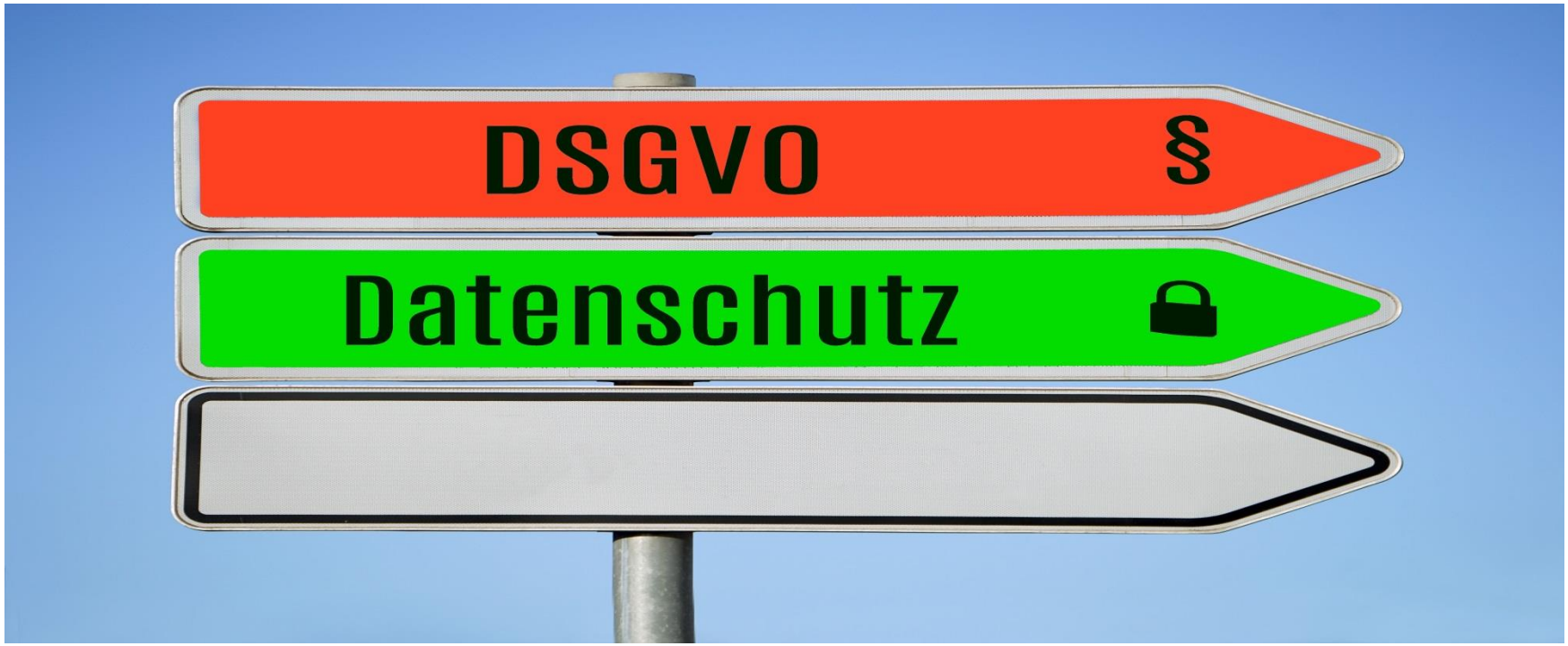
40 Jahre UNIVERSITÄT PASSAU

Informationsveranstaltung zur DSGVO



06.Dezember 2018

AGENDA

I. Personenbezogene Daten
II. Datenschutzgerechter Arbeitsplatz
III. Die einzelnen Datenverarbeitungen
IV. Verarbeitungsverzeichnis

I. Personenbezogene Daten

1. Personenbezogene Daten sind…

Informationen,

die sich auf eine

→ Name, Anschrift, Geburtsdatum, Foto, Beruf, Familienstand (ohne Rücksicht auf die Art der Darstellung)

identifizierte

oder

→ Identität folgt aufgrund von Identifikationsmerkmalen oder aus Kontext unmittelbar aus Informationen (Bsp. Der Leiter der Abteilung XY).

identifizierbare

→ Informationen lassen sich durch Nutzung von (Hilfs-) Mitteln einer Person zuordnen (Der Mitarbeiter mit der Personalnummer XY).

natürliche Person

beziehen.

