

Leitfaden zum Datenschutz und zur Verarbeitung personenbezogener Daten

Universität Passau

Inhaltsverzeichnis

1	Einleitung	4
2	Grundregeln zum Umgang mit personenbezogenen Daten	4
3	Anforderungen und Ziele	5
4	Verhaltensregeln am Arbeitsplatz.....	6
4.1	Clean Desk Policy	6
4.2	Umgang mit Dokumenten in Papierform	6
4.3	Umgang mit personenbezogenen Daten am Telefon.....	6
4.4	E-Mail-Nutzung	7
4.5	Internetnutzung	8
4.6	Nutzung von Druckern, Scannern und Kopierern	9
4.7	Umgang mit mobilen IT-Geräten	9
4.8	Umgang mit Wechselmedien.....	10
4.9	Entsorgung von Dokumenten und Datenträgern	10
4.10	Social Engineering	11
4.11	Warnungen und Fehlermeldungen.....	11
4.12	Installation von Applikationen	11
4.13	Anfertigung von Foto- und Filmaufnahmen am Arbeitsplatz	12
4.14	Sicherheit in sozialen Netzwerken	12
5	Konsequenzen bei Nichtbeachtung	12
6	FAQ.....	13
6.1	Welche Rechtsgrundlagen bestehen für die Verarbeitung personenbezogener Daten?.....	13
6.2	Wir werden die Informationspflichten zum Zeitpunkt der Erhebung personenbezogener Daten erfüllt?.....	14
6.3	Wie wird die Dokumentationspflicht bei der Verarbeitung personenbezogener Daten erfüllt?	14
6.4	Was ist für die Dokumentation der Datenverarbeitungsvorgänge zu beachten?	15
6.5	Wann liegen personenbezogene Daten von Studierenden vor?	15
6.6	Was ist bei einer Übermittlung von Prüfungsleistungen an andere Organisationseinheiten der Universität zu beachten?	16
6.7	Was gilt für die Bekanntgabe von Prüfungsleistungen an Studierende?	16
6.8	Was gilt für Aufbewahrungs-/Speicherdauer gesammelter Datensätze?	16
6.9	Was ist im Umgang mit Kontaktdaten zu beachten?	16
6.10	Wann ist eine Veröffentlichung von Kontaktdaten zulässig?	17
6.11	Wie ist die Verwaltung von Adresslisten, insbesondere in Bezug auf „Altkontakte“, zu handhaben?	17
6.12	Was ist bei dem Versand von Einladungen und Grußkarten zu beachten?	18

6.13 Was ist bei der Vorbereitung und Durchführung von Veranstaltungen zu beachten?	18
6.14 Wie ist der korrekte Umgang mit Kontaktdaten bei Veranstaltungen?	19
6.15 Wie ist der korrekte Umgang mit Fotoaufnahmen bei Veranstaltungen?	19
6.16 Was ist beim Umgang mit personenbezogenen Daten von Beschäftigten zu beachten?	20
6.17 Was ist beim Führen von Geburtstagslisten zu beachten?	20
6.18 Was ist beim Führen von internen Abwesenheitskalendern zu beachten?	21
6.19 Welche Vorlage für Einwilligungserklärung und Datenschutzhinweis ist zu verwenden, und wo finde ich diese?	21
A.1 Grundsätze für die Verarbeitung personenbezogener Daten	22

1 Einleitung

Dieser Leitfaden beinhaltet Verhaltensregeln zur Einhaltung des Datenschutzes an der Universität Passau (nachfolgend Verantwortlicher genannt) sowie zum sicheren Umgang mit personenbezogenen Daten. Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen der Geschäftstätigkeit sind u.a. die Datenschutzgrundverordnung (DSGVO), das Bayerische Datenschutzgesetz (BayDSG) sowie das Bayerische Hochschulgesetz (BayHIG). Die DSGVO bildet dabei die zentrale rechtliche Grundlage, die für den Umgang mit personenbezogenen Daten verbindlich und umzusetzen ist.

Im Anhang A.1 finden Sie die Grundsätze zur Verarbeitung personenbezogener Daten.

Bei Fragen zur Umsetzung datenschutzrechtlicher Anforderungen wenden Sie sich bitte an:

Datenschutzbeauftragter (extern)

Herr Marco Wallek
actago GmbH
Weidenstraße 66
94405 Landau a.d.Isar
Tel.: +49 9951 99990 500
E-Mail: datenschutz@uni-passau.de

Stellvertretung (intern)

Frau Kathrin Bernecker
Raum N12 116
Tel.: +49 851 509 7124
E-Mail: datenschutz@uni-passau.de

2 Grundregeln zum Umgang mit personenbezogenen Daten

- a. Alle personenbezogenen Daten sind grundsätzlich als "vertraulich" einzustufen und dürfen nur von autorisierten Personen verarbeitet werden. Ausnahmen hierzu bilden z.B. Kommunikationsdaten oder Daten, die aus allgemein zugänglichen Quellen erhoben werden können.
- b. Es dürfen nur die für den jeweiligen Zweck notwendigen Daten erhoben, verarbeitet und genutzt werden. Es gilt der Grundsatz der Datenminimierung.
- c. Die erhobenen Daten dürfen nur für den jeweiligen Zweck (z.B. Daten von Beschäftigten für die Abwicklung im Personalwesen) verwendet werden. Es gilt der Grundsatz der Zweckbindung.
- d. Grundsätzlich sind diese Daten unter Angabe des Verwendungszweckes, Kontaktdaten des Datenschutzbeauftragten, der Rechtsgrundlage, möglicher Empfänger, der Speicherdauer und unter Angabe der Identität der verantwortlichen Stelle bei Betroffenen zu erheben. Werden diese Daten nicht bei Betroffenen erhoben, so ist der Betroffene zusätzlich über die Quelle der Erhebung zu benachrichtigen. Auf die Betroffenenrechte nach Punkt 4 f) ist hinzuweisen.
- e. Integrität der Daten, Vertraulichkeit und Datenqualität sind zu gewährleisten. Falsche oder unvollständige Daten sind umgehend zu berichtigen beziehungsweise zu löschen.
- f. Es ist sicherzustellen, dass die Rechte der Betroffenen gewährleistet werden. Hierzu zählen:
 - Das Recht auf Auskunft über Herkunft und Zweck der Verarbeitung und im Falle von Datenübermittlung über die Angabe der Empfänger oder Empfängerkategorien. (Art. 15 DSGVO)
 - Das Recht auf Berichtigung von Daten, wenn diese falsch oder unvollständig sind. (Art. 16 DSGVO)
 - Das Recht auf Einschränkung im Falle, dass sich die Richtigkeit der Daten nicht nachweisen lässt. (Art. 18 DSGVO)
 - Das Recht auf Löschung im Falle der Unzulässigkeit der Datenverarbeitung bzw. wenn der angegebene Verwendungszweck erfüllt ist. Gesetzliche Aufbewahrungsfristen gelten vorrangig. (Art. 17 DSGVO)

