Datenschutz-Richtlinie der Pädagogischen Hochschule Salzburg Stefan Zweig

Richtlinie zur EU-Datenschutzgrundverordnung der Pädagogischen Hochschule Salzburg Stefan Zweig

Inhalt

1 Präambel/Zielsetzung

Der Schutz personenbezogener Daten ist an der Pädagogischen Hochschule Salzburg Stefan Zweig (PHS) von höchster Wichtigkeit und betrifft die Handlungen aller Bediensteten der PHS in deren jeweiligem Verantwortungsbereich. Diese Richtlinie dient der internen Sicherstellung eines datenschutzkonformen Umganges mit personenbezogenen Daten im Hochschulbetrieb.

Mit 25.05.2018 tritt die europäische Datenschutzgrundverordnung (DSGVO) in Geltung. Die PHS treffen in diesem Zusammenhang umfassende Pflichten, die den Schutz von personenbezogenen Daten gewährleisten sollen. Die PHS ist insbesondere verpflichtet eine/n Datenschutzbeauftragte/n zu bestellen, ein Verzeichnis aller an der PHS durchgeführten Verarbeitungstätigkeiten (mit Ausnahme von PH-Online, wofür das bmbwf ein entsprechendes Datenverarbeitungsverzeichnis führt) zu führen, die Sicherheit der personenbezogenen Daten nach den gesetzlichen Vorgaben zu gewährleisten, die Einhaltung der Grundsätze des Datenschutzes an der PHS sicherzustellen und allen betroffenen Personen, deren personenbezogene Daten an der PH verarbeitet werden, die Ausübung ihrer Rechte auf Auskunft, Löschung, Berichtigung, Einschränkung, und Weitergabe ihrer personenbezogenen Daten sowie deren Widerspruchsrecht gegen bestimmte Datenverarbeitungen (Art. 15-22 DSGVO) zu ermöglichen.

Zur Umsetzung dieser Verpflichtungen installiert die PHS ein zentrales Datenschutzmanagementsystem, das hochschulintern von den Datenschutzbeauftragten gepflegt und weiterentwickelt wird. Zur Gewährleistung des internen Informationsflusses wird ein Netzwerk von Datenschutzansprechpersonen (Institutsleiter_innen) eingerichtet, die die Datenschutzbeauftragten im Bedarfsfall unterstützen.

Damit der Datenschutz an der PHS gewährleistet werden kann, ist die Einhaltung der im Folgenden ausgeführten Grundsätze und Pflichten für jede/n Bedienstete/n in seinem/ihrem jeweiligen Wirkungsbereich verpflichtend. Wesentlich ist dabei ein grundlegendes Umdenken des/der Einzelnen: Personenbezogene Daten dürfen **grundsätzlich nicht verarbeitet** werden. Eine Verarbeitung personenbezogener Daten ist nur dann erlaubt, wenn **alle** Grundsätze der Datenverarbeitung eingehalten werden (siehe Punkt 5.1) **und** die Verarbeitung auf eine **geeignete Rechtsgrundlage** (siehe Punkt 5.2) gestützt werden kann. Fällt eine dieser Bedingungen weg, sind verarbeitete personenbezogene Daten zu löschen.

2 Allgemeines

2.1 Sachlicher Geltungsbereich

Diese Richtlinie ist eine verbindliche Anordnung für alle Angehörigen der PHS nach § 72 Hochschulgesetz 2005 idgF mit Ausnahme der Studierenden, um die Umsetzung der DSGVO, insbesondere den rechtlich korrekten Umgang mit personenbezogenen Daten im Hochschulbetrieb sicherzustellen.

2.2 Rechtliche Grundlagen

Für diese Richtlinie sind neben den sonstigen einschlägigen österreichischen und europäischen Normen insbesondere die Europäische Datenschutzgrundverordnung (DS-GVO) sowie das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSG) in der jeweils geltenden Fassung maßgeblich.

2.3 Anwendungsbereich

Diese Richtlinie ist im Kontext der PHS auf jede ganz oder teilweise automatisierte Verarbeitung **personenbezogener Daten** (beispielsweise PH-Online, Excel-Listen, Mailing-Listen) sowie auf die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem erfolgt (beispielsweise handschriftliche Listen, Karteikartensysteme, Telefonbücher, Prüfungsprotokolle), anzuwenden.

