Mitteilungsblatt – Sondernummer

der Paris Lodron-Universität Salzburg Studienjahr 2018/2019

3. Juni 2019

68. Stück

159. PLUS-S Richtlinie zur EU-Datenschutzgrundverordnung

PLUS-S – PLUS-Steuerung
Richtlinie zur EU-Datenschutzgrundverordnung
Version: 1
Stand: im Mitteilungsblatt veröffentlicht am 3.06.2019
PLUS-S Zuständiger: Mag. Hieronymus Bitschnau

Impressum
Herausgeber und Verleger:
Rektor der Paris Lodron-Universität Salzburg
O.Univ.-Prof. Dr. Heinrich Schmidinger
PLUS-S Hauptzuständige: Ing. Mag. Marion Korath
Kapitelgasse 4-6
A-5020 Salzburg

Inhalt

1 Präambel/Zielsetzung

Mit 25.05.2018 ist die Europäische Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Der Schutz personenbezogener Daten ist an der Paris Lodron-Universität Salzburg (PLUS) von höchster Wichtigkeit und betrifft die Handlungen aller Bediensteten der Universität in deren jeweiligem Verantwortungsbereich.

Diese Richtlinie dient der internen Sicherstellung eines datenschutzkonformen Umganges mit personenbezogenen Daten im universitären Betrieb. Im ersten Teil der Richtlinie werden allgemeine Aspekte und Zuständigkeiten an der PLUS erklärt. Im Folgenden sind die einzelnen Themen immer wieder mit praxisnahen Hinweisen aus den Arbeitsbereichen der Bediensteten der PLUS in kursiven Textabschnitten versehen.

Damit Datenschutz an der PLUS 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 4) **und** die Verarbeitung auf eine **geeignete Rechtsgrundlage** (siehe Punkt 6.1) gestützt werden kann. Fällt eine dieser Bedingungen weg, sind verarbeitete personenbezogene Daten zu löschen. **Generell wird empfohlen, anonymisierte Datensätze zu verwenden, um nicht in den Anwendungsbereich der DSGVO zu fallen.**

Zur Umsetzung dieser Verpflichtungen installiert die PLUS ein zentrales Datenschutzmanagementsystem, das universitätsintern von dem/der Datenschutzkoordinator/in gepflegt und weiterentwickelt wird. Die Datenschutzkoordinatorin oder der Datenschutzkoordinator (DSK) arbeitet eng mit dem/der externen Datenschutzbeauftragten, dem/der vornehmlich Beratungs-, Schulungs- und Überwachungsfunktionen zukommen, zusammen. Zur Gewährleistung des internen Informationsflusses wird ein Netzwerk von **Datenschutzansprechpersonen** eingerichtet, die die/den DSK im Bedarfsfall unterstützen.

2 Allgemeines

2.1 Sachlicher Geltungsbereich

Diese Richtlinie ist eine verbindliche Anordnung für alle Angehörigen der PLUS nach § 94 Universitätsgesetz 2002 i.d.g.F. mit Ausnahme der Studierenden, um die Umsetzung der DSGVO, insbesondere den rechtlich korrekten Umgang mit personenbezogenen Daten, im universitären Betrieb sicherzustellen.

2.2 Rechtliche Grundlagen

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

2.3 Anwendungsbereich

Diese Richtlinie ist auf jede Verarbeitung **personenbezogener Daten** (beispielsweise PLUSonline, Excel-Listen, Mailing-Listen, handschriftliche Listen, Karteikartensysteme, Telefonbücher, Prüfungsprotokolle) anzuwenden und gilt für sämtliche Verarbeitungen, die zur Zweckerfüllung der Aufgaben der Universität dienen. Dies umfasst insbesondere Wissenschaft, Forschung, Lehre, Studienadministration und Verwaltung.

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

Verantwortlicher im Sinne der DSGVO ist die PLUS, vertreten durch das Rektorat.