- Das Recht auf Datenübertragbarkeit, d.h. die betroffene Person kann die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format erhalten oder an einen anderen Verantwortlichen übermitteln lassen. (Art. 20 DSGVO)
 - Das Recht auf Widerspruch gegen die Verarbeitung personenbezogener Daten, soweit diese auf Grundlage von Art. 6 Abs. 1 lit. e oder f DSGVO erfolgt. (Art. 21 DSGVO)
 - Das Recht, keine ausschließlich auf automatisierter Verarbeitung beruhende Entscheidung – einschließlich Profiling – zu unterliegen, die gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. (Art. 22 DSGVO)
 - Das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes. (Art. 77 DSGVO)
 - Das Recht, eine Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen, ohne dass die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung berührt wird. (Art. 7 Abs. 3 DSGVO)
- g. Bestehen durch die Zwecke und Inhalte einer Verarbeitungstätigkeit voraussichtlich hohe Risiken für die Rechte und Freiheiten der betroffenen Personen, ist eine Datenschutz-Folgenabschätzung für diese Verarbeitungstätigkeit durchzuführen. Diese ist schriftlich zu dokumentieren. Der Datenschutzbeauftragte ist für die Erstellung hinzuzuziehen.

3 Anforderungen und Ziele

Die Universität Passau besitzt eine hohe Anzahl an Aufgaben, bei denen personenbezogene Daten verarbeitet werden. Deren Vertraulichkeit, Integrität und Verfügbarkeit stellen ein hohes Gut dar, weisen einen erhöhten Schutzbedarf auf und müssen vor unberechtigter Kenntnisnahme durch Dritte besonders geschützt werden.

Die Universität Passau verfolgt mit diesem Leitfaden folgende Ziele:

- Die Gewährleistung der rechtmäßigen Verarbeitung personenbezogener Daten nach Treu und Glauben. (Art. 5 Abs. 1 lit. a DSGVO)
- Die Sicherstellung der Transparenz der Verarbeitung gegenüber den betroffenen Personen. (Art. 5 Abs. 1 lit. a DSGVO)
- Die Gewährleistung der Verarbeitung personenbezogener Daten nur für festgelegte, eindeutige und legitime Zwecke. (Art. 5 Abs. 1 lit. b DSGVO)
- Die Begrenzung der Verarbeitung personenbezogener Daten auf das für die Zwecke notwendige Maß. (Art. 5 Abs. 1 lit. c DSGVO)
- Die Gewährleistung der Richtigkeit und Aktualität der verarbeiteten personenbezogenen Daten. (Art. 5 Abs. 1 lit. d DSGVO)
- Die Gewährleistung, dass personenbezogene Daten nur so lange verarbeitet werden, wie dies für die Zwecke erforderlich ist. (Art. 5 Abs. 1 lit. e DSGVO)
- Die Sicherstellung der Integrität und der Vertraulichkeit der verarbeiteten personenbezogenen Daten. (Art. 5 Abs. 1 lit. f DSGVO)
- Die Nachweisbarkeit der Einhaltung der datenschutzrechtlichen Anforderungen. (Art. 5 Abs. 2 DSGVO)

Ausgerichtet an diesen Zielen werden Anforderungen identifiziert und geprüft, ob zu deren Einhaltung entsprechende Vorbeuge- bzw. Korrekturmaßnahmen ergriffen werden müssen.

Die eingesetzten Mittel zur Erreichung der Ziele der Universität Passau sollen mit einem angemessenen Verhältnis von Aufwand und Wirkung bestimmt werden und tragen zu einer Minimierung aller mit der jeweiligen Datenverarbeitungstätigkeit verbundenen Risiken in geeigneter Art und Weise bei.

4 Verhaltensregeln am Arbeitsplatz

4.1 Clean Desk Policy

Unter der Clean Desk Policy versteht man, dass Beschäftigte alle vertraulichen Dokumente, die sich auf ihrem Arbeitsplatz befinden, verschließen. Unberechtigte Personen (z.B. Reinigungspersonal, unbefugte Kollegen oder Besucher) dürfen keinen Zugriff darauf erhalten. Dabei ist insbesondere Folgendes zu beachten:

- Ausdrucke dürfen nicht im Drucker/Kopierer liegengelassen werden.
- Passwortnotizen dürfen nicht am Arbeitsplatz aufbewahrt werden. Stattdessen können Programme zur Speicherung und Organisation von Passwörtern genutzt werden (z.B. KeePass).
- Der Computer ist auch bei **kurzfristigem** Verlassen des Arbeitsplatzes zu sperren (z.B. unter Windows mit „Windows-Taste + L“). Unbeaufsichtigte, nicht gespernte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten. Unterlagen mit sensiblen Daten sind auch beim kurzzeitigen Verlassen vor unberechtigtem Zugang zu schützen.
- Das Büro ist bei Verlassen abzusperren. Am Ende des Arbeitstages sind alle Fenster zu schließen.
- Sensible und vertrauliche Informationen sind in analoger (z.B. auf Papier) als auch in digitaler Form (z.B. Speichermedium) immer unter Verschluss zu halten, wenn Sie diese nicht benötigen.
- Bei Arbeitsplätzen mit Publikumsverkehr sind Ablagen (z.B. Ablagefächer), Eingabegeräte (z.B. Tastatur, Unterschriftfelder), Anzeigegeräte (z.B. Monitore, integrierte Displays), Ausgabegeräte (z.B. Drucker, Multifunktionsgeräte, Faxgeräte) so aufzustellen, dass die Einsichtnahme durch Unbefugte nicht möglich ist.

4.2 Umgang mit Dokumenten in Papierform

Der sorgfältige Umgang mit papierbasierten Dokumenten erfordert besondere Schutzmaßnahmen. Bitte beachten Sie daher folgende Punkte:

- Unterlagen mit personenbezogenen Daten dürfen nicht für Unbefugte einsehbar sein. Achten Sie darauf, dass diese Dokumente geschützt und nicht offen zugänglich sind.
- Umlaufmappen und Aktenordner müssen mit Aktenzeichen versehen werden.
- Akten, die besonders schützenswerten Daten (z.B. Personal- oder Studierendenangelegenheiten sowie Prüfungsakten) enthalten, sind in verschlossenen Schränken aufzubewahren. Nur berechnigte Personen dürfen Zugriffsschlüssel besitzen.
- Der Zugang zu Papierakten muss kontrolliert sowie nachvollziehbar dokumentiert sein.
- Fordern Sie niemanden dazu auf, Unterlagen mit personenbezogenen Daten an öffentlich zugänglichen Orten abzulegen. Hausarbeiten dürfen z.B. nicht in einer unverschlossenen Box vor dem Büro gesammelt werden.
- Dokumente mit personenbezogenen Daten sind nur in verschlossenen Umschlägen zu versenden.
- Sobald Dokumente in Papierform vor Ort nicht mehr benötigt werden, sind diese der Registratur/dem Archivar zur ordnungsgemäßen Archivierung anzubieten. Dies gilt insbesondere für Klausuren und andere Prüfungsleistungen.