Daten ohne Personenbezug (beispielsweise botanische, zoologische, archäologische, mathematische, wirtschaftliche Daten, die keiner natürlichen Person zugeordnet werden können, sowie anonymisierte Daten) **fallen nicht in den Anwendungsbereich dieser Richtlinie.**

3 Zuständigkeiten

Verantwortliche im Sinne der DSGVO ist der/die Rektor/in der PHS.

Die Funktion des/der Datenschutzbeauftragte/n ist – entsprechend den Vorgaben des BMBWF aufgeteilt in jeweils eine/n rechtlichen Datenschutzbeauftragte/n und eine/n technischen Datenschutzbeauftrage/n. Die Datenschutzbeauftragten sind sowohl im Innenverhältnis als auch nach außen hin zentrale Ansprechperson für Datenschutz. Er/Sie führt unter anderem das Verarbeitungsverzeichnis (insoweit, als dies nicht direkt durch die vorgeordnete Dienststelle BMBWF erfolgt), wickelt Anfragen Betroffener ab und organisiert die Schulung der Bediensteten.

Der/Die Institutsleiter/in oder der/die Leiter/in einer sonstigen Organisationseinheit ist Datenschutzansprechperson und nominiert einen Angehörigen oder eine Angehörige der Organisationseinheit als Stellvertreter/in. Gegenüber den Datenschutzbeauftragten bleiben aber der/die Leiter/in der Organisationseinheit und der/die Stellvertreter/in direkte Ansprechpersonen.

Die Datenschutzansprechpersonen dienen den Datenschutzbeauftragten als Partner in den jeweiligen Organisationseinheiten. Sie koordinieren innerhalb ihrer Organisationseinheit die Bereitstellung der Information über die in der Organisationseinheit vorliegenden personenbezogenen Daten und Verarbeitungstätigkeiten im Einzelfall und sind für die Meldung neuer Verarbeitungstätigkeiten an die Datenschutzbeauftragten zuständig. Innerhalb ihrer Organisationseinheit sind sie erster Ansprechpartner zum Thema Datenschutz für die Angehörigen ihrer Organisationseinheit. Für die Erfüllung ihrer Aufgaben erhalten die Datenschutzansprechpersonen spezielle Schulungen.

4 Begriffsbestimmungen

Zum besseren Verständnis der Richtlinie werden im Folgenden die wichtigsten Definitionen der wesentlichen datenschutzrechtlichen Begriffe erläutert.

Personenbezogene Daten sind Angaben über Betroffene, die entweder direkt oder indirekt auf deren Identität schließen lassen, insbesondere durch Zuordnung von Kennungen (z.B. Matrikelnummer oder Sozialversicherungsnummer). Unerheblich ist, ob es sich dabei um private, berufliche, wirtschaftliche Informationen, Eigenschaften, Kenntnisse oder physiologische Merkmale handelt. Personenbezogene Daten sind daher z.B. Name, Geburtsdatum, Adresse, Geschlecht, Einkommen, Vermögen, Lebensstil, Intelligenzquotient, Umsatz, Beschäftigtenzahl, Gewinn, Angaben zur Bonität sowie auch Bild, Stimme, Fingerabdrücke oder genetische Daten, Matrikelnummer und Sozialversicherungsnummer oder IP-Adressen.

Artikel 9-Daten (Art. 9 DSGVO) sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen und religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgeht sowie genetische und biometrische Daten, die eine eindeutige Identifizierung einer natürlichen Person zulassen, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Artikel 10-Daten (Art. 10 DSGVO) sind personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten. Solche Daten dürfen nur unter behördlicher Aufsicht oder aufgrund spezieller gesetzlicher Bestimmungen, die die Rechte und Freiheiten der betroffenen Personen schützen, verarbeitet werden.

Verarbeitung ist ein Sammelbegriff und schließt jede Handlung im Zusammenhang mit personenbezogenen Daten ein, unerheblich ob mit oder ohne Hilfe von automatisierten Verfahren. Somit ist jedenfalls das Erheben, Erfassen, die Administration, das Ordnen, die Speicherung, Anpassung oder Veränderung, das Auslesen oder Abfragen, die Verwendung, die Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten erfasst.

Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind. Dazu zählen unter anderem physische Dateikarten und Listen, Excel-Tabellen, PC-Speichersysteme und Datenbanken.

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

Pseudonyme Daten sind solche Daten, die sich nicht mehr ohne zusätzliche Information (Schlüssel) einer Person zuordnen lassen. Bei der Pseudonymisierung wird ein Identifikationsmerkmal (beispielsweise Name) durch einen Code (beispielsweise laufende Nummer) ersetzt. Der Schlüssel oder Code zur Feststellung der Identität muss von den pseudonymisierten Daten getrennt aufbewahrt werden. Es müssen geeignete technische und organisatorische Maßnahmen getroffen werden, die der Vermeidung einer Identifizierung der betroffenen Personen dient. Eine geeignete Maßnahme wäre beispielsweise die Aufbewahrung des Schlüssels in verschlüsselter Form auf dem Rechner der PHS oder in einem versperrten Safe. Pseudonymisierte Daten sind weiterhin als personenbezogene Daten zu behandeln. Der Vorteil einer Pseudonymisierung besteht darin, dass bei der pseudonymisierten Verarbeitung personenbezogener Daten im Falle einer Verletzung des Schutzes personenbezogener Daten (Data Breach) kein oder nur ein geringerer Folgeschaden entsteht. Sie dient daher neben der Verschlüsselung als eine Sicherungsmethode für die Verarbeitung von besonders sensiblen Daten (Artikel 9- und Artikel 10-Daten) oder großer Mengen allgemeiner Daten (Art. 6 DSGVO), wie beispielsweise die Übermittlung an Auftragsverarbeiter und Mitverantwortliche.

Anonyme Daten sind Daten, die keinen Rückschluss auf die Identität einer bestimmten Person zulassen. Auf anonyme Daten sind die datenschutzrechtlichen Bestimmungen nicht anzuwenden.

Verantwortlicher ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle die personenbezogene Daten im Auftrag der PHS verarbeitet. Verarbeitet die PHS Daten für einen Dritten, ist sie als Auftragsverarbeiterin tätig (beispielsweise in der Auftragsforschung). Der Auftragsverarbeiter wird ausschließlich aufgrund eines datenschutzkonformen Vertrages tätig.

Betroffener ist jede natürliche Person, deren personenbezogene Daten von einem Verantwortlichen, Auftragsverarbeiter oder Dritten gespeichert werden. Dazu zählen beispielsweise Bedienstete, Studierende und Alumni, Lieferanten und Lieferantinnen, sonstige Vertragspartner und Vertragspartnerinnen, Newsletterempfänger und Newsletterempfängerinnen.

Empfänger ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger.

Dritter ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Per-

sonen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten. Innerhalb der PHS ist daher auch jede Person Dritter, die nicht aufgrund der phs-internen Aufgabenverteilung mit der Erfüllung bestimmter Aufgaben betraut ist. So ist beispielsweise die Weitergabe von personenbezogenen Daten Studierender von Verwaltungspersonal an Lehr- und Forschungspersonal nur in dem Ausmaß zulässig, als das für die Durchführung der Lehre unbedingt notwendig ist.

Einwilligung der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Diese Einwilligung kann grundsätzlich jederzeit widerrufen werden (siehe Punkt 5).

Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (**Data - Breach**). Dazu zählt insbesondere der Verlust von Geräten und Speichermedien, wie Laptops, Tablets und USB-Sticks, auf denen personenbezogene Daten gespeichert sind, aber auch die Verarbeitung personenbezogener Daten auf einem nicht gesicherten Endgerät.

Genetische Daten sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden. Diese Daten zählen zu den ‚Artikel 9-Daten'.

Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten. Lichtbilder zählen grundsätzlich nicht zu biometrischen Daten, es sei denn, sie werden mit speziellen technischen Mitteln verarbeitet, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Diese Daten zählen zu den ‚Artikel 9-Daten'.

Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen, einschließlich der Erbringung von Gesundheitsdienstleistungen, und aus denen Informationen über deren Gesundheitszustand hervorgehen. Diese Daten zählen zu den ‚Artikel 9-Daten'.

