Datenschutzrichtlinie

der

Hochschülerinnen- und Hochschülerschaft an der FH JOANNEUM

Hochschülerinnen- und Hochschülerschaft an der FH JOANNEUM
„öh joanneum“
Eggenberger Allee 11
8020 Graz

Inhaltsverzeichnis

1. Einleitung und Zielsetzung

In dieser Datenschutzrichtlinie sind die Grundsätze, die bei der Verarbeitung von personenbezogenen Daten durch den Verantwortlichen zu beachten sind, festgeschrieben, wobei geltendes Recht dieser Datenschutzrichtlinie vorgeht.

Verantwortlicher ist entweder die Bundesvertretung der Österreichischen Hochschüler- und Hochschülerinnenschaft oder die Hochschulvertretung an der jeweiligen Hochschule, die eigene Rechtspersönlichkeit besitzt, sofern diese Richtlinie kundgemacht wurde.

Adressat_innen sind die einzelnen Studierendenvertreter_innen, Beschäftigten sowie ehrenamtlich tätigen Personen (im Folgenden kurz: Mitarbeiter_innen), denen es insbesondere untersagt ist, personenbezogene Daten unbefugt zu erheben, zu verarbeiten, zu übermitteln oder auf andere Weise zu nutzen.

Diese Datenschutzrichtlinie gilt für die Verarbeitungen personenbezogener Daten von natürlichen Personen. Anonymisierte Daten (das sind Daten, die keiner Person zugeordnet werden können), z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzrichtlinie.

2. Anwendungsbereich

Die Datenschutzrichtlinie gilt für alle Arten der Verwendung von personenbezogenen Daten des Verantwortlichen, unabhängig vom Ort ihrer Erhebung. Personenbezogene Daten können vom Verantwortlichen insbesondere (aber nicht ausschließlich) zu folgenden Zwecken verwendet werden:

a Zur Verwaltung von Studierendendaten durch den Verantwortlichen;

b Zur Verwaltung von Mitarbeiter_innendaten;

c Zur Anbahnung, Durchführung und Abwicklung von Verträgen mit Bildungseinrichtungen, Lieferant_innen und anderen Dienstleister_innen des Verantwortlichen im Rahmen der Erbringung von Leistungen;

d Zum ordnungsgemäßen Umgang mit sonstigen Dritten sowie zur Erfüllung zwingender gesetzlicher Vorschriften.

3. Datenschutzorganisation

3.1 Allgemeines zur Datenschutzorganisation

Der/die Vorsitzende des jeweiligen Verantwortlichen hat dafür Sorge zu tragen, dass die Bestimmungen dieser Datenschutzrichtlinie umgesetzt werden. Der/die Vorsitzende des jeweiligen Verantwortlichen hat zu diesem Zwecke eine/n Datenschutzbeauftragte_n zu bestellen.

Der/die Vorsitzende der Bundesvertretung der Österreichischen Hochschüler- und Hochschülerinnenschaft kann für lokale Hochschüler_innenvertretungen an Hochschulen ohne

Rechtspersönlichkeit Datenschutzkoordinatoren_innen benennen. Solange der/die Vorsitzende keine/n Datenschutzkoordinator_in benannt hat, ist der/die Vorsitzende der/die Datenschutzkoordinator_in.

3.1.1 Datenschutzbeauftragte

Die/der Datenschutzbeauftragte untersteht in dieser Funktion direkt der/dem Vorsitzenden des Verantwortlichen.

Der Verantwortliche stellt sicher, dass die/der Datenschutzbeauftragte die erforderlichen Kompetenzen zur rechtlichen, technischen und organisatorischen Bewertung und Durchführung von datenschutzrelevanten Maßnahmen hat. Sofern die/der Datenschutzbeauftragte als Referent_in, Sachbearbeiter_in oder Angestellte_r des Verantwortlichen bestellt wird, sind zusätzlich die jeweiligen Bestellungs- bzw Wahlvoraussetzungen nach HSG und Satzung einzuhalten.

Die/der Datenschutzbeauftragte hat die Einhaltung des Datenschutzes stichprobenartig laufend zu überprüfen. Die Überprüfungen sind zu dokumentieren.

Weitere Aufgaben des/der Datenschutzbeauftragten:

a Überwachung der Einhaltung der DSGVO und anderer nationaler und europäischer Datenschutzvorschriften;

b Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter_innen;

c Zusammenarbeit mit der Aufsichtsbehörde.

Die/der Datenschutzbeauftragte ist berechtigt, zur operativen Durchführung bzw zu seiner Vertretung geeignete Mitarbeiter_innen zu beauftragen.

Die/der Datenschutzbeauftrage erstellt einmal jährlich einen zusammenfassenden Bericht für die/den Vorsitzende_n des Verantwortlichen betreffend datenschutzrechtliche Themen des vorangehenden Geschäftsjahrs.

Der/die Datenschutzbeauftragte koordiniert die Zusammenarbeit und Abstimmung zu allen wichtigen Fragen des Datenschutzes. Er/Sie informiert bei Bedarf den/die Vorsitzende_n zu den aktuellen Entwicklungen oder formuliert Empfehlungen.