Die Datenschutzkoordinatorin oder der Datenschutzkoordinator (DSK) ist sowohl im Innenverhältnis als auch nach außen hin zentrale Ansprechperson für Datenschutz. Der/Die DSK arbeitet eng mit dem/der externen Datenschutzbeauftragten zusammen, dessen/deren Aufgaben primär in der Beratung der Universität bei der Umsetzung ihrer Verpflichtungen aus der DSGVO, in der Schulung der die Verarbeitungstätigkeiten durchführenden Bediensteten, in der Überwachung der Einhaltung der datenschutzrechtlichen Pflichten der Universität sowie in der Kommunikation mit der Datenschutzbehörde bestehen.

Die Leiterinnen und Leiter der Organisationseinheiten sind Datenschutzansprechpersonen und diese nominieren eine Angehörige oder einen Angehörigen der Organisationseinheit als Stellvertreterin oder Stellvertreter. Das heißt, die Leiterinnen oder Leiter sind immer erste Ansprechpersonen in Datenschutzfragen seitens der Organisationseinheiten wie auch für die/den DSK. Es ist zulässig, zusätzlich weitere Personen neben der Stellvertreterin oder dem Stellvertreter als interne Datenschutzansprechpersonen zu nominieren, um den Informationsfluss im Innenverhältnis zu erleichtern. Gegenüber der/dem DSK bleiben aber die Leiterinnen und Leiter der Organisationseinheiten direkte Ansprechpersonen.

Die Datenschutzansprechpersonen dienen der/dem DSK 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 Verarbeitungstä-

tigkeiten an die/den DSK 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. Bitte tragen Sie die Datenschutzansprechpersonen auch im Identity Management (IDM) für den Mailverteiler datenschutzansprechpersonen@sbg.ac.at ein.

4 Grundsätze für die Verarbeitung personenbezogener Daten

Jede Verarbeitungstätigkeit **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.

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. 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 angemessene Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

Speicherbegrenzung

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

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 PLUS regelt beispielsweise über die Vergabe von Zugriffsrechten (Benutzerrolle), welche Bedienstete Zugriff auf welche Datenkategorien von Betroffenen haben. Die technisch-organisatorischen Maßnahmen, die durch Bedienstete allgemein zu beachten und anzuwenden sind, sind unter Punkt 8 erläutert.

5 Begriffsbestimmungen

Zum besseren Verständnis der Richtlinie werden im Folgenden die wichtigsten Definitionen der wesentlichen datenschutzrechtlichen Begriffe erläutert und mit Hinweisen aus den Arbeitsbereichen der Bediensteten der PLUS in kursiven Textabschnitten versehen.

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 dabei, ob es sich dabei um private, berufliche, wirtschaftliche Informationen, Eigenschaften, Kenntnisse oder physiologische Merkmale handelt.

Personenbezogene Daten sind beispielsweise Daten von Studierenden, Mitarbeitern, Alumni und Emeriti, die in PLUSonline verarbeitet werden.

Besondere Kategorien von 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.

Die Verarbeitung besonderer Kategorien von Daten bedarf eines höheren Schutzes und darf nur aufgrund spezieller Rechtsgrundlage erfolgen. Siehe dazu 6.1.2 Besondere Kategorien von personenbezogenen Daten (Art. 9 und 10 DSGVO).

Daten im Sinne des 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 analog oder digital verarbeitet wird. 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, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten erfasst.

Unter Verarbeitung sind an der PLUS insbesondere Dateisysteme wie PLUSonline, E-Mail, Elearningplattform, etc. zu verstehen.

Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind. Dazu zählen sowohl Daten, die in Papierform vorliegen, wie Anwesenheitslisten, als auch digital verarbeitete Daten, wie Excel-Tabellen oder Datenbanken.

Zusätzlich zu der Speicherung, die digital erfolgt, sind auch Papierarchive von dieser Bezeichnung umfasst, wie Personalarchiv oder Studierendenakte in Papierform.