→ Jede lebende Person, nicht: juristische Personen, verstorbene Personen.

Zentrales Schutzobjekt der DSGVO ist das personenbezogene Datum.

Abgrenzung personenbezogene Daten – reine Sachdaten:

- Vielzahl **personenbezogener Daten** an Einrichtungen/ Instituten/ Lehrstühlen vorhanden, z.B.:
  - Originalklausuren von Studierenden
  - Notenlisten
  - Adressverteiler
  - Geburtstagslisten
  - Urlaubskalender
  - Dienstreisedokumente
  - persönliche Briefe
  - Matrikelnummer

- **Sachdaten** sind keine personenbezogenen Daten und unterfallen demnach nicht datenschutzrechtlichen Anforderungen!
  - Entscheidend: Eine Identifizierbarkeit von Personen darf nicht gegeben sein. Es muss sich um Daten mit reinem Sachbezug handeln!
  - Beispiele für Sachdaten: Projektlaufzeit, Projekttitel (Akronym), Veranstaltungstitel
  - Im Bereich der Sachdaten sind etwaige Vertraulichkeitsregelungen einzuhalten.

2. Besondere Kategorien personenbezogener Daten – sog. „sensitive“ oder „sensible Daten“:

- Genetische Daten (Bsp.: DNS-Analysen)
- Biometrische Daten (Bsp.: Gesichtsbilder, Fingerabdrücke)
- Gesundheitsdaten (Bsp.: ärztliches Attest)
- Sonstige besonders schützenswerte Daten

3. Zentrale Grundsätze der DSGVO

„Datenschutz geht jeden an!“

Rechtmäßige Datenverarbeitung in transparenter Form

Sachliche Richtigkeit der Daten

Zweckbindung der Datenverarbeitung

Zeitliche Begrenzung der Speicherdauer

Datenminimierung – Beschränkung der personenbezogenen Daten auf das notwendige Maß

Integrität und Vertraulichkeit – Schutz vor unbefugter Verarbeitung

4. Datenverarbeitung

Umfassendes Verständnis der Datenverarbeitung, hiervon umfasst sind u.a.:

- 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!)*

Verarbeitung erfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang.

5. Rechtmäßigkeit der Verarbeitung personenbezogener Daten:

Nur wenn keine andere Rechtsgrundlage für die Datenverarbeitung in Betracht kommt, ist eine Einwilligung des Betroffenen in die Verarbeitung seiner personenbezogenen Daten einzuholen!

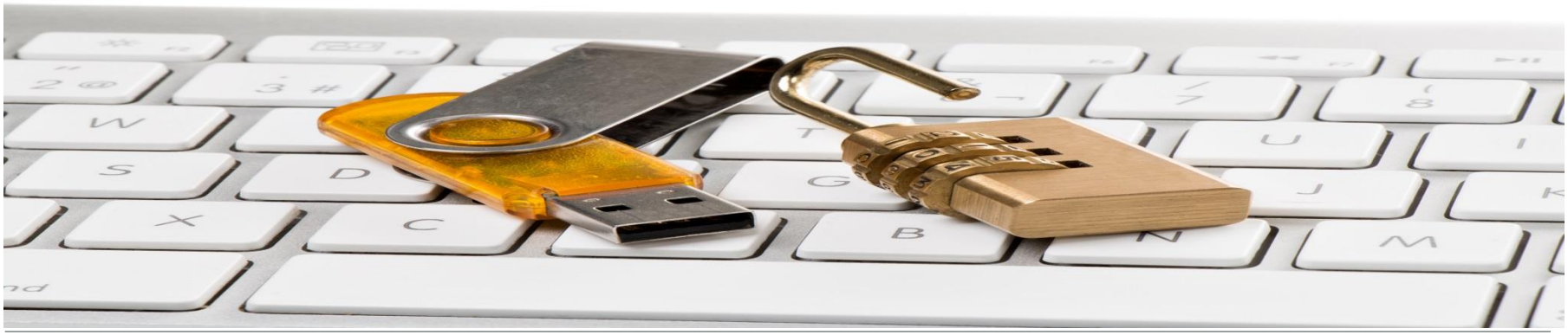
AUFGABENERFÜLLUNG IM ÖFFENTLICHEN INTERESSE
Bsp.: Berichterstattung der Presse über Person von öffentlichem Interesse