4.3 Umgang mit personenbezogenen Daten am Telefon

Im Umgang mit telefonischen Anfragen sind folgende Verhaltensregeln zum Schutz personenbezogener Daten besonders wichtig:

- Geben Sie am Telefon keine Auskünfte, wenn Sie den Anrufer nicht zweifelsfrei identifizieren können.
- Prüfen Sie vor der Weitergabe personenbezogener Daten stets, ob Sie zur Auskunft berechnigt sind, d.h. ob die erforderliche Rechtsgrundlage vorliegt.

- Achten Sie darauf, dass Unberechtigte keine Kenntnis vom Inhalt des Gesprächs erlangen können.
- Bei Anfragen zu abwesenden Mitarbeitern darf der Grund der Abwesenheit (z.B. Krankheit oder Urlaub) nicht genannt werden. Geben Sie lediglich an, wann die Person voraussichtlich wieder erreichbar ist.

4.4 E-Mail-Nutzung

Die E-Mail gehört zur Standardausrüstung eines jeden Büroarbeitsplatzes. Dadurch lohnt es sich auch für Kriminelle, diese Form der Kommunikation zu nutzen. Somit landen auch Spam-, Hoax- oder Phishing-Mails sowie mit Schadprogrammen verseuchte Nachrichten im Posteingang. Solche unerwünschten Nachrichten – mit mehr oder weniger gefährlichem Inhalt – machen den Großteil des weltweiten E-Mail-Aufkommens aus. Daher sind folgende Punkte zu beachten:

- Öffnen Sie keine E-Mails oder Links, wenn Ihnen Absender oder Betreffzeile verdächtig erscheinen oder unbekannt sind (beispielsweise Sie erhalten eine E-Mail von T-Mobile bezüglich Ihres Vertrages, obwohl Sie dort kein Kunde sind). Seien Sie daher grundsätzlich vorsichtig bei E-Mails von externen Kontakten, aber ebenso von Kollegen sowie der Führungsebene, da Urheber von Phishing-Mails seriöse Absender zunehmend besser nachahmen.
- Nehmen Sie sich Zeit für den 3-Sekunden-Sicherheits-Check: Prüfen Sie Absender, Betreff und Anhang vor dem Anklicken.
- Öffnen Sie niemals Dateianhänge, die Ihnen verdächtig vorkommen. Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen: Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen, fehlerhafte Grammatik etc.)? Erwarteten Sie die beigelegten Dateien und passen sie zum Absender, oder kommen sie völlig unerwartet?
- Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, müssen gelöscht werden. Die angeforderten, vertraulichen Informationen dürfen Sie auf keinen Fall weitergeben. Mögliche Indizien für Phishing-Mails sind fehlerhafte Grammatik, fehlende persönliche Anrede und Aufforderung zur Eingabe von Daten über einen Link.
- Oftmals kann in einer E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien Sie dabei vorsichtig: In betrügerischen E-Mails wird bei diesen Links oft eine andere Internet-Adresse hinterlegt, als in der Mail zu sehen ist. Beim Anklicken wird dann eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert. Sicherer ist es, den Link mittels „Hyperlink kopieren“ in den Browser zu übertragen und ihn vor dem Aufrufen noch einmal zu überprüfen.
- Beantworten Sie keine Spam-Mails! Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit Ihrer Mail-Adresse und erhöht dadurch Ihr Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.
- Benachrichtigen Sie auch Ihre Kollegen über verdächtige Zusendungen. Besprechen Sie die aktuellen E-Mails, die Sie als Phishing-Versuche oder Virus-Mails erkannt haben, um gemeinsam die typischen Kennzeichen kennenzulernen. Sie können auf diese Weise sehr rasch Ihre Erkennungsfähigkeit trainieren und verbessern.
- Denken Sie bei Ihrem Urlaubsantritt oder bei Abwesenheit an den Abwesenheitsassistenten, um die Absender über ihre Abwesenheit zu informieren.
- Verwenden Sie stets starke, einmalige Passwörter und geben Sie diese niemals weiter.
- Nehmen Sie keine Veränderungen in den Sicherheitseinstellungen Ihres E-Maildienstes vor.
- Aktivieren Sie die Anzeige aller Datei-Endungen (Dateitypen).
- Schützen Sie die E-Mail-Adressen im Feld „BCC“ als sogenannte „Blindkopie“ bei einem E-Mail-Versand an mehrere Empfänger!
- Beachten Sie für den Versand von Rundmails an Beschäftigte folgende [„Richtlinie zum Versand digitaler Rundschreiben an der Universität Passau“](#).

- Verwenden Sie für den Versand von Rundmails folgenden [„Antrag auf Versand einer Rundmail“](#).
- Leiten Sie keine Kettenbriefe weiter.
- Informieren Sie sich bei Ihrem Vorgesetzten, ob eine Verschlüsselung von E-Mails möglich ist, und setzen Sie diese, insofern vorhanden um. Dadurch kann die E-Mail nur durch den rechtmäßigen Empfänger gelesen werden.
- Beim Versenden von besonders schutzwürdigen Daten im Anhang ist auf eine Passwortsicherung des Anhangs zu achten und den Empfänger durch einen anderen Kommunikationsweg (z.B. telefonisch) das Kennwort zu nennen. Fragen Sie hierzu bei Bedarf Ihre IT-Ansprechpartner.
- 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.