Profiling ist jede Art der Verarbeitung, bei der durch Verknüpfung bestehender personenbezogener Daten diese neu analysiert und Vorhersagen getroffen werden können.

Pseudonyme Daten sind solche Daten, die sich nicht mehr ohne zusätzliche Information (Schlüssel/Code) einer Person zuordnen lassen (beispielsweise Referenztabelle bei Probanden einer klinischen Untersuchung: Patient A kann nur durch die Referenztabelle aufgelöst werden). Der Schlüssel/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. Pseudonymisierte Daten sind weiterhin als personenbezogene Daten zu behandeln.

Besonders im Austausch mit berechtigten Dritten stellt Pseudonymisierung ein Verfahren zur Wahrung der Sicherheit der personenbezogenen Daten dar. Wichtig ist dabei, auf eine korrekte Umsetzung zu achten. Es darf unter keinen Umständen möglich sein, dass Dritte durch Verknüpfung von öffentlich zugänglichen Daten auf die Person schließen können. Weitere Informationen dazu finden Sie unter 8.1 Datensicherheit bei der Verarbeitung.

Die Matrikelnummer ist im Sinne der Pseudonymisierung kein geeigneter Schlüssel/Code.

Anonyme Daten sind Daten, die keinen Rückschluss auf die Identität einer bestimmten Person zulassen. Anonyme Daten sind keine personenbezogenen Daten und unterliegen daher keinen Aufbewahrungsfristen.

Es wird empfohlen, wenn immer möglich, anonyme Daten zu verwenden, um nicht in den Anwendungsbereich der DSGVO zu fallen.

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 PLUS verarbeitet. Verarbeitet die PLUS Daten für einen Dritten, ist sie als Auftragsverarbeiterin tätig (beispielsweise in der

Auftragsforschung). Der Auftragsverarbeiter wird ausschließlich aufgrund eines datenschutzkonformen Vertrages tätig.

Die Frage, ob die PLUS Auftragsverarbeiterin oder unter Umständen Mitverantwortliche der Datenverarbeitung ist, kann pauschal nicht beantwortet werden und muss daher vor allem bei Forschungsprojekten nach § 26 oder § 27 UG 2002 im Einzelfall geklärt werden (8.3).

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, Newsletterempfängerinnen und Newsletterempfänger.

Betroffene können jederzeit Auskunftsbegehren an die PLUS stellen. Das Verfahren dazu finden Sie unter 8.3 Sonstige Pflichten.

Empfänger ist jede natürliche oder juristische Person, Organisationeinheit, Behörde oder andere Stelle, der personenbezogene Daten offengelegt werden. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger.

Empfänger können sowohl als interne und externe Empfänger verstanden werden. Auch ein Cloud-Anbieter kann als Empfänger verstanden werden. Beachten Sie dazu die zentral bereitgestellten Dienste der Dienstleistungseinrichtung (DLE) IT Services unter 8. Datensicherheitsmaßnahmen und sonstige Pflichten.

Dritter ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Innerhalb der PLUS ist daher auch jede Person Dritter, die nicht aufgrund der universitätsinternen 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, das für die Durchführung der Lehre unbedingt notwendig ist.

Einwilligung der betroffenen Person ist jede freiwillig für den bestimmten Fall abgegebene Willenserklärung für die Verarbeitung der personenbezogenen Daten. Die Einwilligung muss informiert und unmissverständlich sein und kann durch eine konkludente Handlung mündlich oder schriftlich erfolgen. Diese Einwilligung kann grundsätzlich jederzeit widerrufen werden (siehe Punkt 6).

Details der Umsetzung an der PLUS finden Sie unter Personenbezogene Daten allgemein (Art. 6 DSGVO). Werden Verarbeitungen auf Basis einer Einwilligungserklärung geplant, ist die Einbindung der/des DSK zwingende Voraussetzung.

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.

Im Falle eines Data Breach ist wie in Kapitel 8.3 vorzugehen.