3.1.2 Datenschutzkoordinator_innen

Der/die Datenschutzkoordinator_in untersteht in dieser Funktion direkt dem/der Vorsitzenden der Bundesvertretung der Österreichischen Hochschülerinnen- und Hochschülerschaft.

Vor der Bestellung einer/eines Datenschutzkoordinators_in ist die/der Datenschutzbeauftragte von der/vom Vorsitzenden zu konsultieren.

Der Verantwortliche stellt sicher, dass die/der Datenschutzkoordinator_in die erforderlichen

Kompetenzen zur rechtlichen, technischen und organisatorischen Bewertung und Durchführung von datenschutzrelevanten Maßnahmen hat.

Der/dem Datenschutzkoordinator_in obliegt die Umsetzung der Vorgaben der/des Datenschutzbeauftragten. Der/dem Datenschutzkoordinator_in sind bereits im Planungsstadium Projekte zur Kenntnis zu bringen, die eine Verarbeitung personenbezogener Daten erfordern können. Fragen von grundsätzlicher Bedeutung sind jedenfalls mit der/dem Datenschutzbeauftragten abzustimmen.

Die/der Datenschutzkoordinator_in hat im Einvernehmen mit der/dem Datenschutzbeauftragten die Einhaltung des Datenschutzes stichprobenartig laufend zu überprüfen. Die Überprüfungen sind zu dokumentieren.

Weitere Aufgaben des/der Datenschutzkoordinators_in:

a Lokale_r Ansprechpartner_in für Mitarbeiter_innen;

b Mitwirkung und Unterstützung bei der datenschutzkonformen Gestaltung von Vorhaben, Verträgen und Projekten;

c Kontrolle der rechtmäßigen Datenverarbeitung;

d Unterstützende_r Ansprechpartner_in für den/die Datenschutzbeauftragten gegenüber nationalen Datenschutzbehörden;

e Unterstützung bei Schulungen der mit personenbezogenen Daten arbeitenden Mitarbeiter_innen der Referate;

f Sonstige in dieser Datenschutzrichtlinie genannte Aufgaben.

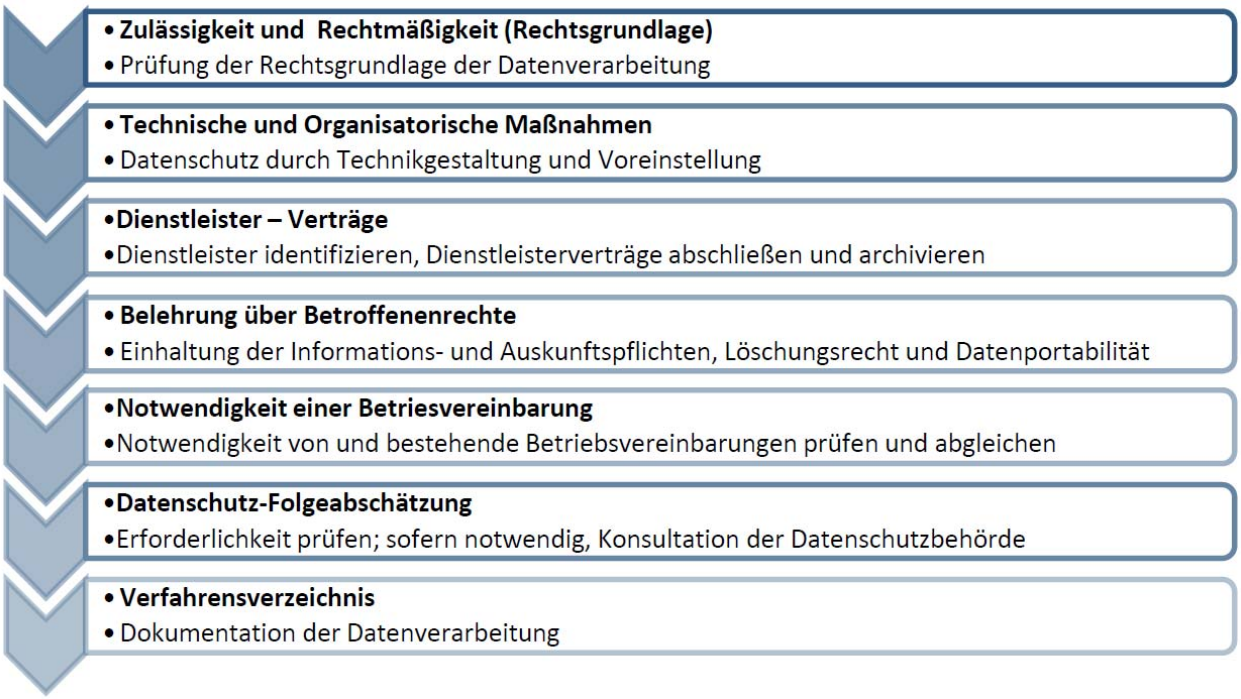
Der/die Datenschutzkoordinator_in berichtet anlassbezogen an den Verantwortlichen. Einmal jährlich erfolgt ein zusammenfassender Bericht durch den/die Datenschutzkoordinator_in an den Verantwortlichen betreffend die datenschutzrechtlichen Themen aus dem vorangehenden Jahr.