VERTRAGSERFÜLLUNG ODER VORVERTRAGLICHE MASSNAHMEN
Bsp.: Kontaktdaten, Zahlungsdaten werden im Rahmen eines Werkvertrages verarbeitet

EINWILLIGUNG DES BETROFFENEN
Bsp.: Ton- und Bildaufnahmen im Rahmen studentischer Pflichtveranstaltungen unter Bereitstellung eines aufnahmefreien Bereichs

Verarbeitung zulässig

II. Datenschutzgerechter Arbeitsplatz



1. Am Arbeitsplatz:

a) Dokumente in Papierform

- Unterlagen mit personenbezogenen Daten dürfen für Unberechtigte nicht einsehbar sein.
- Prüfen, ob Unterlagen nicht ohnehin in der Registratur aufzubewahren sind (z.B. Klausuren).
- Insbesondere Akten zu Personalangelegenheiten, Studierenden- und Prüfungsakten etc. müssen in verschlossenen Schränken aufbewahrt werden.
- Nur Sie, ggf. weitere Zugriffsberechtigte wie Ihr/e Vorgesetzte/r, dürfen einen Schlüssel haben.

- Achten Sie bei Ausdrucken oder Faxempfängen darauf, den Ausdruck sofort an sich zu nehmen. Achten Sie bei der Geräteauswahl insbesondere auf die Auswahl des richtigen Druckers.
- Fordern Sie andere niemals dazu auf, Unterlagen mit personenbezogenen Daten an einem für Unbefugte frei zugänglichen Ort abzulegen (insbesondere Abgabe von Hausarbeiten in unverschlossener Box vor dem Büro).
- Versenden Sie Unterlagen mit personenbezogenen Daten stets in verschlossenen Umschlägen.

b) Am PC

- Stellen Sie Ihren PC-Bildschirm so auf, dass Besucher den Bildschirminhalt nicht (unbeabsichtigt) lesen können.

- Teilen Sie Ihre Passwörter und Log-in-Daten niemals mit anderen.
- Speichern Sie dienstliche Arbeiten nicht lokal, sondern auf einem Netzlaufwerk ab.
- Personenbezogene Daten auf Notebooks oder anderen mobilen Datenträgern wie USB-Sticks sind zu verschlüsseln.
- Verifizieren Sie die eingegebenen E-Mail-Adressen vor dem Versand auf deren Korrektheit.
- Prüfen Sie bei E-Mails an mehrere Personen, ob es erforderlich ist, dass diese sehen wer die E-Mail erhält. Soweit dies nicht erforderlich ist, sind die Empfänger/innen im Bcc-Feld einzutragen. Aus dem Empfängerkreis von Rundmails lassen sich Rückschlüsse auf personenbezogene Daten ziehen.
  → Richtlinien zum Versand digitaler Rundschreiben an der Universität Passau;
  Antrag auf Versand einer Rund-Mail

- Senden Sie personenbezogene Daten niemals per E-Mail an Dritte, auch wenn die Anfrage von einer Behörde kommt. Nutzen Sie stattdessen sichere Cloud-Dienste, wie z.B. Filr, Vibe, Sync+Share. Dies gilt grundsätzlich auch für den universitätsinternen E-Mail-Versand.
- Fordern Sie andere niemals dazu auf, E-Mails mit personenbezogenen Daten an Sie zu übersenden.
- 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.

c) 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.
- 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.

2. Bei Verlassen des Büros:

- Schließen Sie Ihr Büro auch dann ab, wenn Sie es nur kurz verlassen.
- Verwenden Sie an Ihrem PC die Bildschirmsperre oder schalten Sie diesen ganz aus.
- Lassen Sie fremde Personen nicht allein in Ihrem Büro.
- Unterlagen mit personenbezogenen Daten (dies gilt auch für digitale Datenträger wie USB-Sticks) sind in einem verschlossenen Behältnis aufzubewahren.

