2024-06-25-HSL (2024-06-25-HSL)

Vom 25. Juni 2024

Von diesem Geschäft tangierte Erlasse (PHGR Nummern)

Neu:	**210.100**
Geändert:	–
Aufgehoben:	210.100

Der [Autor]

beschliesst:

I.

Der Erlass PHGR 210.100 (Weisung Datenschutz und Datensicherheit (WDD)) wird als neuer Erlass publiziert.

1 Allgemeine Bestimmungen

Art. 1 Zweck

[1] Schützen der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden.

[2] Unterstützen eines erfolgreichen Risikomanagement der PH Graubünden und Schutz der Mitarbeitenden vor möglichen strafrechtlichen Sanktionen.

[3] Benennen der für den Datenschutz an der PH Graubünden verantwortlichen Stellen und regeln der Rechte und Pflichten im Zusammenhang mit der Datenbearbeitung und der Datensicherheit.

Art. 2 Geltungsbereich

[1] Diese Weisung gilt für alle Personen, die im Rahmen des vierfachen Leistungsauftrags der PH Graubünden Personendaten bearbeiten, d.h.

a) Mitarbeitende und Studierende der PH Graubünden;
b) Personen im Honorarverhältnis, insb. auch Praxislehrpersonen;
c) Teilnehmende an Weiterbildungsveranstaltungen und -lehrgängen;
d) allfällige weitere Personen, die im Auftrag der PH Graubünden handeln.

Art. 3 Grundsätze

[1] Bei jeder Bearbeitung von Personendaten sind folgende Grundsätze einzuhalten:

a) Rechtmässigkeit: Die Bearbeitung braucht eine Rechtsgrundlage oder die Einwilligung der betroffenen Person im Einzelfall;
b) Zweckgebundenheit: Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich ist oder gesetzlich vorgesehen ist;
c) Verhältnismässigkeit: Zur Zweckerfüllung dürfen nur so viele Personendaten wie nötig bearbeitet werden – nicht so viele wie möglich;
d) Transparenz: Die Beschaffung von Personendaten und insbesondere auch der Zweck der Bearbeitung müssen für die betroffenen Personen erkennbar sein;
e) Richtigkeit: Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern;
f) Sicherheit: Durch angemessene technische und organisatorische Massnahmen (TOM) müssen für Personendaten die Vertraulichkeit, Verfügbarkeit und Integrität sichergestellt werden.
g) Dokumentation: Die Bearbeitung und die Umsetzung von Massnahmen im Datenschutz müssen nachvollziehbar sein.

[2] Bei Kenntnisnahme oder Vermutung, dass die Persönlichkeit oder Grundrechte einer betroffenen Person gefährdet oder verletzt sind bzw. wurden, ist umgehend der/die Verantwortliche (gem. 210.100 Art. 4) zu informieren.

Art. 4 Verantwortlichkeiten

[1] Grundsätzlich ist die Hochschulleitung für die Umsetzung der geltenden Datenschutzbestimmungen über den gesamten Datenlebenszyklus verantwortlich.

[2] Die Hochschulleitung erlässt mit Anhang VI eine Datenschutzerklärung zur Nutzung auf Webseiten, Apps, Wi-Fi-Netzwerken und in Verträgen.

[3] Die Hochschulleitung informiert über Anpassungen und Ergänzungen dieser Weisung in geeigneter Form, insbesondere durch die Veröffentlichung der jeweils aktualisierten Fassung in der systematischen Rechtssammlung.