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 ‚Art. 9 DSGVO-Daten'.

Abgesehen von einer sehr eingeschränkten Rechtsgrundlage zur Verarbeitung muss bei genetischen Daten besonders auf den Schutz der Daten geachtet werden. Es gilt ein höherer Schutzbedarf als üblich. Siehe dazu 8.1 Datensicherheit bei der Verarbeitung*.*

Biometrische Daten sind 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. Diese Daten zählen zu den ‚Art. 9 DSGVO-Daten'.

Abgesehen von einer sehr eingeschränkten Rechtsgrundlage zur Verarbeitung muss bei biometrischen Daten besonders auf den Schutz der Daten geachtet werden. Es gilt ein höherer Schutzbedarf als üblich. Siehe dazu 8.1 Datensicherheit bei der Verarbeitung.

6 Bedingungen für die rechtmäßige Verarbeitung personenbezogener Daten

Damit eine Verarbeitungstätigkeit erlaubt ist, muss sie den **Grundsätzen für die Verarbeitung personenbezogener Daten** (Art. 5 DSGVO, vgl. 4.) entsprechen. Zudem muss eine entsprechende **Rechtsgrundlage** vorliegen, auf die die Verarbeitungstätigkeit gestützt wird.

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

6.1 Personenbezogene Daten allgemein (Art. 6 DSGVO)

1. Die Verarbeitung personenbezogener Daten ist zulässig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten gegeben hat. 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). Sollen die Daten von Kindern (0-7 Jahre) oder unmündig Minderjährigen (7-14 Jahre), die das 14. Lebensjahr noch nicht vollendet haben, verarbeitet werden, ist die

Zustimmung des gesetzlichen Vertreters auf jeden Fall einzuholen. Mündig Minderjährige (14-18 Jahre) sind zwar beschränkt geschäftsfähig, ob eine Einwilligung des gesetzlichen Vertreters notwendig ist, muss im Einzelfall entschieden werden (Daten zu Gesundheit, Medizin o.Ä.).
Basiert die Verarbeitung auf Einwilligung des Betroffenen, so ist diese so lange zu speichern, wie die Verarbeitung andauert. Ebenso ist ein eventueller Widerruf zu protokollieren.

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.

Dies betrifft beispielsweise Verträge mit Lieferanten oder Daten von Mitgliedern des Alumniclubs.

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 aufzubewahren.

An der PLUS betrifft dies beispielsweise neben der Studienverwaltung auch die Verwaltung der Bediensteten in der Personalabteilung. Von Doppelspeicherungen oder vom Führen von parallelen Listen ist abzusehen, siehe auch 8.3 Sonstige Pflichten.

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 die/den DSK genehmigt werden. Dies ist nur in besonderen Ausnahmefällen möglich.

6.2 Besondere Kategorien von personenbezogenen Daten (Art. 9 und 10 DSGVO)

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

1. Es liegt eine ausdrückliche, schriftliche oder elektronische Einwilligung der betroffenen Person vor.

Werden im Rahmen von Forschungsprojekten Gesundheitsdaten erhoben und sind diese auf eine natürliche Person rückführbar, darf eine Verarbeitung nur nach Information und Einwilligung erfolgen. Eine Konsultation der/des DSK zur Formulierung der Einwilligung wird empfohlen.

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

3. Art. 9 DSGVO-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.

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 (§§ 3, 26 bzw. 27 i.V.m. § 6 Abs. 1 Z 7 UG 2002 i.d.g.F.) 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 Art. 9 DSGVO-Daten an das Bundesministerium 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 grenzüberschreitender Gesundheitsgefahren.

Art. 10 DSGVO-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 die/den DSK zu genehmigen.

7 Informationspflicht

Zum Zeitpunkt der Erhebung von Daten durch die PLUS muss die betroffene Person über die Verarbeitung informiert werden. Details zur Gestaltung eines solchen Informationsblattes gibt Ihnen die/der DSK.