3. Verarbeiten der Daten mittels privaten EDV-Geräten:

- Zugriff auf dienstliche Dokumente mittels privater EDV-Geräte (Laptop, Smartphone) ist auf datenschutzrechtlich unbedenkliche Tätigkeiten und unter dem Aspekt der Geheimhaltung zu beschränken.
- Sämtliche Cloud-Dienste (Dropbox) sowie Messenger (Skype) sind aus datenschutzrechtlicher Sicht hoch kritisch und daher für den Austausch personenbezogener Daten nicht (mehr) zulässig.
- Alternativen nutzen: Filr, Vibe, Sync+Share (ZIM, Online-Zugriff auf Ihre Laufwerke; LRZ Sync+Share)

4. Datenschutzkonforme Entsorgung von Papier und Datenträgern

- Datenträger sind nur solange aufzubewahren/zu speichern, wie diese zur Aufgabenerfüllung benötigt werden.
- Eine dauerhafte Speicherung personenbezogener Daten, bspw. enthalten in E-Mails ist unzulässig.
- Vor Entsorgung/ Löschung sämtlicher Unterlagen Aufbewahrungs- und Archivierungspflichten prüfen!
- Datenschutzgerechte Entsorgung von Papiergut gemäß Dienstanweisung zum Geschäftsgang („Schreddern“); Abholung durch Hauspost/Hausmeister.
- Für sonstige, digitale Datenträger gilt: Formular zur Rückgabe und Verschrottung von Geräten direkt an ZIM-Support.

5. Zusammenfassung:

→ Prüfung, ob für den Umgang mit personenbezogenen Daten die erforderliche Rechtsgrundlage besteht.

→ Hochschulmitarbeiter/innen dürfen nur dann Zugriff auf personenbezogene Daten haben, **wenn, soweit und solange** sie diese Daten zur Erfüllung ihrer Aufgaben benötigen.

→ Einhaltung der notwendigen **Zugangs- und Zugriffskontrollen.**

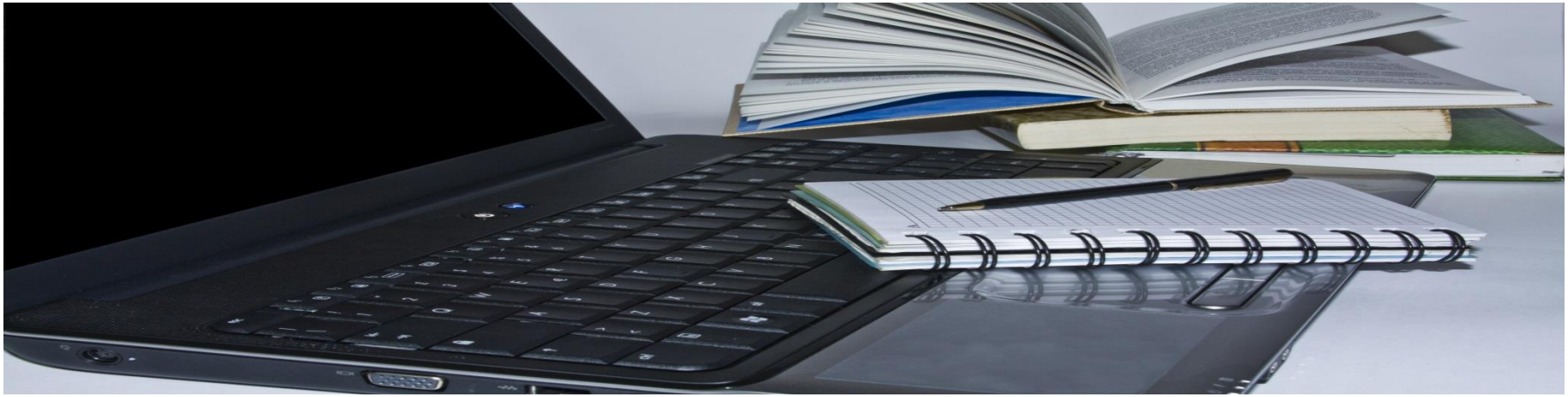
→ Dies gilt grundsätzlich unabhängig davon, ob die Daten auf Papier, auf dem PC oder anderen digitalen Medien gespeichert sind.

→ Dienstanweisung für den Geschäftsgang an der Universität Passau beachten.

→ Schriftgut zur Archivierung anbieten (Lagerung von Prüfungsunterlagen, Kontakt: Referat IX/5 - Archiv, Dokumentation, Registratur).

→ Bei Auskunftsanfragen von Betroffenen oder etwaigen Datenpannen: Unverzügliche Meldung an die Datenschutzbeauftragte (datenschutz@uni-passau.de).