[4] Folgende Verantwortlichkeiten sind definiert:

a) Rektor:in: Verantwortliche:r für die
   1. Umsetzung und Einhaltung der geltenden Datenschutzbestimmungen und der Aktenführung im Hochschulrat, in der Hochschulleitung und dem Rektorat;
   2. Führung eines Verzeichnis aller ihr/ihm unterstellten Bearbeitungen von Personendaten gem. Prozesslandkarte;
   3. Pflege einer Datenschutz-Folgenabschätzung (DSFA) gem. 210.100 Art. 7, wo erforderlich;
   4. Bearbeitung von Meldungen über Datenschutzverletzung gem. 210.100 Art. 6; und
   5. Einhaltung der Bearbeitungsgrundsätze «Privacy by Design» und «Privacy by Default» bei der Planung von Vorhaben durch technische und organisatorische Schutzmassnahmen.

b) Prorektor:in: Verantwortliche:r für die
   1. Umsetzung und Einhaltung der geltenden Datenschutzbestimmungen und die Aktenführung in ihrer/seiner Organisationseinheit, in welcher die Daten bearbeitet werden bzw. die Akten entstehen;
   2. Führung eines Verzeichnis aller ihr/ihm unterstellten Bearbeitungen von Personendaten gem. Prozesslandkarte;
   3. Pflege einer Datenschutz-Folgenabschätzung (DSFA) gem. 210.100 Art. 7, wo erforderlich;
   4. Bearbeitung von Meldungen über Datenschutzverletzung gem. 210.100 Art. 6; und
   5. Einhaltung der Bearbeitungsgrundsätze «Privacy by Design» und «Privacy by Default» bei der Planung von Vorhaben durch technische und organisatorische Schutzmassnahmen.

c) Verwaltungsdirektor:in: Verantwortliche:r für die
   1. Umsetzung und Einhaltung der geltenden Datenschutzbestimmungen und die Aktenführung in der Verwaltung;
   2. Führung eines Verzeichnis aller ihr/ihm unterstellten Bearbeitungen von Personendaten gem. Prozesslandkarte;
   3. Pflege einer Datenschutz-Folgenabschätzung (DSFA) gem. 210.100 Art. 7, wo erforderlich;

4. Bearbeitung von Meldungen über Datenschutzverletzung gem. 210.100 Art. 6; und
5. Einhaltung der Bearbeitungsgrundsätze «Privacy by Design» und «Privacy by Default» bei der Planung von Vorhaben durch technische und organisatorische Schutzmassnahmen.

d) Hochschulangehörige: Verpflichtet zur Einhaltung der geltenden datenschutzrechtlichen Vorgaben sowie der Weisung Datenschutz und Datensicherheit an der PH Graubünden verpflichtet, um ihren/seinen Teil an einem funktionierenden Datenschutz und zur wirksamen Datensicherheit beizutragen.

e) Datenschutzberater:in: verantwortlich für die Beratung und Schulung der Hochschulangehörigen der PH Graubünden in Fragen des Datenschutzes. Ausserdem wirkt sie/er mit beim Erlass und der Anwendung von Nutzungsbedingungen und Datenschutzvorschriften. Sie/Er berät die Verantwortlichen in Datenschutzbelangen, die Verantwortlichen tragen jedoch allein die Verantwortung dafür, dass die Personendaten datenschutzkonform bearbeitet werden.

[5] Ist der Bearbeitungsort der Personendaten oder der Entstehungsort der Akten nicht eindeutig, ist der/die Verwaltungsdirektor:in für die Koordination zwischen den Organisationseinheiten zuständig.

Art. 5 Begriffe

[1] In Anlehnung an das DSG und das Eidgenössische Departement für Auswärtige Angelegenheiten (EDA) bedeuten in dieser Weisung:

a) Personendaten: Sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

b) besonders schützenswerte Personendaten: Sind alle:
1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten;
2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie;
3. genetische Daten;
4. biometrische Daten, die eine natürliche Person eindeutig identifizieren;
5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen; und
6. Daten über Massnahmen der sozialen Hilfe.

c) betroffene Person: Ist eine Person, von der Personendaten bearbeitet werden.

d) Bearbeiten: Umfasst jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, beispielsweise das Abfragen, Abgleichen, Anpassen, Archivieren, Aufbewahren, Auslesen, Bekanntgeben, Beschaffen, Erfassen, Erheben, Löschen, Offenlegen, Ordnen, Organisieren, Speichern, Verändern, Verbreiten, Verknüpfen, Vernichten und Verwenden von Personendaten.