Zur Gewährleistung der einheitlichen Umsetzung der datenschutzrechtlichen Vorgaben stehen der/die Datenschutzkoordinator_in in enger Abstimmung zueinander und mit dem/der Datenschutzbeauftragten.

3.2 Implementierung neuer Datenverarbeitungen oder Erweiterung bestehender Datenverarbeitungen

Der/die Datenschutzbeauftragte oder der/die Datenschutzkoordinator_in unterstützt den Verantwortlichen bei Entwicklungen zur IT-Infrastruktur, zur Netzinfrastruktur, Vorhaben, bei denen personenbezogene Daten verarbeitet werden. Der/die Datenschutzbeauftragte oder der/die Datenschutzkoordinator_in ist bei neuen Entwicklungen frühestmöglich zu beteiligen, um sicherzustellen, dass jegliche Datenschutzbelange berücksichtigt und bewertet werden.

Schritte zur Implementierung von Datenverarbeitungen:



3.3 Überprüfungen des Datenschutzniveaus

Überprüfungen der Einhaltung der Vorgaben dieser Datenschutzrichtlinie und des sich daraus abzuleitenden Datenschutzniveaus erfolgen durch Kontrollen, die von der/vom Datenschutzbeauftragten anhand eines jährlichen Kontrollplans durchgeführt werden, sowie durch andere Maßnahmen wie etwa Kontrollen der Datenschutzkoordinator_innen oder Reports.

Die Kontrollen des/der Datenschutzbeauftragten werden durch interne oder externe Auditoren durchgeführt. Darüber hinaus werden regelmäßige Self-Assessment Verfahren durch den Verantwortlichen durchgeführt und von der/vom Datenschutzbeauftragten koordiniert. Die Ergebnisse wesentlicher Kontrollen sowie die dazu vereinbarten Maßnahmen werden dem/der Vorsitzenden des Verantwortlichen mitgeteilt. Die zuständige Aufsichtsbehörde kann auf Nachfrage eine Kopie des Kontrollergebnisses erhalten. Zudem kann die für einen Verantwortlichen zuständige Aufsichtsbehörde auch eine Kontrollmaßnahme anstoßen. Diese Kontrollmaßnahmen werden vom jeweiligen Verantwortlichen bestmöglich unterstützt und die daraus abgeleiteten Maßnahmen werden umgesetzt.

Werden im Rahmen einer Kontrolle Schwachstellen festgestellt, sind diese durch entsprechende Maßnahmen durch den jeweiligen Verantwortlichen zu beheben. Der/die Datenschutzbeauftragte verfolgt die Umsetzung der Maßnahmen. Sollten diese ohne ausreichende Begründung nicht umgesetzt werden, bewertet der/die Datenschutzbeauftragte die Auswirkungen auf den Datenschutz und leitet die notwendigen Konsequenzen und gegebenenfalls

Sofortmaßnahmen ein und informiert den/die Vorsitzende_n des Verantwortlichen.

Sofern keine gesetzlichen Beschränkungen bestehen, sind der/die Datenschutzbeauftragte befugt, die ordnungsgemäße Verarbeitung von personenbezogenen Daten zu überprüfen. Dazu gewährt der Verantwortliche umfassend Zutritt und Einsicht zu den Informationen, die der/die Datenschutzbeauftragte zur Aufklärung und Bewertung des Sachverhalts für notwendig erachten.

3.4 Mitarbeiter_innenverpflichtung und Schulung

Der Verantwortliche verpflichtet seine Mitarbeiter_innen spätestens bei Aufnahme der Tätigkeit auf das Daten- und Fernmeldegeheimnis. Im Rahmen der Verpflichtung werden die Mitarbeiter_innen ausreichend auf die Belange des Datenschutzes geschult.

Die Mitarbeiter_innen werden regelmäßig auf die Grundlagen im Datenschutz geschult. Je nach Bedarf und Angemessenheit werden die Datenschutzkoordinator_innen und der/die Datenschutzbeauftragte in den Referaten Schulungen durchführen.

3.5 Zuständige Stellen für Kontakte und Anfragen

Zuständige Stelle für Kontakte und Anfragen zu dieser Datenschutzrichtlinie sind die Datenschutzbeauftragten oder die Datenschutzkoordinatoren_innen.

4. Prinzipien für die Verarbeitung personenbezogener Daten

Jede Verarbeitung personenbezogener Daten hat zum Schutz der Rechte, insbesondere dem Recht auf die Privatsphäre, und Freiheiten der betroffenen Personen nach untenstehenden Grundsätzen zu erfolgen. Bei der Konzipierung neuer Datenverarbeitungen und Erweiterung bestehender Datenverarbeitungen werden die unten angeführten Prinzipien beachtet.