III. Die einzelnen Datenverarbeitungen



Ihre rückgemeldeten Datenverarbeitungen zu:

- Studierendendaten
- Adresslisten/Einladungsmanagement
- Durchführung von Veranstaltungen/Fotoaufnahmen
- Personenbezogene Daten von Mitarbeitern/innen

Weitere?

Bitte melden an die Datenschutzbeauftragte!
http://www.uni-passau.de/verfahrensbeschreibung/;
Übersicht der zur Verarbeitung personenbezogener Daten genutzten automatisierten Verfahren;
Verfahrensbeschreibung

1. Bei der Erhebung von Daten ist stets

- **Die Rechtsgrundlage für die Datenverarbeitung zu prüfen, insb.:**
  - Aufgabenerfüllung im öffentlichen Interesse
  - zur Erfüllung eines Vertrags
  - Einwilligung des/r Betroffenen

- **Der/Die Betroffene zu informieren über:**
  - die/den Verantwortliche/n
  - die/den Datenschutzbeauftragte/n
  - Zweck und Rechtsgrundlage der Datenverarbeitung
  - Empfänger
  - ggf. Übermittlung an Drittland
  - Dauer der Speicherung
  - Betroffenenrechte
  - Beschwerderecht bei einer Aufsichtsbehörde

- **Die Datenverarbeitung zu dokumentieren (Nachweispflicht!):**
  - Einhaltung der zentralen Grundsätze der DSGVO (Vgl. S.7)
  - Rechtsgrundlage der Datenverarbeitung
  - Erfüllung der Informationspflichten

  → Schriftliche Dokumentation (ggf. in Form eines eigenen Aktenvermerks oder durch Fotoaufnahmen) erforderlich, wann, wo und wie der Kontakt hergestellt wurde, auf welcher Grundlage die Datenverarbeitung basiert und zu welchem Zweck personenbezogene Daten verarbeitet werden.

2. Umgang mit personenbezogenen Daten von Studierenden
(Prüfungsleistungen, Gutachten, Versand korrigierter Staatsprüfungen, Ausstellung von Zertifikaten, Notenlisten, Teilnehmerlisten, Listen ehemaliger Studierender, Matrikelnummer)

a) Allgemein

- **Rechtsgrundlage für Datenverarbeitung**
  - Aufgabenerfüllung im öffentlichen Interesse (v.a. Lehre und Studium)
  - Zur Erfüllung eines Vertrags
  - Einwilligung des/r Betroffenen
- **Erfüllung der Informations- und Dokumentationspflichten**

b) Einzelfälle

- Verwenden von Daten aus Stud.IP, HISQIS: nur soweit zur Aufgabenerfüllung erforderlich, bspw. zur Durchführung von Lehrveranstaltungen, Erstellung von Teilnehmerlisten etc.
- Auskunft an andere Einrichtungen der Universität: nur soweit zur Aufgabenerfüllung erforderlich, bspw. Übermittlung von Prüfungsleistungen an Studierendensekretariat.
- Prüfungsunterlagen sind vor unberechtigter Einsichtnahme zu schützen.
- Gesammelte Datensätze und Schriftgut sind nur solange aufzubewahren, als dies erforderlich ist. Dokumente nach Ablauf der gesetzlichen Aufbewahrungsfristen dem Archiv über die Registratur zur Aufbewahrung anbieten.

3. Adresslisten/Einladungsmanagement

a) Allgemein

- **Rechtsgrundlage für Datenverarbeitung**
  - Aufgabenerfüllung im öffentlichen Interesse (z.B. Unterrichtung der Öffentlichkeit)
  - Erfüllung eines Vertrags
  - Einwilligung des/r Betroffenen (z.B. Versand von Newsletter)
- **Erfüllung der Informations- und Dokumentationspflichten**