e) Profiling: Meint jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

f) Verantwortliche:r: Bestimmt alleine oder gemeinsam mit anderen den Zweck und die Mittel der Bearbeitung der Personendaten.

g) Auftragsbearbeiter:in: Bearbeitet Personendaten im Auftrag der/des Verantwortlichen (Outsourcing). Entscheidet jedoch nicht über den Zweck und die Mittel einer Datenbearbeitung. Der/Die Auftragsbearbeiter:in darf die Daten nicht für eigene Zwecke bearbeiten.

h) Europäische Wirtschaftsraum (EWR): Umfasst die Mitgliedstaaten der Europäischen Union (EU) sowie das Fürstentum Liechtenstein, Island und Norwegen. Die Datenschutz-Grundverordnung (DSGVO) bezeichnet die Bearbeitung von Personendaten als Verarbeitung von personenbezogenen Daten.

i) Anonymisierung: Daten sind so anonymisiert, dass die betroffene Person nicht mehr identifiziert werden kann und es sich daher nicht mehr um personenbezogene Daten handelt, die somit nicht in den Anwendungsbereich des Datenschutzrechts fallen.

j) Pseudonymisierung: Daten sind von ihren direkten Identifikatoren getrennt, so dass eine Zuordnung zu einer Person nur mit Hilfe zusätzlicher, gesondert aufbewahrter Informationen möglich ist. Die Zusatzinformationen müssen von den verarbeiteten Daten getrennt und sicher aufbewahrt werden, um die Nicht-Zuordnung zu gewährleisten.

k) Privacy by Design: Der Schutz personenbezogener Daten muss durch das Ergreifen technischer und organisatorischer Massnahmen im Entwicklungsstadium eines Produktes oder einer Dienstleistung sichergestellt werden.

l) Privacy by Default: Ein Produkt oder eine Dienstleistung muss einer Person die Wahl lassen, wie viele persönliche Daten diese mit der PH Graubünden teilt, dabei muss die Standardeinstellungen die datenschutzfreundlichste sein.

2 Datenschutz

Art. 6 Datenschutzverletzung

[1] Eine Datenschutzverletzung ist eine Verletzung der Datensicherheit bei Personendaten (einschliesslich pseudonymisierter Personendaten), die dazu führen, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht wurden. In einem solchen Fall ist gem. diesem Prozess vorzugehen.

[2] Eine Datenschutzverletzung oder der blosse Verdacht einer solchen ist unverzüglich nach Kenntnisnahme der nach 210.100 Art. 4 verantwortlichen Person zu melden. Hierfür ist eine Meldung auf der Datenschutz Webseite zu erstellen.

[3] Der Datenschutzvorfall wird von der nach 210.100 Art. 4 verantwortlichen Person gem. Prozess bearbeitet und dokumentiert.

[4] Kann ein Datenschutzvorfall zu einem hohen Risiko für die Grundrechte auf informationelle Selbstbestimmung oder Privatsphäre der betroffenen Personen führen, so ist er unverzüglich dem Kantonalen Datenschutzbeauftragten zu melden. Spätestens 72 Stunden nach Kenntnisnahme. Die Meldung eines Datenschutzvorfalles darf nicht verzögert werden. Eine Meldung muss auch erfolgen, wenn Zweifel bestehen, ob Grundrechte gefährdet sind.

[5] Betroffene Personen sind über den Datenschutzvorfall zu informieren, wenn die Umstände es erfordern oder die zuständige Aufsichtsbehörde es verlangt. Dies ist beispielsweise der Fall, wenn die betroffenen Personen Schutzmassnahmen treffen müssen.

Art. 7 Datenschutz-Folgenabschätzung

[1] Eine Datenschutz-Folgenabschätzung (DSFA) ist immer dann durchzuführen, wenn eine geplante Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person darstellt. Eine Datenschutz-Folgenabschätzung ist gem. Prozess durchzuführen.