4.1 Transparenzprinzip

Die personenbezogenen Daten sind grundsätzlich bei dem/der Betroffenen selbst zu erheben. Um dem Transparenzprinzip Rechnung zu tragen, treffen den Verantwortlichen Informations- und Auskunftspflichten. Bei Verarbeitungen von personenbezogenen Daten muss der/die Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden:

- Identität des/der Verantwortlichen (d. h. wer bestimmt die Mittel und Zwecke der Verarbeitung);
- Zweck(e) und Rechtsgrundlage(n) der Verarbeitung; ggf. die berechtigten Interessen, die mit der Datenverarbeitung verfolgt werden;
- Empfänger_in, an welche die Daten gegebenenfalls weitergegeben werden (auch andere Hochschülerinnen- und Hochschülerschaften fallen hierunter);
- erhobene Datenarten und -kategorien; ggf. die Rechtsgrundlage für internationale Datentransfers;

- Dauer der Datenverarbeitung; Dauer der Datenaufbewahrung; Betroffenenrechte; Beschwerderechte; ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob der Betroffene verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte; automatisierte Entscheidungen.

Die Informationen müssen den Betroffenen bei der Erhebung der Daten sowie danach stets bei Bedarf zur Verfügung stehen.

4.2 Zulässigkeitsvoraussetzung für die Verarbeitung von personenbezogenen Daten

Grundsätzlich ist jede Verarbeitung von personenbezogenen Daten verboten, außer es gibt einen Erlaubnistatbestand. Eine Ausnahme besteht etwa dann, wenn es eine ausdrückliche gesetzliche Regelung dafür gibt oder die Betroffenen in die Verarbeitung ihrer personenbezogenen Daten eingewilligt haben (Rechtfertigung/Erlaubnistatbestand). Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck einer Datenverarbeitung gegenüber der ursprünglichen Zweckbestimmung geändert werden soll. Die Verwendung von bereits erhobenen Daten für andere Zwecke ist nur zulässig, wenn dafür die Zulässigkeitsvoraussetzungen nach Maßgabe der unten angeführten Bestimmungen vorliegen. Erlaubnistatbestände bzw. Rechtfertigungen für eine Verarbeitung personenbezogener Daten sind:

4.2.1 Überwiegende berechtigte Interessen

Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn dies zur Verwirklichung eines berechtigten Interesses des/der Verantwortlichen oder eines Dritten erforderlich ist und schutzwürdige Interessen des/der Betroffenen nicht überwiegen.

Berechtigte Interessen können beispielsweise das Geltendmachen, die Ausübung und Verteidigung rechtlicher Ansprüche, Betrugsbekämpfung, etc. sein.

4.2.2 Erfüllung vertraglicher Verpflichtungen

Die Verarbeitung ist zulässig, sofern sie für die Erfüllung eines Vertrags, dessen Vertragspartei der/die Betroffene ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des/der Betroffenen erfolgen, erforderlich ist.

Bei Verträgen bei denen der Widerruf dazu führt, dass vertragliche Pflichten nicht mehr erfüllt werden können, ist der/die Betroffene darüber zu informieren.

4.2.3 Zustimmungserklärung (Einwilligung des/der Betroffenen)

Die Verarbeitung personenbezogener Daten ist zulässig, wenn eine rechtsgültige Einwilligung der/des Betroffenen zur konkreten Verarbeitung eingeholt wurde.

Einwilligungserklärungen sind aus Beweisgründen schriftlich einzuholen und aufzubewahren.

4.2.4 Gesetze, Verordnungen oder sonstige verbindliche Normen

Die Verarbeitung von personenbezogenen Daten ist auch dann zulässig, wenn dies zur Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt, erforderlich ist.

Darüber hinaus ist die Verarbeitung von personenbezogenen Daten zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde, rechtmäßig.

4.2.5 Lebenswichtige Interessen des/der Betroffenen

Eine Verarbeitung ist weiters gestattet, um lebenswichtige Interessen des/der Betroffenen oder einer anderen natürlichen Person zu schützen.

4.2.6 Verarbeitung sensibler Daten (besondere Kategorien von Daten und Daten mit strafrechtlichem Bezug)

Die Verarbeitung besonderer Kategorien von personenbezogenen Daten (z.B. Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, Gesundheitsdaten, etc.) darf nur sehr eingeschränkt erfolgen, z.B. wenn dies gesetzlich erforderlich ist, der/die Betroffene ausdrücklich eingewilligt hat oder zum Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin für die Beurteilung der Arbeitsfähigkeit erforderlich ist.

Vor Beginn einer solchen Erhebung, Verarbeitung oder Nutzung sensibler Daten ist der/die Datenschutzbeauftragte oder der/die Datenschutzkoordinator_in zu konsultieren.

4.3 Zweckbindungs- und Wesentlichkeitsprinzip

Jeder Verarbeitung von personenbezogenen Daten muss ein bestimmter legitimer Zweck zugrunde liegen. Die Verarbeitung darf nicht in einer mit den festgelegten Zwecken unvereinbaren Weise erfolgen. Personenbezogene Daten dürfen nur für die Zwecke verwendet werden, für die sie ursprünglich erhoben wurden. Die Verwendung von bereits erhobenen Daten für andere Zwecke ist nur dann zulässig, wenn dafür die Zulässigkeitsvoraussetzungen vorliegen.