8 Datensicherheitsmaßnahmen und sonstige Pflichten

8.1 Datensicherheit bei der Verarbeitung

(siehe Punkt 4 Grundsätze für die Verarbeitung personenbezogener Daten*)*

Bei der Verarbeitung personenbezogener Daten ist 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 anzupassen.

Einzelne Daten, die keinem erhöhten Schutz unterliegen (Art. 6 DSGVO, siehe Punkt 6.1), Personenbezogene Daten allgemein (Art. 6 DSGVO), wie beispielsweise ein Name und ein Geburtsdatum oder eine E-Mail-Adresse, können daher weiterhin, wenn die Zweckbindung der Verarbeitung gegeben ist, über die Bediensteten-E-Mail-Adresse an befugte Personen übermittelt werden.

Für die Versendung von größeren Mengen solcher Daten sowie für Art. 9 DSGVO und Art. 10 DSGVO Daten sind immer geeignete Sicherungsmaßnahmen, wie Pseudonymisierung, Anonymisierung, Verschlüsselung oder Übermittlung über die von der PLUS hierzu zur Verfügung gestellten Dienste einzusetzen. Im Zweifel ist die/der DSK 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.

8.2 Technische und organisatorische Maßnahmen

Nutzung der universitären Infrastruktur

Zur grundlegenden Gewährleistung der Datensicherheit sind die Regelungen der PLUS-S Richtlinie für IT Benutzung einzuhalten.

Nutzung von universitätsfremden Diensten

Alle Dienste, die nicht über die DLE IT Services angeboten werden, dürfen nicht zur Verarbeitung personenbezogener Daten, insbesondere zur Übermittlung an Externe, verwendet werden.

Zentral bereitgestellte Dienste

Zum sicheren Umgang mit personenbezogenen Daten stellt die Universität beispielsweise folgende Dienste zur Verfügung:

Für den sicheren Austausch von Daten (wie unter 8.1 Datensicherheit bei der Verarbeitung) mit Externen muss MyFiles eingesetzt werden. Werden via MyFiles Dateien geteilt, ist der Zugang zu den geteilten Inhalten zeitlich zu begrenzen und mit einem Passwort (siehe PLUS-S Richtlinie für IT Benutzung sowie Informationsportal der IT Services) zu sichern.

Zur Kollaboration mit Dritten können über die Einrichtung von Projekt-Accounts Daten regelmäßig sicher ausgetauscht werden.

Für die Erstellung von Newslettern wird seitens der PLUS der Dienst InxMail angeboten.

Umfragen können mittels des zentral bereitgestellten Dienstes limesurvey erstellt und verwaltet werden.

Nutzung von universitätsinternen Anwendungen auf privaten Endgeräten

Für einen sicheren Betrieb des privaten Endgeräts (Laptop, Smartphone, etc.) ist die Mitarbeiterin oder der Mitarbeiter allein verantwortlich und hat für geeignete Sicherungsmaßnahmen zu sorgen. Eine Nutzung von universitären Diensten ist nur dann zulässig, wenn mit der Verarbeitung kein erhöhtes Risiko einhergeht.

So hat die Mitarbeiterin oder der Mitarbeiter insbesondere dafür zu sorgen, dass keine Unbefugten Zugriff zu den Diensten sowie Informationen der Universität erhalten. Als Mindestanforderungen für geeignete Sicherungsmaßnahmen sind zu verstehen, dass das Endgerät im Besitz der Mitarbeiterin oder des Mitarbeiters steht, die aktuellsten Softwareupdates und ein Virenschutz installiert sind.

Für Mitarbeiterinnen und Mitarbeiter der PLUS steht im IT-Infoportal ein Antivirusprogramm zur privaten Verwendung zur Verfügung.