[2] Ein hohes Risiko definiert sich aus der Verwendung von neuen Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. So gilt eine Bearbeitung als besonders risikoreich, wenn umfangreich besonders schützenswerte Personendaten bearbeitet werden oder wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

[3] In Zweifelsfällen ist zugunsten der Datenschutz-Folgenabschätzung zu entscheiden. Der/Die Datenschutzberater:in leistet bei der Umsetzung Hilfestellung.

[4] Ergibt die DSFA, dass die geplante Bearbeitung trotz den vorgesehenen Massnahmen immer noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, so muss eine Vorabkonsultation beim kantonalen Datenschutzbeauftragten durchgeführt werden.

Art. 8 Auftragsbearbeitung

[1] Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem/einer Auftragsbearbeiter:in übertragen werden, wenn:

a) die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und
b) keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

[2] Für die Bearbeitung von personenbezogenen Daten der PH Graubünden durch einen/eine Auftragsbearbeiter:in erstellt die/der Verantwortliche eine schriftlichen Auftragsdatenbearbeitungsvertrag (ADV). Hierfür kann die auf der Datenschutzwebseite zur Verfügung gestellte Vorlage verwendet werden oder muss im Wesentlichen folgende Angaben enthalten:

a) Umschreibung des Projektes/der Dienstleistung und Angabe des Zwecks der Datenbearbeitung;
b) Zweckbindung: Verbot, die Daten in anderer Weise bzw. für eigene Zwecke zu benutzen;
c) Sicherheit: Durch angemessene technische und organisatorische Massnahmen (TOM) müssen für Personendaten die Vertraulichkeit, Verfügbarkeit und Integrität, sowie die Nachvollziehbarkeit der Bearbeitung sichergestellt werden;
d) Pflicht, nach den Weisungen der PH Graubünden zu handeln;
e) Pflicht, Unterauftragnehmer:in inkl. Datenstandorte anzugeben, sowie Pflicht, die Unterauftragnehmer:in vorgängig von der PH Graubünden genehmigen zu lassen (pauschale Genehmigung ist möglich) und Unterzeichnung einer Geheimhaltungsvereinbarung;
f) Pflicht zur Umsetzung geeigneter technischen und organisatorischen Massnahmen zwecks Datensicherheit und Beschreibung der implementierten Massnahmen;

g) Pflicht bei einer Verletzung des Datenschutzes oder bei Verdacht auf eine solche den für die Verarbeitung Verantwortlichen innerhalb von 72 Stunden nach Kenntniserlangung mit den gesetzlich vorgeschriebenen Angaben zu informieren und alles Erforderliche zu unternehmen, um die Datensicherheit wiederherzustellen;

h) Pflicht ein Verzeichnis sämtlicher Datenbearbeitungen im Zusammenhang mit der Dienstleistung an die PH Graubünden zu erstellen, auf dem aktuellen Stand zu halten und dem Verantwortlichen auszuhändigen;

i) Auditrechte und Pflichten bei Vertragsende.

[3] Für die Prüfung der ADV ist jeweils der/die Datenschutzberater:in beizuziehen, welche:r bei Vertragsredaktion und -verhandlung unterstützt.

[4] Eine Kopie des Verzeichnisses der Bearbeitungstätigkeiten der Auftragsbearbeiterin/des Auftragsbearbeiters ist einzufordern und in der Vertragsablage des jeweiligen Vertragspartners abzulegen.

Art. 9 Bekanntgabe von Personendaten ins Ausland

[1] Unter der Bekanntgabe von Personendaten ins Ausland kann die Veröffentlichung der Daten im Ausland, ein Transfer an eine/einen ausländische:n Verantwortliche:n oder einen/eine ausländische:n Auftragsbearbeiter:in fallen. Die Bekanntgabe umfasst nicht nur die Weitergabe, sondern auch das Einsicht gewähren (Fernzugriff). Irrelevant ist, wie das Zugänglichmachen erfolgt, für wie lange dieses andauert und aufgrund wessen Veranlassung die Bekanntgabe geschieht.