5 Bedingungen für die Verarbeitung personenbezogener Daten

Damit eine Verarbeitungstätigkeit erlaubt ist, muss sie den **Grundsätzen für die Verarbeitung personenbezogener Daten** (Art. 5 DSGVO) entsprechen. Zudem muss eine entsprechende **Rechtsgrundlage** vorliegen, auf die die Verarbeitungstätigkeit gestützt wird.

5.1 Grundsätze für die Verarbeitung personenbezogener Daten

Jede Verarbeitungstätigkeit, sofern sie eine der Bedingungen des Punkt 5.2 erfüllt und somit zulässig ist, **muss sämtlichen folgenden Grundsätzen der DSGVO entsprechen**:

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Jede Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach Treu und Glauben und in nachvollziehbarer Weise erfolgen. Das bedeutet, dass alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten für die betroffene Person leicht zugänglich und verständlich in klarer und einfacher Sprache formuliert sind. Der Grundsatz betrifft insbesondere die Information über die Zwecke der Verarbeitung sowie die Auskunft über die Art und den Umfang der personenbezogenen Daten, die verarbeitet werden.

Zweckbindung

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden. Eine Weiterverarbeitung, die über diese Zwecke hinausgeht, ist nicht gestattet, es sei denn, die Weiterverarbeitung dient im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen, historischen oder statistischen Zwecken.

Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dazu zählt auch, dass Verantwortliche durch technische Voreinstellungen sicherzustellen haben, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Es dürfen somit keine Daten erhoben werden, die nicht für die Erreichung des Zweckes notwendig sind.

Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Das bedeutet, dass im Falle eines Berichtigungsansuchens vorhandene Daten gegebenenfalls berichtigt werden müssen.

Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Daher muss jede/r Bedienstete für seinen/ihren Verantwortungsbereich Fristen für die Löschung definieren und geeignete technische und organisatorische Maßnahmen für die Umsetzung der Löschung vorsehen. (Liste gesetzlicher Lösch- und Aufbewahrungsfristen siehe Anhang 1).

Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und organisatorische Maßnahmen soll insbesondere auch gewährleistet werden, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können. Die PHS regelt beispielsweise über die Vergabe von Zugriffsrechten, welche Bediensteten Zugriff auf welche Datenkategorien von Betroffenen haben. Die technisch-organisatorischen Maßnahmen, die durch Bedienstete allgemein zu beachten und anzuwenden sind, sind unter Punkt 7 erläutert.

5.2 Rechtmäßigkeit der Verarbeitung

Die Verarbeitung von personenbezogenen Daten (Art. 6 DSGVO) ist **nur auf Basis einer der folgenden Rechtsgrundlagen zulässig**. Artikel 9- und Artikel 10-Daten unterliegen eigenen Bestimmungen.

5.2.1 Personenbezogene Daten allgemein (Art. 6 DSGVO)

1. Es liegt eine Einwilligung der betroffenen Person zur Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke vor. Die Einwilligung muss durch eine eindeutige **bestätigende Handlung** erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Diese Einwilligung kann **schriftlich oder elektronisch** erfolgen, etwa auch durch Anklicken eines Kästchens auf einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder andere Erklärungen oder Verhaltensweisen, die im jeweiligen Kontext eindeutig das Einverständnis der betroffenen Person zur Datenverarbeitung signalisieren. Bloßes Schweigen, bereits vorangekreuzte Kästchen oder Untätigkeit können keine Einwilligung darstellen. **Freiwilligkeit** bedeutet zudem, dass beispielsweise die Erfüllung eines Vertrages oder die ordnungsgemäße Durchführung des Studiums als Verwaltungsverfahren nicht von der Einwilligung zur Verarbeitung von personenbezogenen Daten abhängig gemacht werden darf, die nicht für den Zweck der Vertragserfüllung oder Durchführung des Studiums notwendig sind (Koppelungsverbot). In Zusammenhang mit Lehrveranstaltungen ist eine Freiwilligkeit seitens der Studierenden jedenfalls ausgeschlossen. Eine Einwilligung ist in diesem Kontext daher immer nichtig. Wenn die Verarbeitung mehreren Zwecken dient, ist für

jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig. Im Bereich der wissenschaftlichen Forschung ist es ausreichend, wenn als Zweck die Forschungsbereiche oder Forschungsprojekte, bzw. Teile davon als Zweck angegeben werden (broad consent). Jede Einwilligung muss zudem auf das Recht zum jederzeitigen Widerruf der Einwilligung hinweisen. Sollen die Daten von Minderjährigen, die das 14. Lebensjahr noch nicht vollendet haben, verarbeitet werden, ist zusätzlich die Zustimmung der Erziehungsberechtigten einzuholen.