4.4 Datenvermeidung und -sparsamkeit

Unter Datenvermeidung und Datensparsamkeit versteht man, dass nur so viele personenbezogene Daten erhoben, verarbeitet und genutzt werden sollen, wie zur Erreichung des angestrebten, legitimen Zwecks erforderlich sind.

Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder pseudonymisierte personenbezogene Daten zu verwenden.

Pseudonymisierung bedeutet, dass personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden

können.

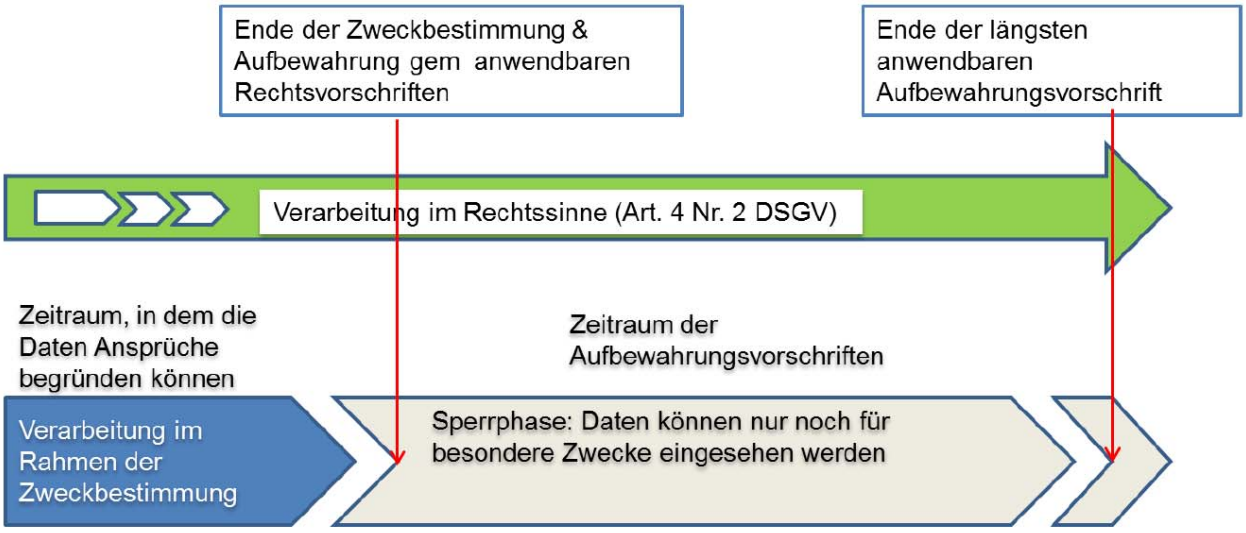
Anonymisierung bedeutet, dass sich (ursprünglich) personenbezogene Daten, nicht oder nicht mehr auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch lokales Recht vorgeschrieben oder erlaubt.

4.5 Löschen und Sperren

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder prozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Dazu ist der Verantwortliche verpflichtet für jede Verarbeitungstätigkeit entsprechende Löschkonzepte zu erarbeiten.

Personenbezogene Daten sind zu sperren, wenn der ursprüngliche Verwendungszweck erfüllt ist und (gesetzliche, vertragliche oder satzungsmäßige) Aufbewahrungsfristen anzuwenden sind. Sperren ist das kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.



4.6 Profiling und automatisierte Entscheidungen

Automatisierte Verarbeitungen von personenbezogenen Daten, durch die einzelne Persönlichkeitsmerkmale (z. B. Auswertung von Fähigkeitsprofilen oder sonstigen Auswertungen im Rahmen der Arbeitsleistung, Analyse der wirtschaftlichen Lage, etc.) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit rechtlichen Folgen oder erheblichen Beeinträchtigungen für den/die Betroffene_n sein. Dem/der Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die

Möglichkeit zu einer Stellungnahme gegeben werden. Zur Vermeidung von Fehlentscheidungen müssen die Kontrolle und eine Plausibilitätsprüfung durch eine/n Mitarbeiter_in gewährleistet werden.

4.7 Richtigkeit

Die verarbeiteten personenbezogenen Daten müssen richtig, vollständig und soweit erforderlich auf dem aktuellen Stand sein. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

4.8 Vertraulichkeit und Datensicherheit

Personenbezogene Daten unterliegen dem Datengeheimnis und sind streng vertraulich zu behandeln. Der Zugang zu personenbezogenen Daten durch Mitarbeiter_innen ist nur soweit zulässig, soweit dies zur Erfüllung der jeweiligen Aufgaben erforderlich ist („Need-to-Know-Prinzip“).

Mitarbeiter_innen dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

Mitarbeiter_innen müssen bei Beginn ihrer Tätigkeit über die Pflicht zur Wahrung des Datengeheimnisses unterrichtet werden. Diese Verpflichtung muss auch nach Beendigung des Beschäftigungsverhältnisses fortbestehen.