b) Einzelfälle

- **Umgang mit Bestandskontakten, Auswirkung der DSGVO?**
  - Problem der Nachweisbarkeit für das Vorliegen einer rechtmäßig erteilten Einwilligung.
  - Bestätigung einer bestehenden Einwilligungserklärung für “Bestandsdaten“ grdsl. nicht erforderlich, ggf. datenschutzrechtlichen Hinweis und Informationspflichten bspw. mit dem nächsten Anschreiben versenden, die Antwort ist zur Erfüllung der Dokumentationspflicht zu speichern.
  - Versand von Weihnachtskarten als „Kontaktpflege“ zulässig.
- **Umgang mit neuen Kontakten**
  - Bei der Entgegennahme von Visitenkarten handelt es sich um eine konkludente Einwilligung des Betroffenen in die Verarbeitung (Speicherung, Verwendung) seiner Kontaktdaten, Informationen sollten jedenfalls vorgehalten werden.
  - Bei Veranstaltungen kann eine „Kontaktbox“ für den Einwurf von Visitenkarten aufgestellt werden, Dokumentation dieses Vorgangs (ggf. durch Fotos).
  - Über den konkreten Verwendungszweck, bspw. zur Einladung von wiederkehrenden Veranstaltungsreihen, ist zu informieren .

4. Durchführung von Veranstaltungen/Fotoaufnahmen

a) Allgemein

- **Rechtsgrundlage für Datenverarbeitung**
  - Aufgabenerfüllung im öffentlichen Interesse (z.B. Unterrichtung der Öffentlichkeit)
  - Erfüllung eines Vertrags
  - Einwilligung des/r Betroffenen (v.a. bei studentischen (Pflicht-)veranstaltungen)
- **Erfüllung der Informations- und Dokumentationspflichten**

b) Einzelfälle

- **Durchführung von Veranstaltungen:**
  - Bereits bei der Anmeldung zur Veranstaltung ist auf die Erstellung sowie ggf. anschließende Veröffentlichung von Fotoaufnahmen hinzuweisen.
  - Bei der Veranstaltung ist durch Hinweisschilder auf die Erstellung und ggf. anschließende Veröffentlichung von Fotoaufnahmen hinzuweisen, ggf. kann ein “fotofreier Bereich“ eingerichtet werden.
  - Im Falle von Portraitfotos ist eine explizite Einwilligung des Betroffenen unter Angabe der beabsichtigten Verwendungszwecke (bspw. zur Veröffentlichung im Internet) einzuholen.
  - Bei studentischen Pflichtveranstaltungen ist eine Einwilligung des/r betroffenen Studierenden erforderlich, der Besuch der Veranstaltung muss aber möglich sein, auch wenn keine Einwilligung erteilt wird.

5. Umgang mit personenbezogenen Daten von Mitarbeiter/innen

a) Allgemein

- **Rechtsgrundlage für Datenverarbeitung**
  - Aufgabenerfüllung im öffentlichen Interesse
  - Zur Erfüllung eines Vertrages (v.a. Erfüllung der Pflichten aus Arbeitsvertrag)
  - Einwilligung des/r Betroffenen (z.B. Führen von Geburtstagslisten)
- **Erfüllung der Informations- und Dokumentationspflichten**

b) Einzelfälle

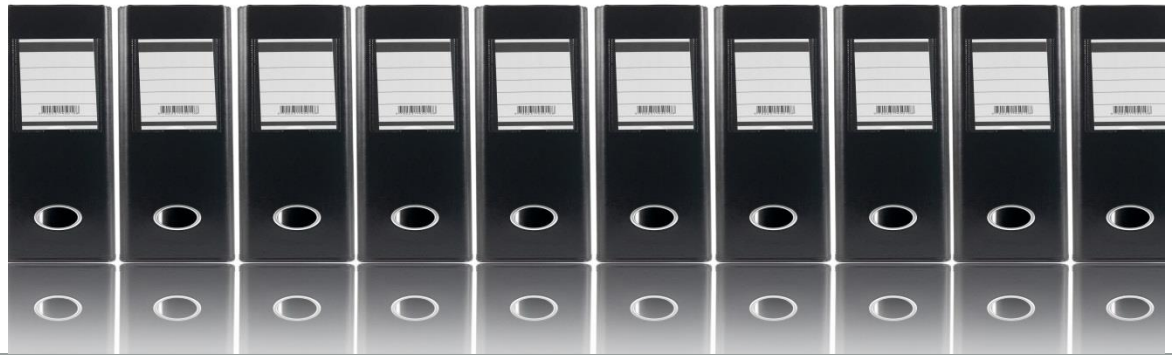
- **Beschäftigtendatenschutz**:
  - Bei Anträgen auf Einstellung (SHK, wiss. Mit.) findet eine Verarbeitung personenbezogener Daten statt.
  - Führen von Geburtstagslisten bedarf der Einwilligung jedes/r einzelnen Mitarbeiters/in. Aus Gründen der Datensparsamkeit ist auf die Eintragung des Geburtsjahres zu verzichten.
  - Führen von Urlaubskalendern/Abwesenheitskalendern über einen längeren Zeitraum hinweg ist unzulässig. Soweit eine solche Liste erforderlich ist (zur Erfüllung der Dienstpflicht/Jahresplanung), soll jedenfalls auf die Angabe des Abwesenheitsgrundes verzichtet werden.
  - Veröffentlichung von Kontaktdaten auf der Internetseite auch ohne Einwilligung zulässig, soweit es sich um Mitarbeiter/innen mit regelmäßigem Außenkontakt/Kundenkontakt handelt (Grundlage der Datenverarbeitung ist die Erfüllung der Dienstpflichten).
- **Führen von Personalakten/ Personalnebenakten:**
  Veranstaltung der Personalabteilung im Frühjahr 2019