2. Die Verarbeitung der personenbezogenen Daten dient dem Zweck der Vertragserfüllung oder vorvertraglicher Pflichten. Es dürfen alle personenbezogenen Daten einer Vertragspartei verarbeitet werden, die notwendig sind um einen Vertrag zu erfüllen. Vor Vertragsabschluss dürfen personenbezogene Daten nur über Initiative der betroffenen Person verarbeitet werden.

3. Personenbezogene Daten dürfen auch dann verarbeitet werden, wenn dies für die Erfüllung einer rechtlichen Verpflichtung notwendig ist (beispielsweise Meldepflichten aus dem Bildungsdokumentationsgesetz). Zu beachten sind insbesondere auch gesetzliche Aufbewahrungspflichten. So sind beispielsweise im Regelfall Beurteilungsunterlagen 6 Monate ab Prüfungsdatum zum Zweck der Einsichtnahme durch den Studierenden aufzubewahren. Die Universität darf hingegen alle Studierendendaten, die zur Führung des Studiums als hoheitliches Verwaltungsverfahren notwendig sind, zum Zweck der Studienverwaltung verarbeiten und ist verpflichtet, die Studierendendaten über das Studium hinaus 80 Jahre lang aufbewahren.

4. Trifft keine der obenstehenden Bedingungen zu, dürfen personenbezogene Daten jedenfalls dann verarbeitet werden, wenn sie dem Schutz lebenswichtiger Interessen des/der Betroffenen oder einer anderen natürlichen Person dienen.

5. Eine Verarbeitung kann im Einzelfall zur Wahrung berechtigter Interessen der PLUS unter Abwägung der Betroffeneninteressen durch den/die Datenschutzkoordinator/in genehmigt werden. Dies ist nur in besonderen Ausnahmefällen möglich.

5.2.2 Besondere Kategorien von personenbezogenen Daten (Artikel 9 und 10 DSGVO)

Artikel 9-Daten dürfen nur **auf Basis einer der folgenden Rechtsgrundlagen** verarbeitet werden:

1. Es liegt eine ausdrückliche, schriftliche Einwilligung der betroffenen Person vor, die darüber hinaus den unter Punkt 5.1 dargelegten Bedingungen für eine Einwilligung entspricht.

2. Die Datenverarbeitung ist notwendig, um die Geltendmachung von Betroffenenrechten und die Erfüllung von Pflichten der PHS, die auf dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes beruhen, sicherzustellen.

3. Artikel 9-Daten, die die betroffene Person öffentlich gemacht hat, dürfen verarbeitet werden. So darf beispielsweise die von der betroffenen Person veröffentlichte politische Meinung oder Zugehörigkeit zu einer Gewerkschaft verarbeitet werden, sofern die Datenschutzgrundsätze eingehalten werden und insbesondere ein legitimer Zweck für die Verarbeitung besteht.

4. Die Datenverarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit eines Bediensteten ist nur aufgrund von Rechten und Pflichten aus dem Arbeitsrecht gestattet und darf nur von zuständigem Fachpersonal vorgenommen werden.

5. Die Datenverarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen notwendig.

6. Die Datenverarbeitung dient wissenschaftlichen oder historischen Forschungszwecken oder im öffentlichen Interesse liegenden Archivzwecken und muss durch gesetzliche Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen geschützt sein. Die Verarbeitung darf nur mit entsprechender Rechtsgrundlage erfolgen. So ist die Verarbeitung im Rahmen der Forschung auf den gesetzlichen Forschungsauftrag und dessen gesetzliche Ausgestaltung gestützt, die Archivierung personenbezogener Daten durch das Bundesarchivgesetz gerechtfertigt.

7. Die Datenverarbeitung beruht auf einer bestimmten Rechtsgrundlage und ist von erheblichem öffentlichen Interesse, wie beispielsweise die Übermittlung von Artikel-9-Daten an das Bundesministerium für Bildung, Wissenschaft und Forschung aufgrund von Pflichten aus dem Bildungsdokumentationsgesetz.

