnahme an der Veranstaltung muss möglich sein, ohne gleichzeitig die Abbildung der eigenen Person auf Fotoaufnahmen hinnehmen zu müssen.

→ Bei/während Veranstaltungen ist durch Hinweisschilder auf die Erstellung und ggf. anschließende Veröffentlichung von Fotoaufnahmen hinzuweisen. Zudem empfiehlt es sich, einen „aufnahmefreien Bereich" für diejenigen Veranstaltungsteilnehmer/innen einzurichten, welche nicht abgebildet werden möchten.

→ Im Falle von Portraitfotos oder bei Videoaufnahmen ganzer Vorträge kann eine explizite Einwilligung des Betroffenen unter Angabe der beabsichtigten Verwendungszwecke (bspw. zur Veröffentlichung im Internet) erforderlich sein.
→ Unterscheidung anhand folgender Abgrenzungsfrage: „Muss der/die durchschnittliche Veranstaltungsteilnehmer/in damit rechnen, auf Fotografien abgebildet zu werden?" Für Personen von öffentlichem Interesse (bspw. Redner/in der Veranstaltung) gelten hierbei andere Maßstäbe als für bloße Teilnehmer/innen der Veranstaltung. So wird der/die Redner/in bereits vor der Veranstaltung davon ausgehen, dass er/sie während des Vortrags fotografiert werden wird um die Bilder zu veröffentlichen.

5.

Was ist beim Umgang mit personenbezogenen Daten der Beschäftigten zu beachten?

Eine Verarbeitung personenbezogener Daten Beschäftigter ist nur dann zulässig, wenn hierfür eine **Rechtsgrundlage** (Verarbeitung bspw. zur Aufgabenerfüllung, zur Erfüllung eines Vertrages oder aufgrund einer Einwilligung) gegeben ist. Zudem sind wiederum die **Informationspflichten** zu erfüllen und der Vorgang der Datenverarbeitung zu **dokumentieren**.[57]

5.1. → **Beachten Sie hierzu unbedingt die Ausführungen zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten auf den Seiten 8 bis 11 dieses Leitfadens!**

Einstellungsanträge

Bei Anträgen auf Einstellung von studentischen Hilfskräften, oder aber auch wissenschaftlichen Mitarbeitern/innen findet eine datenschutzrechtlich relevante Verarbeitungstätigkeit statt. Denn

[56] Weiterführende Informationen unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki16.html
[57] Vgl. S. 8 – 11 sowie S. 16 – 18

die Antragsformulare sind mit personenbezogenen Daten wie bspw. Namen oder Geburtsdatum zu befüllen.

Führen von Geburtstagslisten

Das Führen von Geburtstagslisten bspw. innerhalb einer Abteilung/Einrichtung bedarf der Einwilligung jedes/r einzelnen Mitarbeiters/in. Aus Gründen der Datensparsamkeit ist auf die Eintragung des Geburtsjahres zu verzichten, denn für die Überbringung der Geburtstagsglückwünsche ist das konkrete Geburtsjahr in der Regel gerade nicht erforderlich. Diese kann wie jede Einwilligung mündlich, schriftlich oder auch nur konkludent dadurch erklärt werden, dass der/die jeweilige Betroffene selbst sein/ihr Geburtsdatum in den Kalender einträgt.

5.2

Führen von internen Abwesenheitskalendern

5.3. Das Festhalten von Termin- sowie ggf. Abwesenheitsinformationen einzelner Beschäftigter in einem gemeinsam geführten Kalender stellt eine Verarbeitung personenbezogener Daten dar. Für eine zulässige Datenverarbeitung bedarf es einer Rechtsgrundlage.

Wird ein Abwesenheitskalender geführt, ist die ggf. erforderliche **Beteiligung des Personalrats zu beachten**. Umfang der Datenerhebung, Dauer der Speicherung sowie Möglichkeiten ihrer Auswertung und die zugriffsberechtigten Personen können in einer **Dienstvereinbarung** festgelegt werden.