4.5 Internetnutzung

Nicht nur die E-Mail-Kommunikation, sondern auch die Nutzung des Internets birgt Gefahren, die nicht gleich als solche erkannt werden können. Bitte beachten Sie daher folgende Punkte:

- Wählen Sie einen Internet-Browser, der von Ihrer IT freigegeben wurde.
- Konfigurieren Sie Ihren Browser so, dass Pop-up-Meldungen unterdrückt werden. Wenn Sie unsicher sind wie, fragen Sie bei Ihren IT-Ansprechpartnern nach.
- Achten Sie auf Hinweise bezüglich ungültiger und/oder abgelaufener Sicherheitszertifikate von Web-Diensten. Fragen Sie im Zweifel bei Ihren IT-Ansprechpartnern nach.
- Übermitteln Sie keine persönlichen Daten an unbekannte Anbieter, vor allem nicht, wenn die Verbindung nicht als sicher (HTTPS oder Schlosssymbol  links von der Websiteadresse) markiert wird.
- Geben Sie auch bei bekannten Anbietern nur diejenigen Daten an, die für den jeweiligen Zweck unbedingt notwendig sind und achten Sie insbesondere bei besonders schutzwürdigen Daten auf ausreichende Schutzmaßnahmen.
- Websites, die mit dem Download kostenloser Zusatzsoftware oder unseriösen Gewinnspielen locken, ist grundsätzlich zu misstrauen.
- Das Herunterladen von Dateien kann – abgesehen von der Gefahr des Einschleppens von Schadsoftware – auch zu lizenz- und urheberrechtlichen Problemen führen. Das gilt auch für Software, die nicht installiert oder ausgeführt wurde und nur auf dem Bürorechner gespeichert ist.
- Meiden Sie Hackerseiten und solche, auf denen kommerzielle Software, möglicherweise in ge-crackter Form, zum Download angeboten wird.
- Rufen Sie keine Websites mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten auf. Das kann gravierende rechtliche Probleme – auch für den Verantwortlichen – nach sich ziehen.
- Lockern Sie nicht die Sicherheitseinstellungen Ihres Browsers.
- Fragen Sie lieber einmal zu viel bei Ihren IT-Ansprechpartnern nach.

4.6 Nutzung von Druckern, Scannern und Kopierern

Die Geräte, die vereinfacht immer noch Fotokopierer genannt werden, weisen mittlerweile zahlreiche Funktionen auf. Je nach Ausstattung lassen sie sich als Drucker an einen oder mehrere Computer anschließen, versenden Faxe oder sind als Scanner für Dokumentenstapel einsetzbar. Kopiergeräte haben sich zu Multifunktionsgeräten gewandelt und sind dabei meist schnell und einfach zu bedienen. Und weil sie an ihren Einsatzorten und für ihre vielfältigen Zwecke mit den jeweiligen Computern vernetzt sind, haben in der Regel mehrere Menschen Zugriff darauf, ohne deshalb ständig neben ihnen stehen zu müssen. Da die Druckerzeugnisse selbst personenbezogene Daten enthalten können, beachten Sie bitte die folgenden Punkte:

- Originale und Kopien sind immer sofort nach Ende der Nutzung aus dem Gerät zu entfernen. Bitte vergessen Sie in diesem Zuge keine Unterlagen auf der Scanfläche des Geräts.
- Fehlkopien sind datenschutzgerecht zu vernichten (siehe Punkt 4.9).
- Das System des Geräts ist nach Gebrauch in seinen ursprünglichen Zustand zurückzusetzen, beispielsweise durch Drücken der "C"-Taste oder einer Tastenkombination, mit der das System in den Stand-by-Modus geschaltet wird.
- Werden die Kopierer als Arbeitsgruppendrucker von mehreren Personen genutzt, so sollten dort möglichst keine Dokumente mit personenbezogenen oder anderweitig sensiblen Daten ausgedruckt werden. Lässt sich dies nicht vermeiden, ist sicherzustellen, dass die ausgedruckten Dokumente sofort nach Abschluss des Druckvorgangs entfernt werden und dass keine unbefugten Personen Kenntnis der ausgedruckten Daten erhalten können.
- Erfolgt die Verwendung des Gerätes erst durch eine vorherige Benutzeranmeldung, stellen Sie sicher, dass Sie sich anschließend auch wieder abmelden.

4.7 Umgang mit mobilen IT-Geräten

Notebooks, Smartphones, Tablets, u.Ä. stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar. Portable Geräte sind für Diebe ein attraktives Ziel. Bitte beachten Sie daher folgende Punkte:

- Nehmen Sie keine IT-Komponente oder Datenträger mit nach Hause, die nicht ausdrücklich dafür ausgewiesen wurden.
- Nutzen Sie nur die offiziell von der IT-Abteilung freigegebene Software auf Ihren Arbeitsgeräten.
- Die Nutzung des Messengerdienstes WhatsApp und anderer, nicht datenschutzkonformer Dienste (z.B. Telegram) auf Dienstgeräten ist grundsätzlich untersagt und nur in Ausnahmefällen möglich.
- Sperren Sie den Zugriff auf Ihrem Gerät, sobald Sie Ihren Arbeitsplatz verlassen – auch wenn es sich nur um eine kurze Abwesenheit von wenigen Minuten handelt.
- Lassen Sie das Gerät nicht unbeaufsichtigt. Sollten Sie das Gerät nicht benötigen, verwahren Sie es an einem Ort, um es gegen Verlust oder Diebstahl zu sichern.
- Melden Sie einen Diebstahl oder Verlust sofort Ihren IT-Ansprechpartnern.
- Überlassen Sie das Gerät nicht anderen Personen.
- Schützen Sie ihre mobilen Geräte mit sicheren Passwörtern. Geben Sie diese nicht weiter.
- Achten Sie bei Passworteingabe am Gerät auf Ihren Sichtschutz (ähnlich wie bei einem Bankautomaten).
- Verwenden Sie Ihren privaten Cloud-Speicher nicht für betriebliche Daten.
- Achten Sie auf Vertraulichkeit der Umgebung bei Gesprächen und Arbeiten am Notebook außer Haus. Verwenden Sie ggf. eine Sichtschutzfolie für den Notebook-Bildschirm und verwenden Kürzel anstatt voller Namen bei Telefongesprächen, wenn Sie in öffentlichen Bereichen (beispielsweise Zugabteile) arbeiten.

4.8 Umgang mit Wechselmedien

Als Wechselmedien gelten alle externen Datenträger wie z.B. USB-Sticks, SD-Karten, externe Festplatten, CDs, DVDs, die per USB oder Laufwerk an einen Computer angeschlossen werden. Der Einsatz stellt ein großes Sicherheitsrisiko dar, speziell wenn diese Datenträger aus externer Quelle stammen. Auf diesen Wechselmedien kann Schadsoftware gespeichert sein, welche das gesamte Organisationsnetzwerk lahmlegen kann. Generell ist die Verwendung von Wechselmedien untersagt. Bitte beantragen Sie eine Ausnahmegenehmigung, falls Sie dennoch Wechselmedien verwenden müssen. Bitte beachten Sie daher folgende Punkte:

- Verwenden Sie keine geschenkten oder gefundenen Wechselmedien unbekannter Herkunft. Bei einem USB-Stick kann beispielsweise bereits Schadsoftware auf Ihrem Computer installiert werden, sobald Sie diesen am Computer anschließen.
- Gehen Sie mit Ihrem Wechselmedium nur an Rechner, die vertrauenswürdig sind.
- Möchten Sie einen Datenträger transportieren, wenden Sie sich bitte an die IT-verantwortliche Stelle, die entsprechende Sicherheitsvorkehrungen vornehmen wird.
- Speichern Sie keine personenbezogenen Daten auf mobilen Datenträgern.
- Wenn Sie personenbezogenen Daten auf mobilen Datenträgern speichern möchten, konsultieren Sie die IT-verantwortliche Stelle, welche anschließend die entsprechende Funktionalität zur Verfügung (z.B. Datenträger-Kryptographie) stellt.
- Geben Sie das Wechselmedium nicht an unberechtigte Dritte weiter.
- Nicht mehr benötigte Daten auf dem Wechselträger sind zu löschen, gegebenenfalls muss der Datenträger unbrauchbar gemacht werden.
- Achten Sie auf eine sichere Löschung und Entsorgung von auszusondernden Datenträgern. Ein einfaches Formatieren reicht nicht aus. Bitte beachten Sie dazu die Hinweise zur sicheren Entsorgung aus Punkt 4.9.