Bei der Verarbeitung von personenbezogenen Daten sind angemessene organisatorische und technische Maßnahmen umzusetzen, um unberechtigte Zugriffe, unrechtmäßige Verarbeitungen oder Weitergaben sowie versehentlichen Verlust, Veränderung oder Zerstörung zu verhindern. Insgesamt muss durch das Ergreifen von technischen und organisatorischen Maßnahmen ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau erreicht werden. Diese Maßnahmen haben sich am Stand der Technik, den Implementierungskosten, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren.

4.9 Internet und Telekommunikation

Werden auf Webseiten oder in Apps des Verantwortlichen personenbezogene Daten erhoben, verarbeitet und genutzt, sind die Betroffenen hierüber in Datenschutzhinweisen und gegebenenfalls Cookie-Hinweisen entsprechend zu informieren. Die Datenschutzhinweise und Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps des Verantwortlichen Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen und Cookie-Hinweisen informiert werden. Soweit erforder-

lich, ist die Einwilligung der Betroffenen vor der Erstellung von Nutzungsprofilen einzuholen.

4.10 Betroffenenrechte

Betroffene haben nicht nur das Recht auf Information über die zu ihrer Person verarbeiteten Daten, sondern auch ein Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragung und Widerspruch zur Datenverarbeitung.

Stellt eine betroffene Person ein Auskunftsbegehren an einen Verantwortlichen, unterstützt der/die Datenschutzbeauftragter_e den Verantwortlichen bei der Bearbeitung des Auskunftsbegehrens.

5. Besonderheiten bei Vertragspartner_innendaten

5.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten eines/einer Vertragspartner_in dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrags verarbeitet werden. Interessent_innen dürfen während der Vertragsanbahnung unter Verwendung der personenbezogenen Daten kontaktiert werden, die sie mitgeteilt haben. Von Interessent_innen geäußerte Einschränkungen sind dabei zu beachten.

5.2 Datenverarbeitung zu Werbezwecken

Wendet sich der/die Betroffene mit einem Informationsanliegen an einen Verantwortlichen (z. B. Wunsch nach Zusendung von Informationsmaterial), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

6. Besonderheiten bei Mitarbeiter_innendaten

6.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrags erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerber_innen verarbeitet werden. Nach Ablehnung sind die Daten des/der Bewerber_in unter Berücksichtigung von beweisrechtlichen Fristen zu löschen. In der Regel sind Bewerber_innendaten acht Monate ab dem Zeitpunkt, ab dem endgültig klar ist, dass einem/einer Bewerber_in kein Angebot gemacht wird oder dieser ein Angebot ablehnt, zu löschen. Darüber hinaus können die Daten aufbewahrt werden, sofern der/die Bewerber_in in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt hat. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren erforderlich.

6.2 Datenverarbeitung aufgrund rechtlicher Verpflichtung

Die Verarbeitung personenbezogener Mitarbeiter_innendaten ist auch dann zulässig, wenn

Rechtsvorschriften die Datenverarbeitung verlangen. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

6.3 Kontrollmaßnahmen

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiter_innendaten erfordern, dürfen nur durchgeführt werden, wenn die Menschenwürde der Mitarbeiter_innen durch die Kontrollmaßnahme nicht berührt wird, eine rechtliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Darüber hinaus sind die arbeitsrechtlichen Normen des ArbVG, AVRAG oder des BDG 1979 zu beachten.

7. Weitergabe von personenbezogenen Daten

7.1 Arten und Zwecke der Weitergabe von personenbezogenen Daten

Personenbezogene Daten können derart weitergegeben werden, dass die empfangende Stelle für die erhaltenen Daten eigenverantwortlich ist (Übermittlung), oder dass die empfangende Stelle personenbezogenen Daten nur aufgrund von Weisungen des Verantwortlichen verarbeiten darf (Auftragsverarbeitung).

7.2 Datenverarbeitung im Auftrag

Der Verantwortliche hat im Zusammenhang mit der Verarbeitung von personenbezogenen Daten die in Punkt 4 normierten Prinzipien einzuhalten. Jede Heranziehung eines Auftragsverarbeiters setzt eine schriftliche Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter voraus („Auftragsverarbeitungsvereinbarung“ oder „Data Processing Agreement“), die einen vorgegebenen Mindestinhalt regeln muss (Gegenstand und Dauer der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien der Betroffenen und die Pflichten und Rechte der Verantwortlichen und des Auftragsverarbeiters).

Ein Auftragsverarbeiter darf die ihm überlassenen personenbezogenen Daten nicht für eigene oder fremde Zwecke verwenden. Die Einbindung von sogenannten Unter- oder Subauftragsverarbeitern durch den Auftragsverarbeiter zur Erfüllung der vertraglichen Verpflichtungen (Datenverarbeitungstätigkeiten), bedarf der vorherigen Zustimmung des Verantwortlichen. Die Zustimmung kann entweder für jedes Subauftragsverarbeitungsverhältnis gesondert oder allgemein mit Information und Widerspruchsrecht des Verantwortlichen erteilt werden und ist in der Auftragsverarbeitungsvereinbarung entsprechend zu regeln. Bei der zulässigen Einbindung von Subauftragsverarbeiter hat der Auftragsverarbeiter den Subauftragsverarbeiter auf die Vereinbarungen (in Form der „Auftragsverarbeitungsvereinbarung“), die zwischen dem Auftragsverarbeiter und dem Verantwortlichen getroffen wurden, entsprechend zu verpflichten.