8.3 Sonstige Pflichten

Mitarbeit bei Auskunftsbegehren

Auskunftsbegehren von Betroffenen werden an der PLUS ausschließlich von der/dem DSK abgewickelt. Treffen Auskunftsbegehren an anderer Stelle ein, ist auf die/den DSK zu verweisen. Aufforderungen der/des DSK zur Bereitstellung von Daten ist schnellstmöglich, spätestens aber binnen 2 Wochen nachzukommen.

Führen eines Verarbeitungsverzeichnisses und Pflicht zur Meldung von Änderungen bei den Verarbeitungstätigkeiten und neuen Verarbeitungstätigkeiten

Die PLUS ist verpflichtet, ein aktuelles Verzeichnis aller Verarbeitungstätigkeiten, die im universitären Betrieb durchgeführt werden, anzuführen.

*Zu diesem Zweck werden von der/dem DSK **sämtliche Verarbeitungen personenbezogener Daten**, die an der PLUS durchgeführt werden, erhoben und in das **Verarbeitungsverzeichnis** eingepflegt. Die Bediensteten sind verpflichtet, Veränderungen bei den Verarbeitungstätigkeiten sowie neue Verarbeitungstätigkeiten an die/den DSK zu melden.*

Der Informationsfluss hat soweit möglich über die Datenschutzansprechpersonen der Organisationseinheiten an die/den DSK zu erfolgen. Beispiel für eine neue Verarbeitungstätigkeit wäre die Speicherung, das Auslesen und Verwenden der Daten von Studierenden, 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, etc.) sowie der Zweck und die Rechtsgrundlage an die/den DSK zu melden.

Meldepflicht bei Data Breach

Jede Verletzung des Schutzes personenbezogener Daten (vgl. 5.) ist **ausnahmslos ohne jeden Aufschub** an die/den DSK zu melden, da eine gesetzliche Meldepflicht an die Datenschutzbehörde von maximal 72 Stunden besteht. Das gilt auch für solche Fälle, in denen ein Auftragsverarbeiter der PLUS einer Bediensteten oder einem Bediensteten eine Verletzung des Schutzes personenbezogener Daten meldet. Bedienstete haben im Falle eines Data Breaches mit der/dem DSK zu kooperieren und auf Anfrage alle notwendigen Informationen zur Verfügung zu stellen.

Ein Data Breach können der Verlust eines mobilen Gerätes, falsch versendete Nachrichten oder fehlgeleitete Druckaufträge sein. Wichtig ist die unverzügliche Meldung an die/den DSK.

Pflicht zur Speicherbegrenzung und Datenminimierung

Personenbezogene Daten müssen **gelöscht werden, sofern kein Zweck oder keine Aufbewahrungsfrist besteht** (siehe Punkt 4 Grundsätze für die Verarbeitung personenbezogener Daten).

Dies betrifft insbesondere Doppelspeicherungen von personenbezogenen Daten: Kopien von personenbezogenen Daten, die aus der zentralen Daten-Speicherung der Universität (beispielsweise PLUSonline oder SAP) exportiert und für einen bestimmten Zweck rechtmäßig verarbeitet werden, sind nach Beendigung des Zweckes und sofern keine spezifische gesetzliche Aufbewahrungspflicht besteht, zu löschen. Ebenso ist auf das Anlegen eigener paralleler Datenbanken zu verzichten. (Liste gesetzlicher Lösch- und Aufbewahrungsfristen).

Anfragen von Externen per E-Mail werden an der PLUS für ein halbes Jahr gespeichert, um Anschlussfragen bearbeiten zu können, und sind dann ausnahmslos zu löschen.

Verträge zur Verarbeitung personenbezogener Daten

Auftragsverarbeitung: Beauftragt die PLUS als Verantwortliche einen Dritten mit der Datenverarbeitung, so ist mit diesem eine Datenverarbeitungsvereinbarung zu schließen.

Wird hingegen die PLUS von einem anderen Verantwortlichen mit der Verarbeitung von personenbezogenen Daten beauftragt (beispielsweise Auftragsforschung), ist die PLUS Auftragsdatenverarbeiterin.