4.9 Entsorgung von Dokumenten und Datenträgern

Sorglos weggeworfene Dokumente stellen ein ernstes Sicherheitsproblem dar, wenn diese Daten in falsche Hände geraten. Aus diesem Grund müssen Dokumente, Datenträger (USB-Stick, Festplatte, SD-Karte, CD/DVD, o.Ä.) sicher entsorgt werden. Für die sichere Entsorgung eignet sich ein Dokumenten-Shredder oder ein Dienstleistungsunternehmen, welches sich auf die sichere Entsorgung spezialisiert hat. Das Dienstleistungsunternehmen stellt Ihnen anschließend ein Zertifikat aus, welches die fachgerechte Entsorgung bestätigt. Bitte beachten Sie folgende Punkte:

- Werfen Sie Datenträger oder wichtige Dokumente auf keinen Fall in den Papierkorb! Sofern es sich um Inhalte handelt, die Außenstehenden nicht zugänglich gemacht werden dürfen, müssen die Datenträger und Dokumente sicher entsorgt werden. Beachten Sie, dass diese Vorgehensweise auch bei Archivmaterial einzuhalten ist.
- Maßnahmen zur Papiervernichtung:
 - Lassen Sie keine Dokumente auf dem Tisch liegen und verwahren Sie die Dokumente weiterhin bis zu ihrer Vernichtung gesichert auf.
 - Führen Sie eine sichere und vertrauliche Sammlung und Vernichtung von Papierunterlagen durch.
 - Nutzen Sie zur Papiervernichtung die vorhandene Datentonne oder alternativ einen Aktenvernichter (Shredder), der mindestens Crosscut-Qualität (Kreuzschnitt/Partikelschnitt) aufweist (ab einer Sicherheitsstufe von P-4). Bitte beachten Sie hierzu die [„Dienststanweisung für den Geschäftsgang“](#).
 - Für größere Mengen an Datenmüll ist ggf. der Container einer zertifizierten Datenmüllentsorgungsfirma zu verwenden.

- Maßnahmen bei elektronischen Datenträgern:
 - Übergeben Sie die nicht mehr benötigten Datenträger den Verantwortlichen Ihrer IT bzw. einer eigens zu diesem Zweck bestimmten Person, die für die sichere Entsorgung zuständig ist. Füllen Sie hierzu das Formular [„Rückgabe und Verschrottung von Geräten“](#) aus und senden Sie es an den ZIM-Support.

4.10 Social Engineering

Unter Social Engineering versteht man das Manipulieren von Personen, um unbefugten Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Vorwiegend wird dieser Angriff per Telefon oder E-Mail durchgeführt.

Social Engineers geben sich gerne als Mitarbeiter aus. Vielleicht behaupten sie auch, eine Behörde oder ein wichtiges Kundenunternehmen zu vertreten oder zu Ihrer IT-Abteilung zu gehören. Ihre Opfer werden durch firmeninternes Wissen oder Kenntnisse spezieller Fachbegriffe getäuscht, die sie sich zuvor durch Telefonate oder Gespräche mit anderen Kollegen erworben haben. Beim Angriff appellieren sie dann als „gestresster Kollege“ an Ihre Hilfsbereitschaft oder drohen als „Kunde“ mit dem Verlust eines Auftrages. Kommt ein Social Engineer bei einem Beschäftigten nicht ans Ziel, wird der Angriff bei der nächsten Ansprechperson wiederholt – bis er erfolgreich ist.

Bitte beachten Sie daher folgende Punkte:

- Seien Sie bei Telefonanrufen oder E-Mails skeptisch, speziell wenn der Wunsch oder der Auftrag des Kollegen außergewöhnlich ist.
- Falls möglich, besprechen Sie die Angelegenheit mit Ihrem Kollegen persönlich.
- Fragen Sie bei verdächtigen E-Mails Ihre IT-Ansprechpartner.
- Lassen Sie sich von anfragenden Personen nicht unter Druck setzen, sondern rückversichern Sie sich stattdessen intern, bevor Sie vertrauliche Informationen herausgeben.
- Bedenken Sie, dass Social Engineering sehr oft angewandt wird, aber meistens lange Zeit unentdeckt bleibt. Bleiben Sie daher stets aufmerksam.
- Geben Sie keine vertraulichen Informationen per Telefon oder E-Mail weiter, wenn der Empfänger Ihnen nicht bekannt ist oder unklar ist, ob die anfragende Person tatsächlich diejenige ist, für die sie sich ausgibt. Fragen Sie im Zweifel bei der jeweiligen Person nach.
- Melden Sie verdächtige Vorfälle stets Ihrem Vorgesetzten.

4.11 Warnungen und Fehlermeldungen

Warnungen oder Fehlermeldungen, die Sie selbst nicht verursacht haben, bzw. die Sie nicht lösen können, müssen unverzüglich Ihren IT-Ansprechpartnern gemeldet werden.

4.12 Installation von Applikationen

Die Installation von Applikationen ist untersagt. Dies gilt sowohl für Windows-Geräte (PCs, Notebooks, Server), aber auch für organisationseigene Mobilgeräte wie Smartphone und Tablets. Falls Sie eine Applikation benötigen, senden Sie eine schriftliche Anfrage an Ihre IT-Ansprechpartner. Auch harmlos wirkende Applikationen können Schadsoftware enthalten oder sind lizenzrechtlich nicht für den Einsatz freigegeben.

4.13 Anfertigung von Foto- und Filmaufnahmen am Arbeitsplatz

Aufgrund der geltenden Datenschutzbestimmungen ist es Mitarbeitern untersagt, Fotos mit privaten Mobilgeräten am Arbeitsplatz zu machen und zu verbreiten. Dies gilt sowohl für Arbeitsbereiche als auch für Arbeitskollegen am gesamten Gelände und in Einrichtungen des Verantwortlichen.