Formulierungsbeispiel zur Einwilligung:

□ Ich stimme der Verarbeitung meiner Daten durch die Universität Passau zur ……. ausdrücklich zu. Rechtsgrundlage dieser Einwilligung ist Art. 6 Abs. 1 Satz 1 lit. a DSGVO. Meine Daten werden verwendet zum Zweck ……. und werden ……. gelöscht. Eine Übermittlung an ……. 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.

„Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“

IV. Verarbeitungsverzeichnis



Zur Erfüllung der Dokumentationspflicht:
Bereits **gemeldete Verfahren** bspw.

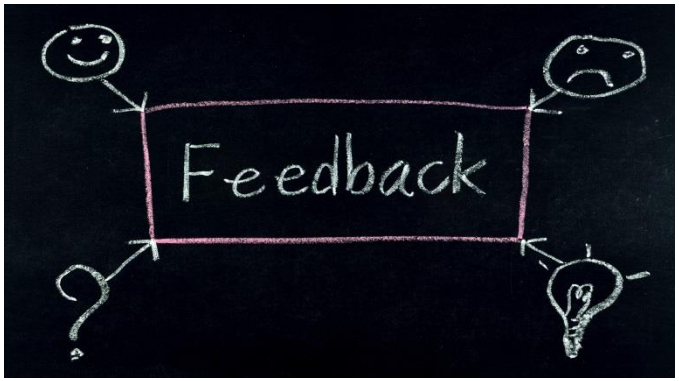
- Stud.IP (hiervon insb. abgedeckt Anmeldung zu Lehrveranstaltungen, Lehrangebote)
- HISQIS/HISinOne
- FIS

- Gilt für automatisierte (Verarbeitung unter Nutzung von EDV) sowie nicht automatisierte Datenverarbeitungen.
- Verantwortliche für die Datenverarbeitung ist die Universität Passau.
- Diejenige Person, die das Verfahren der Datenverarbeitung einsetzt und steuert ist verantwortlich für das jeweilige Verfahren.
  - Verhältnis Lehrstuhl – externer Lehrbeauftragter?
    Lehrbeauftragte werden in Erfüllung der universitären Aufgabenverpflichtung zur Lehre eingesetzt, Verfahrensverantwortlichkeit verbleibt beim Lehrstuhl.
- Als Empfänger von Daten kommen auch Stellen innerhalb der Verantwortlichen in Betracht, soweit voneinander abgrenzbare Bereiche von gewisser Eigenständigkeit vorliegen.

bei Weitergabe personenbezogener Daten an andere Abteilung/ Einrichtungen **innerhalb** der Universität liegt eine Übermittlung, also eine Datenverarbeitung vor!

Vielen Dank
für
Ihre Aufmerksamkeit!

Weitere Fragen oder Feedback gerne an



Ihre Ansprechpartnerinnen für datenschutzrechtliche Fragen:

- **Datenschutzbeauftragte**
  Anna Sperrhake
  Raum N12 210
  Tel.: +49 851 509-1107
  datenschutz@uni-passau.de

- **Mitarbeiterin**
  Carolin Erbersdobler
  Raum N12 206
  Tel.: +49 851 509-1114
  datenschutz@uni-passau.de

Ihre Ansprechpartnerin für datenschutzrechtliche Schulungen:

- **Mitarbeiterin**
  Iris Köckerandl
  Raum N12 110
  Tel.: +49 851 509-1112
  Iris.Koeckerandl@uni-passau.de