[2] Drittstaaten, welche einen angemessenen Schutz gewähren finden sich im Anhang 1 DSV 235.11. Bereits unter der DSGVO genehmigte Standardklauseln der Europäischen Kommission werden vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) anerkannt.

[3] Bei unsicheren Drittstaaten ist die Nutzung der Dienstleistung grundsätzlich zu vermeiden und es müssen primär Alternativlösungen aus Europa, d.h. EWR/Schweiz oder sonstigen sicheren Drittländern, gesucht werden. Alternativ müssen die Personen- und anderen schützenswerten Daten rechtlich genügend verschlüsselt (oder vollständig anonymisiert) werden.

[4] Befindet sich ein betroffener Drittstaat nicht auf der Liste im Anhang 1 DSV 235.11, dürfen Daten wie nach bisherigem Recht trotzdem dorthin geleitet werden, wenn ein geeigneter Datenschutz auf andere Weise gewährleistet wird. So durch einen völkerrechtlichen Vertrag oder Datenschutzklauseln, die dem EDÖB vorgängig mitzuteilen sind. Allfälligen Restrisiken sind durch die Verantwortlichen zu tragen und die Risikoeinschätzung ist zu dokumentieren.

[5] Bei der Ermittlung, ob ein Auslanddatentransfer vorliegt, sowie bei den notwendigen Risikoabwägungen und Umsetzung gesetzlich vorgesehener Schutzmassnahmen ist der/die Datenschutzberater:in beizuziehen.

Art. 10 Forschungsprojekte

[1] Wenn immer möglich sollen in Forschungsprojekten anonymisierte oder pseudonymisierte Daten verwendet werden.

[2] Wenn in einem Forschungsprojekt dennoch Personendaten bearbeiten werden, sind immer die sogenannten „W-Fragen“ zu beantworten und dokumentieren: Wer bearbeitet welche Daten zu welchem Zweck für wie lange, wo werden sie aufbewahrt sowie wie werden sie geschützt und wann werden sie anonymisiert bzw. vernichtet.

[3] Wenn das Forschungsprojekt Studien über Krankheiten, Struktur und Funktionen des menschlichen Körpers beinhaltet, die in der Schweiz durchgeführt werden, muss vor dem Start die Ethikkommission des Kanton Zürich (KEK) kontaktiert werden.

Art. 11 Datenschutz-Management-System

[1] Um die gesetzlichen und betrieblichen Anforderungen an den Datenschutz zusammenzuführen und eine systematische Organisation, Steuerung und Kontrolle zu gewährleisten und damit die Einhaltung der datenschutzrechtlichen Bestimmungen sicherzustellen, kann ein Datenschutz-Management-System (DSMS) eingeführt werden.

[2] Zur Unterstützung und Dokumentation des Datenschutzmanagements stellt das DSMS Prozesse, Verfahren, Methoden und Auswertungen zur Verfügung.

[3] Durch regelmässige Überprüfungen und Aktualisierungen soll das DSMS sicherstellen, dass Datenschutzmassnahmen kontinuierlich verbessert werden, um sich an veränderte Bedrohungen und Anforderungen anzupassen.

[4] Durch Schulungsprogramme und Sensibilisierungsmassnahmen stellt das DSMS sicher, dass alle Hochschulangehörigen die Bedeutung des Datenschutzes verstehen und entsprechende Best Practices befolgen.

[5] Das DSMS stellt Prozesse zur Vorbereitung auf Datenschutzvorfälle und zur schnellen Wiederherstellung von Daten nach Vorfällen wie Sicherheitsverletzungen oder Datenverlusten bereit.

3 Bild-, Ton- und Videoaufzeichnungen

Art. 12 Bild-, Ton- und Videoaufzeichnungen

[1] Der datenschutzkonforme Umgang mit Bild-, Ton- und Videoaufzeichnungen wird im Anhang VII geregelt.