8. Die Datenverarbeitung erfolgt im öffentlichen Interesse im Bereich der öffentlichen Gesundheit und ist durch eine Rechtsgrundlage gedeckt, die Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorsieht, beispielsweise zur Abwehr grenzüberscheitender Gesundheitsgefahren.

Artikel 10-Daten dürfen nur unter behördlicher Aufsicht oder aufgrund spezieller Rechtsgrundlagen, die die Rechte und Freiheiten der betroffenen Personen ausreichend schützen, verarbeitet werden. Die Verarbeitung solcher Daten ist immer durch den/die Datenschutzbeauftragte/n zu genehmigen.

6 Informationspflicht

Im Zeitpunkt der Erhebung von Daten durch die PHS bei der betroffenen Person müssen folgende Informationen zur Verfügung gestellt werden:

- Name und Kontaktdaten der PHS und des/der Datenschutzbeauftragten
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
- die Rechtsgrundlage für die Verarbeitung (siehe Punkt 5.2)
- gegebenenfalls die Empfänger der personenbezogenen Daten
- gegebenenfalls die Übermittlung in ein nicht-europäisches Drittland (genehmigungspflichtig durch den Datenschutzkoordinator!)
- die Dauer, für die die Daten gespeichert werden sollen
- Aufklärung über die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragung sowie auf Widerspruch gegen die Verarbeitung

- im Falle einer Einwilligung in die Datenverarbeitung, die Aufklärung über das Widerrufsrecht
- das Bestehen eines Beschwerderechtes bei der Behörde
- ob die personenbezogenen Daten einem Profiling zugeführt werden
- ob die Bereitstellung von personenbezogenen Daten seitens der betroffenen Person gesetzlich oder vertraglich vorgeschrieben ist, und welche Folgen eine Nichtbereitstellung hätte (beispielsweise die Unmöglichkeit des Vertragsabschlusses, wobei nicht gegen das Koppelungsverbot (siehe Punkt 5.2) verstoßen werden darf).

Sollen die erhobenen Daten zu anderen Zwecken (z.B. zum Zweck der wissenschaftlichen Forschung) weiterverarbeitet werden, so sind diese Zwecke und die weiteren obengenannten Informationen vor der Weiterverarbeitung der betroffenen Person zur Verfügung zu stellen.

7 Datensicherheitsmaßnahmen und sonstige Pflichten

7.1 Datensicherheit bei der Verarbeitung

(siehe Punkt 5.1: Grundsatz der Integrität und Vertraulichkeit)

Bei der Verarbeitung personenbezogener Daten ist insbesondere auch auf deren Sicherheit zu achten. Das bedeutet, dass die Daten so zu schützen sind, dass kein Zugriff durch unbefugte Personen auf diese Daten erfolgen kann. Sicherheitsvorkehrungen sind der Art und dem Umfang der Daten entsprechend einzusetzen. Einzelne Daten, die keinem erhöhten Schutz unterliegen (Art. 6 DSGVO, siehe Punkt 5.1 Allgemeine Daten), wie beispielsweise ein Name und ein Geburtsdatum oder eine E-Mail-Adresse können daher weiterhin auch über die Bediensteten-E-Mail-Adresse an befugte Personen und zu legitimen Zwecken versandt werden. Für die Versendung von größeren Mengen solcher Daten sowie für Artikel 9- und Artikel 10-Daten sind immer geeignete Sicherungsmaßnahmen, wie Pseudonymisierung, Anonymisierung, Verschlüsselung oder Übermittlung über die von der Universität hierzu zur Verfügung gestellten Dienste einzusetzen. Im Zweifel ist der/die Datenschutzkoordinator/in zu kontaktieren.

Zu beachten ist, dass sowohl in Fällen, in denen die PLUS Verantwortliche ist, als auch in jenen Fällen, in denen sie Auftragsverarbeiterin ist, vertragliche Regelungen zu Datenschutz und Datensicherheit getroffen werden müssen.

7.2 Technische und organisatorische Maßnahmen

Nutzung der hochschulischen Infrastruktur

Zur grundlegenden Gewährleistung der Datensicherheit sind die Regelungen der gegenständlichen Richtlinie einzuhalten.