Der Grund dafür ist, dass die Verbreitung von Fotos ohne Zustimmung der abgebildeten Personen eine Verletzung der Privatsphäre darstellen kann und zudem auch vertrauliche Informationen des Verantwortlichen preisgeben kann. Sollten Mitarbeiter dennoch Fotos machen müssen, sind diese ausschließlich mit hierfür bereitgestellten Kameras anzufertigen und nur für geschäftliche Zwecke zu verwenden.

4.14 Sicherheit in sozialen Netzwerken

Auch im Umgang mit sozialen Netzwerken für berufliche Zwecke können Risiken für die Vertraulichkeit personenbezogener oder betriebsinterner Daten einhergehen. Dies betrifft beispielsweise Beschäftigte, die die Social-Media-Accounts des Verantwortlichen verwalten und mit Inhalten pflegen. Bitte beachten Sie dabei die folgenden Punkte:

- Die Verwendung eines sozialen Netzwerks erfordert zwingend eine Rechtsgrundlage. Möchten Sie eine neue soziale Plattform verwenden, informieren Sie sich vorab bei Ihrem Datenschutzbeauftragten und berücksichtigen die Inhalte der Richtlinie zur Dienstleistersteuerung.
- Veröffentlichen Sie keine personenbezogenen Daten von Mitarbeitern, Studierenden und anderen natürlichen Personen ohne deren ausdrückliche, schriftliche Einwilligung. Im Zuge der Einwilligungserklärung muss zudem die Informationspflicht über den Zweck und die Verwendung der Daten erfolgen. Die Einwilligung muss freiwillig erfolgen und muss jederzeit widerrufen werden können.
- Verweisen Sie innerhalb des beruflichen Social Media Profils auf die Datenschutzerklärung Ihrer Institution.
- Überprüfen Sie die Rechte des Verantwortlichen an Bildern, Musikstücken oder Videos vor ihrer Verwendung.
- Pflegen Sie die Vertraulichkeitseinstellungen des Nutzerprofils sorgfältig und überprüfen Sie diese laufend.

5 Konsequenzen bei Nichtbeachtung

Verhalten, das den Grundsätzen dieses Leitfadens zum Datenschutz und zur Verarbeitung personenbezogener Daten widerspricht, kann disziplinar- bzw. arbeitsrechtliche Folgen nach sich ziehen. Grob fahrlässige oder vorsätzliche Verstöße können zu finanziellen Schäden und damit zu Regressforderungen bzw. gegebenenfalls auch zu strafrechtlichen Konsequenzen führen.

Verstöße gegen den Datenschutz sind unverzüglich dem zuständigen Datenschutzbeauftragten (datenschutz@uni-passau.de) zu melden.

6 FAQ

Im universitären Kontext finden vielfältige Verarbeitungen personenbezogener Daten statt. Im Folgenden sollen zunächst die wichtigsten Anwendungsfälle, deren zugrundeliegenden Rechtsvorschriften sowie der richtige Umgang mit diesen kurz erläutert werden:

6.1 Welche Rechtsgrundlagen bestehen für die Verarbeitung personenbezogener Daten?

Werden personenbezogene Daten erhoben oder anderweitig verarbeitet, ist stets das Vorliegen einer Rechtsgrundlage in Bezug auf die Datenverarbeitung zu überprüfen. Dabei kommen im Hochschulkontext folgende Rechtsgrundlagen in Betracht:

- Verarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, Art. 6 Abs. 1 lit. e DSGVO.
- Verarbeitung zur Erfüllung eines Vertrages, Art. 6 Abs. 1 lit. b DSGVO.
- nachrangig die Verarbeitung aufgrund einer erteilten Einwilligung der betroffenen Person, Art. 6 Abs. 1 lit. a DSGVO.

Bitte beachten Sie, dass eine Verarbeitung personenbezogener Daten nur mit Vorliegen einer entsprechenden Rechtsgrundlage zulässig ist.

Nach der Regelung des Bayerischen Datenschutzgesetzes, Art. 4 Abs. 1 BayDSG 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.

Das Bayerische Hochschulinnovationsgesetz weist den Universitäten in Art. 2 BayHIG 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 Nachwuchses.
- Die wissenschaftliche Betreuung Promovierender.
- Die soziale Förderung Studierender.
- Zusammenwirken mit Wirtschaft und beruflicher Praxis und Förderung des Wissens- und Technologietransfers 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.

Nachrangig zu einer Datenverarbeitung zur Erfüllung einer Aufgabe kommt als weitere Rechtsgrundlage für die Verarbeitung personenbezogener Daten Studierender die Einwilligung des Betroffenen in Betracht. Im Rahmen der Einholung einer Einwilligung ist stets zu gewährleisten, dass die Voraussetzungen für eine wirksame Einwilligung tatsächlich vorliegen.

6.2 Wir werden die Informationspflichten zum Zeitpunkt der Erhebung personenbezogener Daten erfüllt?

Zum Zeitpunkt der Erhebung personenbezogener Daten ist der Betroffene über die konkrete Verarbeitung seiner personenbezogenen Daten zu informieren. Eine Mitteilung pauschaler Informationen ohne konkreten Bezug zur jeweiligen Datenverarbeitung erfüllt nicht die datenschutzrechtlichen Anforderungen an die Einhaltung der Informationspflicht. Konkret ist der Betroffene zu informieren über:

- den Verantwortlichen für die Datenverarbeitung samt Kontaktdaten
- den Datenschutzbeauftragten des Verantwortlichen samt Kontaktdaten
- den Zweck und die Rechtsgrundlage der Datenverarbeitung
- ggf. die Empfänger der personenbezogenen Daten
- ggf. die Übermittlung personenbezogener Daten an ein Drittland
- die Dauer der Speicherung bzw. die Kriterien für die Speicherdauer und Überprüfungsfristen
- die Betroffenenrechte
- das Beschwerderecht bei einer Aufsichtsbehörde

Werden personenbezogene Daten nicht direkt bei dem Betroffenen selbst erhoben, handelt es sich um eine Dritterhebung gem. Art. 14 Abs. 1 DSGVO (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 Betroffene aber zudem darüber zu informieren, aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen.

Die DSGVO selbst nennt eine Beschränkung der Informationspflicht in Art. 13 Abs. 4 DSGVO, Art. 14 Abs. 5 lit. a DSGVO 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 jeweiligen Studierenden zuordnen zu können.

6.3 Wie wird die Dokumentationspflicht bei der Verarbeitung personenbezogener Daten erfüllt?

Aus Art. 33 Abs. 2 DSGVO erfolgt eine Dokumentationspflicht über die Einhaltung der zentralen Grundsätze der DSGVO. Diese Einhaltung muss nachgewiesen werden können. Insoweit folgt aus den Normen der DSGVO in Art. 5 Abs. 2 DSGVO auch eine Dokumentationspflicht über die Einhaltung der zentralen Grundsätze. Dazu sind folgende Punkte festzuhalten:

- Wann, wo und wie ein Kontakt hergestellt worden ist,
- Auf welcher Rechtsgrundlage sowie zu welchem Zweck personenbezogene Daten verarbeitet werden,
- Dass dem Betroffenen die erforderlichen Informationen erteilt wurden.