4 Datensicherheit

Art. 13 Datensicherheit

[1] Die/Der Verantwortliche und der/die Auftragsbearbeiter:in müssen technische und organisatorische Massnahmen (TOMs) treffen, damit die bearbeiteten Daten im Hinblick auf das Risiko ihrem Schutzbedarf entsprechend:

a) Vertraulichkeit: nur Berechtigten zugänglich sind;
b) Verfügbarkeit: verfügbar sind, wenn sie benötigt werden;
c) Integrität: nicht unberechtigt oder unbeabsichtigt verändert werden;
d) Nachvollziehbarkeit: Bearbeitungen nachvollziehbar sind.

Zur Nutzung der Informations- und Kommunikationstechnologien an der PH Graubünden liefert die Weisung Verwaltung 610.110 die Vorgaben.

[2] Bei der Festlegung der technischen und organisatorischen Massnahmen werden zudem die folgenden Kriterien berücksichtigt. Entscheide sind schriftlich zu begründen.

a) Stand der Technik;
b) Implementierungskosten.

[3] Der Schutzbedarf der Personendaten, das Risiko und die technischen und organisatorischen Massnahmen sind über die gesamte Bearbeitungsdauer hinweg periodisch zu überprüfen. Die Massnahmen sind nötigenfalls anzupassen.

5 Aktenführung und Archivierung

Art. 14 Ordnungssystem

[1] Die Aktenführung erfolgt in der Regel digital. Begründete Ausnahmen können durch das zuständige Mitglied der Hochschulleitung genehmigt werden.

[2] Archivwürdige Unterlagen werden im Anhang I bestimmt und einem Archivierungsdossier zugewiesen. Aufbewahrungsfristen und -regeln werden ebenfalls im Anhang I den einzelnen Dossiers zugewiesen.

[3] Die Aktenführung erfolgt im Dokumentenmanagementsystem der PH Graubünden, namentlich SharePoint Online (SPO), sofern nichts anderes in Anhang II vermerkt ist.

[4] Alle Daten und Dokumente der PH Graubünden werden den vier Vertraulichkeitsklassen Öffentlich, Intern, Vertraulich und Geheim zugeordnet. Die Zugehörigkeit zu einer Vertraulichkeitsklasse wird anhand der Bestimmungen und Kriterien in Anhang II festgelegt.

[5] Bei der Ablage bzw. beim Versand von Dateien bzw. Dokumente finden die Bestimmungen gemäss Anhang II Anwendung.

[6] Die Ablagestruktur der PHGR folgt dem 7x3 Grundsatz. Pro Ablageebene können maximal sieben Ordner und pro Ordner maximal drei Ebenen definiert werden. Eine Ablageebene darf ausschliesslich aus Ordnern oder Dokumenten bestehen. Die Benennung der Ordner auf jeder Ebene muss einer einheitlichen Logik folgen.

[7] Die Namenskonvention gilt gleichermassen für Ordner als auch für Dokumente und Dateien. Bei der Benennung von Ordnern, Dateien und Dokumenten sind die Vorgaben gemäss Anhang III einzuhalten.

Art. 15 Archiv und Archivierung

[1] Grundsätzlich werden Unterlagen digital archiviert. Papierbasierte Akten werden für die Archivierung digitalisiert und die papierbasierten Akten anschliessend vernichtet. Akten gemäss Anhang IV sind bei der Archivierung ebenfalls zu vernichten.

[2] Bei der Vernichtung von Akten ist auf die Wahrung der Vertraulichkeit zu achten.

[3] Die Archivierung der digitalen Unterlagen erfolgt in einem dedizierten Bereich des Dokumentenmanagementsystems der PH Graubünden. Das System ist redundant ausgelegt und schützt die archivierten Unterlagen vor Naturgefahren, Feuer, Wasser, Einbruch und Diebstahl sowie vor unbefugter Einsichtnahme.

[4] Es wird ein für die Langzeitarchivierung geeignetes Dateiformat eingesetzt. Das digitale Archivgut wird periodisch auf seine Vollständigkeit und Lesbarkeit überprüft. Mindestens alle 5 Jahre wird zudem das verwendete Dateiformat überprüft und bei Bedarf werden Formatmigrationen durchgeführt.