Nutzung von hochschulfremden Diensten

Alle Dienste, die nicht über die PHS angeboten oder nicht von dieser freigegeben werden, dürfen nicht zur Verarbeitung personenbezogener Daten, insbesondere zur Übermittlung an Externe, verwendet werden.

Nutzung von hochschulinternen Anwendungen auf privaten Endgeräten

PH-Online darf über Bediensteten-Konten auf privaten Endgeräten ausnahmslos nicht genutzt werden. Für alle anderen Anwendungen der PHS gilt, dass diese auf privaten Endgeräten nur dann genutzt werden dürfen, wenn der/die einzelne Bedienstete geeignete Sicherungsmaßnahmen (Pseudonymisierung, Anonymisierung personenbezogener Daten) ergreift.

7.3 Sonstige Pflichten

Mitarbeit bei Auskunftsbegehren

Auskunftsbegehren von Betroffenen werden an der PHS ausschließlich von den Datenschutzbeauftragten (rechtlich und technisch gemeinsam) abgewickelt. Treffen Auskunftsbegehren an anderer Stelle ein, ist auf den/die Datenschutzbeauftragten zu verweisen. Aufforderungen der Datenschutzbeauftragten zur Bereitstellung von Daten ist schnellstmöglich, spätestens aber binnen 2 Wochen, nachzukommen.

Pflicht zur Meldung von Änderungen bei den Verarbeitungstätigkeiten und neuen Verarbeitungstätigkeiten

Die PHS ist verpflichtet, ein nichtöffentliches Verzeichnis aller Verarbeitungstätigkeiten, die im hochschulischen Betrieb durchgeführt werden, zu führen. Zu diesem Zweck werden von den Datenschutzbeauftragten **sämtliche Verarbeitungen personenbezogener Daten**, die an der PHS durchgeführt werden, erhoben und in das **Verarbeitungsverzeichnis** eingepflegt. Die Bediensteten sind verpflichtet, Veränderungen bei den Verarbeitungstätigkeiten sowie neue Verarbeitungstätigkeiten an die Datenschutzbeauftragten zu melden. Der Informationsfluss hat soweit möglich über die Datenschutzansprechpersonen (Institusleitung) in koordinierter Weise zu erfolgen. Da auch pseudonymisierte Daten weiterhin als personenbezogene Daten gelten, muss auch die Verarbeitung solcher Daten an die Datenschutzbeauftragten gemeldet werden. Dabei sind die Verarbeitungstätigkeiten nicht im Einzelnen, sondern in Daten- und Betroffenenkategorien zu melden. Das bedeutet somit, dass nicht jede einzelne Verarbeitungstätigkeit pro Betroffenem zu melden ist. Beispiel für eine neue Verarbeitungstätigkeit wäre die Speicherung, das Auslesen und Verwenden von Studierendendaten, die sich für ein neugeschaffenes Projekt anmelden: In diesem Fall wären das Projekt und die Betroffenengruppe (Studierende) sowie alle erfassten Datenkategorien (Name, Adresse, E-Mail-Adresse, Matrikelnummer, Geschlecht, Haarfarbe, etc.), sowie, soweit möglich, auch der Zweck und die Rechtsgrundlage, an die Datenschutzbeauftragten zu melden.

Meldepflicht bei Data Breaches

Jede Verletzung des Schutzes personenbezogener Daten (siehe Punkt 4.) ist **ausnahmslos ohne jeden Aufschub** an die Datenschutzbeauftragten zu melden, da eine gesetzliche Meldepflicht an die Datenschutzbehörde von maximal 72 Stunden besteht. Das gilt auch für solche Fälle, in denen ein Auftragsverarbeiter einem Bediensteten eine Verletzung des Schutzes personenbezogener Daten meldet. In der Meldung ist wenn möglich anzugeben, wie viele und welche Personen, sowie wie viele und welche Art von Datensätzen von der Verletzung betroffen sind. Bedienstete haben im Falle eines Data Breaches mit den Datenschutzbeauftragten zu kooperieren und ihnen auf Anfrage alle notwendigen Informationen zur Verfügung zu stellen.