Sollte darüber hinaus ein Abwesenheitskalender geführt werden, kann dies nur aufgrund freiwillig erteilter Einwilligungen der einzelnen Mitarbeiter/innen geschehen. Die Eintragung von Termin-/Abwesenheitszeiten muss für die Erfüllung der dienstlichen Aufgaben erforderlich sein. In jedem Fall ist sicherzustellen, dass keine personenbezogenen Daten Dritter oder vertrauliche Informationen (an unberechtigte Dritte) preisgegeben werden.

5.4.

→ Auf eine Angabe des konkreten Abwesenheitsgrundes, bspw. Urlaub, Krankheit, Fortbildungen, Dienstreisen, ist aus Gründen der Datensparsamkeit sowie zum Schutz der betroffenen Mitarbeiter/innen zu verzichten!

Veröffentlichung von Kontaktdaten

Für eine zulässige Veröffentlichung von Mitarbeiterdaten im Internet kommt es darauf an, ob deren Veröffentlichung zur Aufgabenerfüllung erforderlich ist. Bezüglich des Lehrangebots besteht ein berechtigtes Informationsinteresse Studierender. Aufgrund ihres Aufgabenbereichs müssen Lehrpersonen regelmäßig mit Dritten in Kontakt treten. Daher kann für folgende Daten eine Veröffentlichung als erforderlich angesehen werden:

- Name, akademische Grade und Titel
- Dienstliche Anschrift
- Dienstliche Telefon- und Faxnummer
- Dienstliche E-Mail

– Aufgabenbereich, insb. Bezeichnung, Art, Zeit und Ort von Lehrveranstaltungen sowie Sprechzeiten

→ Belästigungen oder Beeinträchtigungen der Arbeitssituation sind zu vermeiden, private Telefonnummern oder E-Mail-Adressen dürfen daher ohne Einwilligung des/der Betroffenen gerade nicht veröffentlicht werden.

→ Dienstliche Erreichbarkeitsdaten Beschäftigter können im Internet veröffentlicht werden, wenn und soweit diese eine herausgehobene Funktion wahrnehmen und die Veröffentlichung zur dienstlichen Aufgabenerfüllung auch erforderlich ist.

Was ist für die Dokumentation der Datenverarbeitungsvorgänge zu beachten?

6. Zur Dokumentation der stattfindenden Datenverarbeitungsvorgänge ist an der Universität Passau ein schriftliches Verarbeitungsverzeichnis zu führen[58].

Die einzelnen Datenverarbeitungsvorgänge sind hierbei mithilfe von Verfahrensbeschreibungen abzubilden, welche dann gebündelt in dem Verarbeitungsverzeichnis zusammengeführt werden.

Die Verfahrensbeschreibungen haben dabei folgende Angaben zu beinhalten:

- Namen und Kontaktdaten des/der Verantwortlichen
- Namen und Kontaktdaten des/der Datenschutzbeauftragten
- Zwecke der Verarbeitung
- Kategorien betroffener Personen der Verarbeitung
- Ggf. Übermittlung personenbezogener Daten an ein Drittland
- Fristen für die Löschung der verschiedenen Datenkategorien
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Dieses Verarbeitungsverzeichnis bildet den Rahmen zu den stattfindenden einzelnen Datenverarbeitungsvorgängen und dient dem **Nachweis** über die Einhaltung zentraler datenschutzrechtlicher Grundsätze. Weiter dient es der **Auskunft** einerseits gegenüber Aufsichtsbehörden, andererseits auch gegenüber Betroffenen u.a. darüber, welche personenbezogenen Daten auf welche Art und Weise verarbeitet werden. Das Verarbeitungsverzeichnis unterliegt der Pflicht zur fortlaufenden Aktualisierung, d.h. auch bereits gemeldete Verarbeitungstätigkeiten müssen an ggf. geänderte Verarbeitungen angepasst und diese entsprechend in der jeweiligen Verfahrensbeschreibung abgebildet werden.