Nur wenn eine schriftliche Dokumentation dieser Punkte vorliegt, kann die Nachweispflicht erfüllt werden. Daher sollten bspw. Einwilligungen in die Datenverarbeitung in Schriftform eingeholt werden.

6.4 Was ist für die Dokumentation der Datenverarbeitungsvorgänge zu beachten?

Zur Dokumentation der stattfindenden Datenverarbeitungsvorgänge ist an der Universität Passau ein Verarbeitungsverzeichnis (VVT) nach Art. 30 Abs. 1 DSGVO zu führen.

Die einzelnen Datenverarbeitungsvorgänge sind hierbei mithilfe von Verfahrensbeschreibungen abzubilden, welche anschließend gebündelt im Verarbeitungsverzeichnis zusammengeführt werden. Die Verfahrensbeschreibungen haben dabei folgende Angaben zu beinhalten:

- Namen und Kontaktdaten des 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 (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, EXA-Management/HISinOne oder aber auch zu dem Forschungsinformationssystem FIS.

Die Rückmeldung der einzelnen Verarbeitungsvorgänge kann dabei über das [„Formular zur Übersicht der zur Verarbeitung personenbezogener Daten“](#) genutzten automatisierten Verfahren erfolgen.

6.5 Wann liegen personenbezogene Daten von Studierenden vor?

Eine Verarbeitung personenbezogener Daten Studierender findet insbesondere statt bei:

- 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

6.6 Was ist bei einer Übermittlung von Prüfungsleistungen an andere Organisationseinheiten 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 Verantwortlichen in Betracht, und zwar immer dann, soweit voneinander abgrenzbare Bereiche von gewisser Eigenständigkeit vorliegen.

Hier ist insbesondere auf den Schutz vor einer unberechtigten Kenntnisnahme zu achten. Bitte nutzen Sie daher sichere Kommunikationswege.

6.7 Was gilt für die Bekanntgabe von Prüfungsleistungen an Studierende?

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.

6.8 Was gilt für Aufbewahrungs-/Speicherdauer gesammelter Datensätze?

Sämtliche gesammelten Datensätze (hierzu zählt auch der Schriftverkehr via E-Mail) sowie Schriftgut in Papierform (bspw. Prüfungsakten) sind nur so lange 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. Bitte informieren Sie sich hierzu auch unter dem Punkt 4.9 zur Entsorgung von Datenträgern und Dokumenten.

6.9 Was ist im Umgang mit Kontaktdaten zu beachten?

Die Verarbeitung von Kontaktdaten ist nur dann zulässig, wenn eine entsprechende Rechtsgrundlage vorliegt. Häufig kommt hier die Aufgabenerfüllung in Betracht, Art. 6 Abs. 1 lit. e DSGVO i.V.m. Art. 4 Abs. 1 BayDSG, soweit die Verarbeitung von Kontaktdaten zur Erfüllung einer universitären Aufgabe erforderlich ist. 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 weitere den Universitäten durch das Bayerische Hochschulgesetz zugewiesene Aufgabe, geschehen.

Der aus DSGVO und Bayerischem Datenschutzgesetz (BayDSG) folgende Erforderlichkeitsmaßstab begrenzt wiederum den Anwendungsbereich einer rechtmäßigen Datenverarbeitung zur Aufgabenerfüllung. Eine Verarbeitung der Kontaktdaten ist allerdings aufgrund des Merkmals der Erforderlichkeit 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, Art. 6 Abs. 1 lit. b DSGVO 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. Im Rahmen von Vertragsverhandlungen ist es erforderlich, dass diese auf Anfrage der betreffenden Person erfolgen, nicht jedoch, dass es im Nachgang tatsächlich zu einem Vertragsabschluss kommt.

Kommt eine Datenverarbeitung weder unter dem Gesichtspunkt der Aufgabenerfüllung noch zur Vertragserfüllung in Betracht, so sollte eine Einwilligung der betroffenen Personen für eine rechtmäßige Datenverarbeitung eingeholt werden.

6.10 Wann ist eine Veröffentlichung von Kontaktdaten zulässig?

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

6.11 Wie ist die Verwaltung von Adresslisten, insbesondere in Bezug auf „Altkontakte“, zu handhaben?

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.

Beruhet die Datenverarbeitung bspw. auf einer Einwilligung des 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 genügt. Für den Umgang mit „Altkontakten“ gem. Art. 6 Abs. 1 lit. e DSGVO, Art. 4 Abs. 1 BayDSG i.V.m. Art. 2 BayHIG 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.

6.12 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. 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. 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, Art. 6 Abs. 4 i.V.m. Art. 23 DSGVO, 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, Art. 6 Abs. 2 Nr. 1 BayDSG 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. Dies ergibt sich aus Art. 13 Abs. 3 DSGVO für die Direkterhebung und Art. 14 Abs. 4 im Falle der Dritterhebung.

Beispielformulierung: 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).

6.13 Was ist bei der 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, 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.

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 offenstehen 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 in Betracht.

6.14 Wie ist der korrekte Umgang mit Kontaktdaten bei Veranstaltungen?

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 Betroffenen, da dieser durch sein Verhalten zum Ausdruck bringt, dass er eine Kontaktaufnahme im Nachgang der Veranstaltung wünscht, auch wenn dies nicht ausdrücklich so kommuniziert wird.

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.

6.15 Wie ist der korrekte Umgang mit Fotoaufnahmen bei Veranstaltungen?

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. 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 auf Foto-/Videoaufnahmen einer Rechtsgrundlage. Als mögliche Rechtsgrundlage kommt dabei die Erfüllung der

Öffentlichkeitsarbeit (Gesamtschau von Art. 6 Abs. 1 lit. e DSGVO, Art. 4 Abs. 1 BayDSG i.V.m. Art. 2 BayHIG), als weitere den staatlichen Hochschulen durch das BayHIG zugewiesene Aufgabe, soweit diese in Form von Bildberichterstattung auch erforderlich ist, in Betracht. 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 Öffentlichkeitsarbeit erforderlich ist. So ist es beispielsweise evtl. nicht erforderlich, eine weltweite Öffentlichkeit durch Veröffentlichung der Aufnahmen im Internet herzustellen.

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

Folgende Punkte sollten beachtet werden:

- 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 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 „aufnahme-freien Bereich“ für diejenigen Veranstaltungsteilnehmer 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.