Die Auftragsverarbeiter sind vom Verantwortlichen sorgfältig nach deren Fähigkeit, die Datenverarbeitung im Einklang mit datenschutzrechtlichen Anforderungen zu erbringen und den Schutz der Rechte der betroffenen Personen zu gewährleisten, auszuwählen.

Trotz Abschlusses einer Auftragsverarbeitungsvereinbarung bleiben die Pflichten des Verantwortlichen unverändert aufrecht.

Nach Möglichkeit sind die zur Verfügung gestellten Muster zu verwenden. Bei nicht kritischen Datenverarbeitungstätigkeiten kann die Version „Basic“ verwendet werden. Bei heiklen Datenverarbeitungstätigkeiten, bei denen beispielsweise besondere Kategorien personenbezogener Daten, umfangreich Daten verarbeitet werden oder die überhaupt für die Verantwortlichen besondere Bedeutung haben, sind die ausführlicheren Muster, jeweils aus Sicht des Verantwortlichen bzw. des Auftragsverarbeiters, zu verwenden. Sofern ein/e Vertragspartner_in nicht dazu gebracht werden kann eines der zur Verfügung gestellten Muster zu unterschreiben, ist entweder ein anderer Auftragsverarbeiter zu suchen oder sind Vertragsverhandlungen zu führen und gegebenenfalls ist rechtsfreundliche Beratung beizuziehen.

7.3 Grenzüberschreitender Transfer personenbezogener Daten

Der Verantwortliche hat im Falle eines Transfers personenbezogener Daten in ein Drittland zu prüfen, ob ein gleichwertiges Datenschutzniveau im Drittland gewährleisten ist.

Ein geleichwertiges Datenschutzniveau ist gewährleistet, wenn:

- Der/die Empfänger_in seinen/ihren Sitz im Europäischen Wirtschaftsraum hat;
- Der/die Empfänger_in seinen/ihren Sitz in einem Land hat, welches nach Feststellung der Europäische Kommission ein angemessenes Datenschutzniveau bietet („gleichgestellte Länder“), das sind derzeit: Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Japan, Jersey, Kanada, Neuseeland, Schweiz, Uruguay
- Vereinbarung der EU-Standardvertragsklauseln in der jeweils gültigen Fassung;
- Teilnahme des/der Empfänger_in an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus (z. B.: EU-U.S. Privacy Shield).

Kann ein gleichwertiges Datenschutzniveau nicht nachgewiesen werden, ist der/die Datenschutzbeauftragte dahingehend zu konsultieren, ob kann dennoch ein Transfer personenbezogener Daten auf einen Ausnahmetatbestand gestützt werden kann.

8. Verletzung des Schutzes personenbezogener Daten („Datenschutzverletzung“)

Eine Verletzung des Schutzes personenbezogener Daten (auch „Data Breach“ genannt) sind unbeabsichtigte oder unrechtmäßige Datenvernichtungen, -verluste, -veränderungen, und -offenlegungen. Im Falle der Verletzung des Schutzes personenbezogener Daten (z.B. aufgrund eines Hackerangriffs, Verlust externer Datenträger, etc.) sind die gesetzlichen Melde- und Informationspflichten zu beachten.

Der Verantwortliche informiert den/die Datenschutzbeauftragte_n dahingehend unverzüglich. Der/die Datenschutzbeauftrager_e unterstützt den Verantwortlichen bei der weiteren Bewältigung.

Eine Datenschutzverletzung im Sinne dieser Datenschutzrichtlinie liegt unabhängig davon vor, ob die Datenschutzverletzung durch bewusste oder unbewusste Aktivitäten erfolgt ist, und unabhängig davon, ob Originaldateien oder Kopien betroffen sind.

Eine Melde- oder Informationspflicht besteht jedenfalls, wenn aufgrund der Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Dies ist beispielsweise der Fall, wenn dem/der Betroffenen ein physischer, materieller oder immaterieller Schaden entsteht, wie etwa der Verlust der Kontrolle über seine/ihre personenbezogenen Daten, Identitätsdiebstahl oder –betrug, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andre erhebliche wirtschaftliche oder gesellschaftsrechtliche Nachteile.

Der Verantwortliche prüft, inwieweit eine Meldung an die lokale Aufsichtsbehörde (Frist im Regelfall 72 Stunden ab Kenntnis der Datenschutzverletzung), an den/die Betroffene_n sowie an die Öffentlichkeit zu erfolgen hat.

9. Konsequenzen für Mitarbeiter_innen

Der/die Datenschutzbeauftragte hat den/die Vorsitzende_n zu informieren, wenn er gravierende Verstöße gegen diese Datenschutzrichtlinie durch eine/n Mitarbeiter_in des Verantwortlichen erkennt.