Gemeinsame Verantwortung: Kooperiert die PLUS 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 Betroffenenrechte, erfüllt.

Sollen solche Verträge (beispielsweise Aufträge an Dritte, Kooperationsverträge), die die Verarbeitung personenbezogener Daten zum Inhalt haben, abgeschlossen werden, sind diese daher **verpflichtend der/dem DSK vorzulegen** und dürfen erst mit der **nachweislichen Genehmigung** hinsichtlich ihrer datenschutzrechtlichen Konformität unterfertigt werden.

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 der/dem DSK anzugeben, ob eine Übermittlung in ein nicht-europäisches Drittland beabsichtigt ist.

Verträge zu Drittmittelprojekten gemäß §§ 27 und 26 UG: Sofern es sich um **Forschungsprojekte gemäß § 27 UG** (beispielsweise FFG, Oesterreichische Nationalbank, HORIZON 2020) handelt, prüft das DLE Forschungsservice der PLUS im Rahmen der obligatorisch vorgesehenen Projektantragsmeldung die Datenschutzkonformität des Projektes.

Sofern es sich um **Lehr- bzw. Mobilitätsprojekte gemäß § 27 UG** (beispielsweise OeAD, APPEAR) handelt, prüft die DLE Büro für internationale Beziehungen der PLUS im Rahmen der obligatorisch vorgesehenen Projektantragsmeldung die datenschutzrechtliche Konformität des Projektes.

Für **Drittmittelprojekte gemäß § 26 UG** (ad personam) gilt, dass die jeweilige Projektleiterin bzw. der jeweilige Projektleiter für die Einhaltung der datenschutzrechtlichen Bestimmungen zu sorgen hat.

Es ist daher bei der Projektantragsmeldung anzugeben, ob eine Übermittlung in ein nicht-europäisches Drittland beabsichtigt ist.

Anhang

Die wichtigsten gesetzlichen Aufbewahrungs- und Löschfristen im Überblick

Gesetzliche Aufbewahrungspflichten sind unter anderem Rechtsgrundlagen für die Speicherung personenbezogener Daten. Dazu zählen jedenfalls direkte Anweisungen, Daten aufzuheben. Personenbezogene Daten, die in Dokumenten, für die gesetzliche Aufbewahrungspflichten bestehen, enthalten sind, können ebenfalls nicht gelöscht werden.

Im Folgenden werden die wichtigsten Aufbewahrungs- und Löschfristen des universitären Betriebes dargestellt. Diese Aufzählung ist jedenfalls nicht abschließend, in bestimmten Fällen können andere gesetzliche Aufbewahrungspflichten gelten.

1. Personenbezogene Daten von Studierenden

Anwendungsfall	Aufbewahrungsfrist	Praxis
Prüfungsspezifische Daten und Beurteilungsunterlagen von Studierenden Bsp. Gutachten, Korrekturen schriftlicher Prüfungen Prüfungsprotokolle Korrekturen schriftlicher Arbeiten Plagiatsberichte (Safe Assign) (Pro-)Seminararbeiten Bachelorarbeit	6 Monate ab Bekanntgabe der Beurteilung in PLUSonline	Vernichtung aller analogen und digitalen Unterlagen an den Organisationseinheiten, sofern die Ergebnisse zentral im PLUSonline erfasst wurden.
Universitätsspezifische Daten des Studierenden Bezeichnung von Prüfungen, vergebene ECTS-Anrechnungspunkte, Beurteilung Name des Prüfers/Beurteilers bzw. der Prüferin/Beurteilerin, Datum der Prüfung/ Beurteilung, Name und Matrikelnummer des/der Studierenden	80 Jahre	zentrale Speicherung PLUSonline
Beurteilungsunterlagen für Diplom-/ Masterarbeiten und Dissertationen Bsp. Gutachten, Korrekturen	6 Monate ab Bekanntgabe der Beurteilung in PLUSonline	Vernichtung aller analogen und digitalen Unterlagen an den Organisationseinheiten, Hochschulschrift bzw. die Abschlussarbeit wird regelmäßig in der UB veröffentlicht
Sozialversicherungsnummer	2 Jahre ab Abgang von der Bildungseinrichtung	zentral im PLUSonline
Daten zu Ansprüchen auf Studienförderung	3 Jahre ab Zahlung der letzten gesetzlich nicht gebührenden Studienbeihilferate (Hemmung bei Auslandsaufenthalt)	Nur im Bereich Leistungsstipendien oder Studienförderungen für Universitätsangehörige relevant