Ein Verarbeitungsverzeichnis ist über sämtliche automatisierte (d.h. unter Nutzung von EDV, bspw. bei der Verarbeitung personenbezogener Daten mittels einer Excel-Liste) aber auch über sämtliche nicht automatisierte Datenverarbeitungen zu führen. Hieraus folgt, dass auch über die Verarbeitung personenbezogener Daten in Papierform eine Verfahrensbeschreibung zu erstellen ist, soweit von einer Aufbewahrung der Daten mittels eines geordneten Ablagesystems ausgegangen werden kann. Ein geordnetes Ablagesystem liegt bereits dann vor, wenn die Daten

[58] Art. 30 Abs. 1 DSGVO

(vor)sortiert und/oder geordnet, bspw. nach Eingangsdatum/Matrikelnummer/Anfangsbuchstabe, aufbewahrt werden.

> → Hier finden Sie eine Übersicht über bereits **gemeldete Verfahren** zu Datenverarbeitungsvorgängen an der Universität Passau, bspw. zu **Stud.IP, HISQIS/HISinOne** oder aber auch zu dem Forschungsinformationssystem **FIS**.

Ziel des Verarbeitungsverzeichnisses ist es, sämtliche Verarbeitungsvorgänge über die Verfahrensbeschreibungen hinreichend bestimmt, d.h. jeden einzelnen Verarbeitungsvorgang, abzubilden. Daher gilt es, soweit noch nicht geschehen, in einem ersten Schritt einen Überblick über alle Verarbeitungsvorgänge zu gewinnen.

> → Die Rückmeldung der einzelnen Verarbeitungsvorgänge kann dabei über das Formular zur **Übersicht der zur Verarbeitung personenbezogener Daten genutzten automatisierten Verfahren** erfolgen.

Im nächsten Schritt wird geprüft, inwieweit einzelne Verarbeitungsvorgänge übergreifend zusammengefasst werden können. Auf dieser Grundlage kann dann ggf. eine übergeordnete Verfahrensbeschreibung für gleichartige Verarbeitungen an mehreren Einheiten, z. B. Sekretariaten, erfolgen.

6.1. Wer ist Verfahrensverantwortlicher für die Erstellung einer Verfahrensbeschreibung?

Verantwortlich für die Erstellung einer Verfahrensbeschreibung über einen konkreten Datenverarbeitungsvorgang ist diejenige Person, die das jeweilige Verfahren der Datenverarbeitung einsetzt und auch steuert.

Wer ist Verfahrensverantwortlicher, wenn ein externer Lehrbeauftragter Lehrtätigkeit an einem Lehrstuhl ausübt?

Lehrbeauftragte werden in Erfüllung der universitären Aufgabenverpflichtung zur Lehre eingesetzt[59], die Verfahrensverantwortlichkeit verbleibt daher beim Lehrstuhl.

6.2.

[59] Art. 31 BayHSchPG

Muster

Nachfolgende Muster sollen als Formulierungshilfe dienen. Eine individuelle Anpassung für den konkreten Einzelfall ist jedoch zwingend erforderlich.

IV.

→ Bei Fragen oder Unklarheiten wenden Sie sich bitte an Ihre Ansprechpartnerinnen für datenschutzrechtliche Fragen.

Formulierungsbeispiel zur Einwilligung

1.

□ Ich stimme der Verarbeitung meiner Daten durch die Universität Passau zur [bitte Verarbeitungstätigkeit eintragen] ausdrücklich zu. Rechtsgrundlage dieser Einwilligung ist Art. 6 Abs. 1 S.1 lit. a DSGVO. Meine Daten werden verwendet zum Zweck [bitte Zweck eintragen] und werden [bitte Zeitpunkt oder festgelegte Zeiträume eintragen] gelöscht. Eine Übermittlung an [bitte Empfänger der Übermittlung eintragen] findet statt/nicht statt.

Ich wurde ausdrücklich auf meine Rechte gemäß Art. 15 DSGVO (Auskunftsrecht), Art.16 DSGVO (Recht auf Berichtigung), Art. 17 DSGVO (Recht auf Löschung) und Art. 18 (Recht auf Einschränkung der Verarbeitung) hingewiesen.

Des Weiteren kann ich diese Einwilligung jederzeit gegenüber der Universität Passau widerrufen.

→ Die Einwilligung hat in verständlicher, leicht zugänglicher Form und in einer klaren und einfachen Sprache zu erfolgen.