6.16 Was ist beim Umgang mit personenbezogenen Daten von 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.

Auch bei Anträgen auf Einstellung von studentischen Hilfskräften, oder aber auch wissenschaftlichen Mitarbeitern findet eine datenschutzrechtlich relevante Verarbeitungstätigkeit statt, da die Antragsformulare mit personenbezogenen Daten wie bspw. Namen oder Geburtsdatum zu befüllen sind. Hierbei ist darauf zu achten, dass nur die erforderlichen Daten verarbeitet und diese in Übereinstimmung mit den geltenden Datenschutzbestimmungen geschützt und gespeichert werden.

6.17 Was ist beim Führen von Geburtstagslisten zu beachten?

Das Führen von Geburtstagslisten bspw. innerhalb einer Abteilung/Einrichtung bedarf der Einwilligung jedes einzelnen Mitarbeiters. 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 jeweilige Betroffene selbst sein Geburtsdatum in den Kalender einträgt.

6.18 Was ist beim Führen von internen Abwesenheitskalendern zu beachten?

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 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.

6.19 Welche Vorlage für Einwilligungserklärung und Datenschutzhinweis ist zu verwenden, und wo finde ich diese?

Eine aktuelle Vorlage für Einwilligungserklärungen sowie die entsprechenden Datenschutzinformationen gemäß Art. 13, 14 DSGVO finden Sie unter [hier](#).

A.1 Grundsätze für die Verarbeitung personenbezogener Daten

In Artikel 5 der Datenschutz-Grundverordnung ist ein Katalog von Grundsätzen für die Verarbeitung von personenbezogenen Daten enthalten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- festgelegte, eindeutige Zweckbindung
- Datenminimierung
- Richtigkeit
- Integrität und Vertraulichkeit

Diese bilden eine Art Leitlinie, wie das Datenschutzrecht bei Auslegungs- und Entscheidungsspielräumen anzuwenden ist.

1. **Rechtmäßigkeit (Art. 5 Abs. 1 lit. a DSGVO)**

Daten müssen danach „auf rechtmäßige Weise“ verarbeitet werden. Art. 8 Abs. 2 S. 1 GRCh verbietet die Verarbeitung von personenbezogenen Daten, außer es liegt eine Einwilligung oder eine andere gesetzlich geregelte legitime Grundlage vor. Diese Angaben zur Rechtmäßigkeit werden in Art. 6 DSGVO noch konkretisiert.

2. **Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a DSGVO)**

Art. 5 Abs. 1 lit. a DSGVO konkretisiert die Pflicht einer Verarbeitung nach Treu und Glauben aus Art. 8 Abs. 1 GRCh. Es soll gewährleistet werden, dass der Verantwortliche bei der Verarbeitung personenbezogener Daten die Interessen der Betroffenen angemessen berücksichtigt.

3. **Transparenz (Art. 5 Abs. 1 lit. a DSGVO)**

Der Grundsatz der Transparenz wird ebenso durch Art. 5 Abs. 1 lit. a DSGVO gewährleistet. Die Verarbeitung muss danach in einer für den Betroffenen nachvollziehbaren Weise erfolgen.

4. **Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)**

Der Grundsatz der Zweckbindung wird in Art. 5 Abs. 1 lit. b DSGVO geregelt. Bei Universitäten ist die Zweckbindung dementsprechend zu verstehen, dass Daten für den Zweck verarbeitet werden dürfen, für den sie rechtmäßig erhoben wurden.

Eine Weiterverarbeitung zu anderen Zwecken würde eine neue Rechtfertigung benötigen. Bei Verarbeitung im privaten Interesse ist die Verarbeitung zu einem anderen Zweck grundsätzlich verboten, wenn sie mit dem ursprünglichen Erhebungszweck unvereinbar ist. Dieses Prinzip findet eine Konkretisierung in Art. 6 Abs. 4 DSGVO, sodass Verarbeitungen, welche einen anderen Zweck als den ursprünglichen verfolgen, nur unter den Voraussetzungen des Art. 6 Abs. 4 DSGVO zulässig sind.

Daraus folgt auch, dass die zulässigen Verarbeitungszwecke bereits vor der ersten Verarbeitung eindeutig festgelegt werden müssen.

5. **Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)**

Personenbezogene Daten dürfen nach Art. 5 Abs. 1 lit. c DSGVO nur verarbeitet werden, soweit dies für einen legitimen Verarbeitungszweck angemessen und erheblich ist. Dabei muss die Verarbeitung auf das für den Zweck erforderliche Maß beschränkt sein. Dies gilt insbesondere personenbezogene Daten, die die Identifizierung einer natürlichen Person ermöglichen.

6. **Richtigkeit und Aktualität (Art. 5 Abs. 1 lit. d DSGVO)**

Art. 5 Abs. 1 lit. d DSGVO verpflichtet den Verantwortlichen zur Qualitätssicherung hinsichtlich der verarbeiteten personenbezogenen Daten. Dieser Grundsatz wird nochmals durch Art. 16 DSGVO konkretisiert, der einen Berichtigungsanspruch enthält.

7. **Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)**

Personenbezogene Daten dürfen nach Art. 5 Abs. 1 lit. e DSGVO grundsätzlich nur solange gespeichert werden, wie dies für den jeweiligen Verarbeitungszweck erforderlich ist. In Erwägungsgrund 39 DSGVO wird darauf hingewiesen, dass Verantwortliche regelmäßige Löscho- und Speicherfristen überprüfen sollten.

8. Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO)

Die Grundsätze der Integrität und Vertraulichkeit der Verarbeitung aus Art. 5 Abs. 1 lit. f DSGVO werden in Art. 24 ff. DSGVO, insbesondere durch Art. 25 und Art. 32 DSGVO ausgeformt.

9. Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)

Die Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO besagt, dass der Verantwortliche dazu in der Lage sein muss, die Einhaltung der Datenschutz-Grundsätze nachweisen zu können. Dafür müssen Dokumentationspflichten vom Verantwortlichen erfüllt werden, wie sie beispielsweise im Verzeichnis der Verarbeitungstätigkeiten oder der Datenschutz-Folgeabschätzung aufgegeben sind.

10. Besonderer Schutz sensibler Daten

In Art. 9 DSGVO wird die Verarbeitung besonderer Kategorien an personenbezogenen Daten geregelt („sensible Daten“). Im Zusammenhang mit diesen Daten könnten besondere Risiken für die Grundrechte und Grundfreiheiten entstehen. Die Verarbeitung ist deshalb grundsätzlich verboten. Die Risiken der Verarbeitung hängen oftmals vom Verwendungszusammenhang ab. Es gibt außerdem triftige Gründe, aus denen diese Daten trotz des Risikos verarbeitet werden müssen (Gründe in Art. 9 Abs. 2, 3, 4 DSGVO durchbrochen).

Art. 10 DSGVO sieht wiederum eher einen organisatorisch-verfahrensrechtlichen Schutz für Daten wie Strafverurteilungen an, indem die Verarbeitung grundsätzlich unter behördliche Aufsicht gestellt wird.