Im Fall eines Verstoßes gegen datenschutzrechtliche Vorschriften oder gegen Bestimmungen dieser Datenschutzrichtlinie muss jede/r Mitarbeiter_in mit disziplinären, arbeits- oder strafrechtlichen Konsequenzen rechnen.

10. Verwendete Begriffe

anonymisierte Daten	Bei anonymisierten Daten gibt es keinerlei Personenbezug. Es handelt sich dabei um Daten, bei welchen die Identität des/r Betroffenen für niemanden mehr feststellbar ist. Derartige Daten sind daher auch nicht datenschutzrelevant und unterliegen nicht dieser Datenschutzrichtlinie.
Auftragsverarbeiter	Auftragsverarbeiter (oder datenschutzrechtliche/r Dienstleister_in) ist eine natürliche oder juristische Person bzw. Personengemeinschaft, die personenbezogene Daten ausschließlich im Auftrag des Verantwortlichen verarbeitet. Als Auftragsverarbeiter sind häufig beispielsweise die IT-Dienstleister_innen zu qualifizieren. Aber auch im Falle eines Outsourcings spricht man von Auftragsverarbeitern. Zu beachten ist jedoch, dass Auftragsverarbeiter in Bezug

	auf die personenbezogenen Daten ihrer eigenen Mitarbeiter_innen, Lieferanten_innen, etc. selbst als Verantwortliche gelten.
Betroffene/r	Jede natürliche Person, über die personenbezogene Daten verarbeitet werden.
Datenverarbeitung	Unter „Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung (d.h. Erfassen, Aufnehmen oder Aufbewahren auf einem Datenträger zum Zweck der weiteren Verarbeitung und Nutzung), die Anpassung oder Veränderung (d.h. inhaltliches Umgestalten), das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung (d.h. Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, da die Daten an den Dritten weitergegeben werden oder der/die Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft), Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen (d.h. dauerhaftes Unkenntlichmachen bzw. Vernichten gespeicherter personenbezogener Daten) oder die Vernichtung zu verstehen.
personenbezogene Daten	Von den datenschutzrechtlichen Regelungen sind ausschließlich personenbezogene Daten inklusive sensible Daten (besonderer Kategorien personenbezogener Daten), welche nicht anonymisiert sind, betroffen. Erfasst sind somit alle Informationen, die sich auf eine identifizierte oder identifizierbare (natürliche) Person beziehen. Dazu gehören unter anderem: Name; Firmenname, sofern juristische Personen unter den Anwendungsbereich von Datenschutzgesetzen fallen; Geburtsdatum; Personalnummer; Private und berufliche Kontaktdaten (Adresse, Telefonnummer, Email); Familienstand; Geschlecht; Bild- und Tonaufzeichnungen (Videos, Fotos, etc.); Sensible Daten (besondere Kategorien personenbezogener Daten wie unten definiert)

Pseudonymisierte Daten	„Pseudonymisierung“ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Pseudonymisierte Daten sind vom Anwendungsbereich der datenschutzrechtlichen Vorschriften und der gegenständlichen Datenschutzrichtlinie ebenfalls erfasst.
Sensible Daten (besondere Kategorien personenbezogener Daten)	Unter „sensible Daten“ (besondere Kategorien personenbezogener Daten) sind Daten zu verstehen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Sensible Daten sind beispielsweise Religionsbekenntnis; Medizinische Diagnose; Fingerabdruck; Parteizugehörigkeit. Diese Daten gelten als besonders schutzwürdig, weswegen bei der Verarbeitung dieser Daten erhöhte Vorsicht geboten ist. Aufgrund lokalen Rechts können weitere Daten als besonders schutzwürdig eingestuft sein. So genießen Daten über strafrechtliche Verurteilungen und Straftaten vielfach einen besonderen Schutz.
Verantwortlicher	Verantwortlicher ist jene natürliche oder juristische Person bzw. Personengemeinschaft, die die Entscheidung trifft, personenbezogene Daten für einen bestimmten Zweck zu verwenden, bzw. über die Zwecke und Mittel der Verarbeitung entscheidet.

11. Inkrafttreten und Geltungsdauer

Diese Datenschutzrichtlinie tritt mit Beschlussfassung durch die Bundesvertretung oder die jeweilige lokale Hochschüler_innenvertretung sowie Kundmachung in geeigneter Form in Kraft.

Diese Datenschutzrichtlinie wird bei Bedarf aktualisiert und gegebenenfalls um spezielle Regelungen und Richtlinien ergänzt.

Die Bindungswirkung dieser Datenschutzrichtlinie endet, wenn diese mit Beschluss der Bundevertretung oder der jeweiligen lokalen Hochschüler_innenvertretung außer Kraft gesetzt wird. Die Beendigung oder Außerkraftsetzung dieser Datenschutzrichtlinie befreit den Verantwortlichen jedoch nicht von den Verpflichtungen und/oder Regelungen dieser Datenschutzrichtlinie für die Verwendung bereits übermittelter Daten.

***