2. Personenbezogene Daten von Bediensteten

Anwendungsfall	Aufbewahrungsfrist	Praxis
Notwendige Daten zur Ausstellung eines Dienstzeugnisses/ bereits ausgestelltes Dienstzeugnis	30 Jahre ab Beendigung des Dienstverhältnisses	Speicherung im Personalakt
Daten zu Regressansprüchen des Dienstgebers aufgrund eines Schadenersatzes zur Dienstnehmerhaftpflicht	3 Jahre ab Bekanntwerden des Schadens	Je Organisationseinheit
Daten zu Entgeltansprüchen	3 Jahre ab Fälligkeit	Speicherung im Personalakt sowie durch Rechnungswesen und Controlling
Aufzeichnungen und Berichte über Arbeitsunfälle	5 Jahre ab Zeitpunkt des Unfalls	Speicherung im Personalakt sowie durch Arbeitssicherheit/ Arbeitsmedizin
Daten zu Ersatzansprüchen des Arbeitgebers bzw. des Arbeitnehmers/ der Arbeitnehmerin aus einer vorzeitigen Beendigung des Arbeitsverhältnisses	6 Monate	Speicherung im Personalakt

3. Personenbezogene Daten in Wissenschaft und Forschung

Anwendungsfall	Aufbewahrungsfrist	Praxis
Archivgut Daten, die Archivgut gemäß dem Bundesarchivgesetz sind	unbefristet	Beurteilung im Einzelfall nach dem Bundesarchivgesetz
Personenbezogene Daten, die Gegenstand wissenschaftlicher Forschung sind (Rohdaten)	10 Jahre zu Zwecken des Beweises guter wissenschaftlicher Praxis	Zentrale Speicherung durch den/die verantwortliche/n Forscher/in am Universitätsserver
Personenbezogene Daten, die Gegenstand wissenschaftlicher Forschung sind (Rohdaten)	30 Jahre zu Zwecken der Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen	Zentrale Speicherung durch den/die verantwortliche/n Forscher/in am Universitätsserver

4. Allgemeine Fristen

Anwendungsfall	Aufbewahrungsfrist	Praxis
Aufbewahrung von Aufzeichnungen zur umsatzsteuerlichen Erfassung	7 Jahre oder 22 Jahre (bei Liegenschaften)	Rechnungswesen und Controlling
Aufbewahrung vertraglicher Unterlagen und Korrespondenz für Gewährleistung	2 Jahre für bewegliche Sachen, 3 Jahre für unbewegliche Sachen	je Organisationseinheit
Aufbewahrung vertraglicher Unterlagen und Korrespondenz bei Kaufpreisforderung	3 Jahre für bewegliche Sachen, 30 Jahre für unbewegliche Sachen	je Organisationseinheit
Aufbewahrung von Werkverträgen und allen Unterlagen zur Vertragserfüllung	3 Jahre	je Organisationseinheit; länger nach Vorgaben von Kooperationspartnern bzw. Fördergebern
Aufbewahrung sämtlicher notwendiger Unterlagen zur Geltendmachung oder Abwehr von Schadenersatz	3 Jahre (Schaden und Schädiger bekannt), ansonsten 30 Jahre	je Organisationseinheit

Im Zweifelsfalle kann die Datenschutzkoordinatorin oder der Datenschutzkoordinator oder Dienstleistungseinrichtung Rechtsabteilung konsultiert werden.