Pflicht zur Speicherbegrenzung

Personenbezogene Daten müssen **gelöscht werden, sofern kein legitimer Zweck und keine Rechtsgrundlage für ihre Speicherung (mehr) besteht** (siehe Punkt 5). Ob ein legitimer Zweck und eine Rechtsgrundlage vorliegt, ist nach den Bestimmungen dieser Richtlinie zu ermitteln (siehe Punkt 5). Dies betrifft insbesondere Doppelspeicherungen von personenbezogenen Daten: Kopien von personenbezogenen Daten, die aus der zentralen Daten-Speicherung der PHS (beispielsweise PH-Online oder SAP) extrahiert und für einen bestimmten Zweck rechtmäßig verarbeitet werden, sind nach Beendigung des Zweckes und sofern keine spezifische gesetzliche Aufbewahrungspflicht besteht, zu löschen (Liste gesetzlicher Lösch- und Aufbewahrungsfristen siehe Anhang 1). Anfragen von Externen per E-Mail werden an der PHS für ein halbes Jahr gespeichert, um Anschlussfragen bearbeiten zu können.

Pflicht zur Einholung und Administration von Einwilligungen und Widerrufen

Soll eine Datenverarbeitung auf eine Einwilligung gemäß Punkt 5.2 gestützt werden, ist verpflichtend eine datenschutzkonforme Einwilligung einzuholen und solange zu speichern, als die Datenverarbeitung andauert. Widerruft ein Betroffener seine Einwilligung, so ist der Widerruf den Datenschutzbeauftragten zu übermitteln und in Absprache mit diesen die Löschung der Daten und/oder die Einschränkung der Datenverarbeitung der betroffenen Person durchzuführen.

Verträge zur Verarbeitung personenbezogener Daten

Wird seitens der PHS die Beauftragung eines Dritten mit der Verarbeitung von personenbezogenen Daten angestrebt, so ist ein datenschutzkonformer Auftragsverarbeitervertrag abzuschließen. In diesen Fällen ist die PHS Verantwortliche. Wird hingegen die Universität von einem anderen Verantwortlichen mit der Verarbeitung von personenbezogenen Daten beauftragt (beispielsweise Auftragsforschung), ist die PHS Auftragsverarbeiterin. Kooperiert die PHS mit einem anderen Verantwortlichen derart, dass Zweck und Mittel der Datenverarbeitung gemeinsam bestimmt werden (beispielsweise ein interuniversitäres Forschungsprojekt), ist ein Vertrag abzuschließen, in dem festgelegt wird, wer welche datenschutzrechtlichen Verpflichtungen, insbesondere hinsichtlich der Informationspflichten und Betroffenenrechten, erfüllt.

Sollen solche Verträge, die die Verarbeitung personenbezogener Daten zum Inhalt haben, abgeschlossen werden, sind diese daher **verpflichtend den Datenschutzbeauftragten vorzulegen** und dürfen erst mit der **nachweislichen Genehmigung durch die Datenschutzbeauftragten** hinsichtlich ihrer datenschutzrechtlichen Konformität unterfertigt werden. Verträge, die **Forschungsprojekte** zum Inhalt haben, sind verpflichtend den Datenschutzbeauftragten zur Prüfung der Datenschutzkonformität vorzulegen. Dies gilt sowohl für Verträge, in denen die PHS Verantwortliche ist, als auch für solche Verträge in denen sie Auftragsverarbeiterin ist. Die Übermittlung personenbezogener Daten in nicht-europäische Drittländer (außerhalb der EU und des EWR) bedarf einer gesonderten Prüfung. Es ist daher bei der Kontaktaufnahme mit den Datenschutzbeauftragten anzugeben, ob eine Übermittlung in ein nicht-europäisches Drittland beabsichtigt ist.

ANHANG 1: Aufbewahrungs- und Löschfristen

Beurteilungsunterlagen gem. § 44 Abs. 3 HG mindestens sechs Monate

Prüfungsprotokolle § 44 Abs. 4 HG mindestens sechs Monate

Beurteilungen wissenschaftlicher oder künstlerischer Arbeiten gem. § 48b Abs. 1 HG mindestens sechs Monate

Prüfungsdaten § 3 Abs. 3 Z 9 Bildungsdokumentationsgesetz mindestens 80 Jahre