[5] Das Archiv wird entsprechend den Dossiers gemäss Anhang I organisiert und die Dossiers gemäss Anhang V strukturiert, beide Anhängen dienen gleichzeitig als Verzeichnis.

[6] Die Bibliothek der PH Graubünden trägt die Verantwortung für das Archiv der PH Graubünden und ist die Kontaktstelle für das Staatsarchiv. Für das Anbieten der Unterlagen an das zuständige Archiv, gemäss Gesetz über die Aktenführung und Archivierung 490.010 Art. 4 ist der/die Leiter:in Bibliothek der PH Graubünden zuständig.

6 Schlussbestimmungen

Art. 16 Konsequenzen bei Nichteinhaltung

[1] Die Nichteinhaltung dieser Weisung stellt einen Verstoss gegen die arbeits- und vertragsrechtlichen Pflichten dar und kann disziplinarrechtlich geahndet werden.

[2] Zudem sieht das Datenschutzgesetz vor, dass bei Datenschutzverletzungen sowohl Sanktionen des Kantonalen Datenschutzbeauftragten als auch Klagen von betroffenen Personen und strafrechtliche Bussen in Frage kommen. In allen Fällen können Hochschulangehörige belangt werden, entweder durch eine direkte Busse oder durch Rückgriff auf die fehlbare Person.

Anhänge

Anhang I:	Aktenplan
Anhang II:	Datenklassifizierung
Anhang III:	Namenskonvention
Anhang IV:	Negativliste
Anhang V:	Dossierstruktur
Anhang VI:	Datenschutzerklärung für Webseiten, Apps, Wi-Fi-Netzwerke und Verträge
Anhang VII:	Datenschutz im Umgang mit Bild-, Ton- und Videoaufzeichnungen

II.

Keine Fremdänderungen.

III.

Der Erlass PHGR 210.100 (Weisung Datenschutz und Datensicherheit (WDD) vom 22. August 2023) wird aufgehoben.

IV.

[Abschlussklausel]

[Ort], [Datum]

[Behörde]

[Funktion 1]
[Name 1]

[Funktion 2]
[Name 2]

Anhang I – WEISUNG DATENSCHUTZ UND DATENSICHERHEIT 210.100 – Aktenplan

Ordnungssystem position	Titel/ Bezeichnung	Hauptprozess	Abteilung	Aufbewahrungsfrist
1.1	Sitzungsprotokoll HSL	Strategie	Rektorat	10
1.2	Sitzungsprotokoll HSR	Strategie	Rektorat	10
5.1	Studiengang	Ausbildung	GA	10
5.2	Studienjahr	Ausbildung	GA	10
5.3	Studierendenakte	Ausbildung	GA	50
6.1	Lehrgang/Kurse	Weiterbildung	WB	10
8.1	Projektdokumentation	Dienstleistung	Alle	10
8.2	Tagungsdokumentation	Dienstleistung	Alle	10
11.1	Publikationen	Marketing und Kommunikation	Alle	10
12.1	Personalakte	Personaladministration	Dienste	10
13.1	Rechtsgrundlagen	Informations-& Wissensmanagement	Dienste	10
13.2	Beschlussprotokoll	Informations-& Wissensmanagement	Alle	10

Anhang II – Weisung Datenschutz und Datensicherheit 210.100 – Datenklassifizierung

Vertraulichkeitsklasse	Beispiele (Auflistung nicht abschliessend)	Ablageort
Öffentlich Daten gelten als öffentlich, falls sie im Sinne der PHGR nicht schützenswert sind und die unerlaubte Veröffentlichung, Änderung oder Zerstörung keine Auswirkungen auf die PHGR, deren Mitarbeitende oder Partner hat.	**Veröffentlichung durch das Rektorat bzw. durch die Abteilungsleitung** Jahresberichte, Beiträge in Schulblätter, Stundenpläne, Modulbeschreibungen, Forschungsberichte, Veranstaltungsflyer und Publikationen **Veröffentlichung durch das Rektorat mit Zustimmung des/der Urheber/in** Forschungsergebnisse, Publikationen **Veröffentlichung durch den/die Urheber/in** Skripte, Arbeitsblätter, Musterlösungen	**Keine Vorgaben** Empfohlen ist der Einsatz von SharePoint Online der PHGR damit eine ausreichende Sicherung gewährleistet werden kann, des Weiteren gelten die Bestimmungen gemäss "Weisungen zur Nutzung von IKT-Mitteln an der PHGR".
Intern Daten gelten als intern, falls sie im Sinne der PHGR nicht schützenswert sind und die unerlaubte Veröffentlichung, Änderung oder Zerstörung kurzfristig niedrige Auswirkungen auf die PHGR, deren Mitarbeitende oder Partner hat. *Standardmässig sind alle Daten als intern zu behandeln, sofern diese nicht ausdrücklich anderweitig klassifiziert wurden.*	**Unterrichtsmaterialien** Vorlesungs-, Seminar- und Kursunterlagen **Rechtsmittel** Reglemente, Weisungen und Richtlinien, die die Grundlage für Studium, Weiterbildungen und Arbeit an der PHGR bilden. **Vorlage- und Prozessdokumente** Vorlagen, Checklisten, Formulare etc. sowie Prozessbeschreibungen und Prozesszeichnungen	SharePoint Online der PHGR E-Mail[1] und Post

1 Es gilt zu beachten, dass der E-Mail-Verkehr der PHGR nicht verschlüsselt wird und für dritte leicht einsehbar ist.

Vertraulichkeitsklasse	Beispiele (Auflistung nicht abschliessend)	Ablageort
Vertraulich Daten gelten als vertraulich, falls sie im Sinne der PHGR schützenswert sind und die unerlaubte Veröffentlichung, Änderung oder Zerstörung erhebliche Auswirkungen auf die PHGR, deren Mitarbeitende oder Partner hat.	Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Besonders schützenswerten Personendate sind ebenfalls als vertraulich einzustufen und mit entsprechenden technischen und organisatorischen Massnahmen zu schützen. Weiter gelten im Sinne der PHGR folgende Daten als vertraulich: Personaldossier, Lohneinstufungen, Mitarbeiterbeurteilungen, Leistungsnachweise und Beurteilungen von Studierenden, Protokolle mit vertraulichem Inhalt, Evaluationsergebnisse sowie allgemeine und persönliche Passwörter	Dedizierter Bereich auf SharePoint Online der PHGR. Keine Ablage auf OneDrive oder in allgemeine Bereiche auf SharePoint Online. *Der Versand als E-Mail-Anhang oder in Teams ist untersagt[2].* Der Schutz dieser Daten muss auch nach dem Ausdruck und beim Versand gewährleistet werden (unter Verschluss, eingeschrieben etc.).
Geheim Daten gelten als geheim, falls sie im Sinne der PHGR besonders schützenswert sind und die unerlaubte Veröffentlichung, Änderung oder Zerstörung erhebliche Auswirkungen auf die PHGR, deren Mitarbeitende oder Partner hat.	**Strategische Ausrichtungs- und Führungsunterlagen** Alle Daten, welche die strategische Ausrichtung und Führung der PHGR betreffen und durch Mitbewerber zum Nachteil der PHGR ausgenützt werden könnten.	Laufwerk I Dedizierter Bereich auf SharePoint Online mit aktiver Verschlüsselung. Keine Ablage auf OneDrive. *Der Versand als E-Mail-Anhang oder in Teams ist untersagt[2].*

2 Die Verwendung eines passwortgeschützten Links zu SharePoint Online ist zulässig.

Anhang III – Weisung Datenschutz und Datensicherheit 210.100 – Namenskonvention

Konvention	Beispiel
Keine Sonderzeichen Die Verwendung von Sonderzeichen mit Ausnahme von Boden- und Bindestrich (_ / -) ist nicht zulässig. Leerzeichen dürfen ebenfalls nicht verwendet werden und sind, wenn nötig, durch Bodenstriche zu ersetzen. Der Einsatz von Gross- und Kleinbuchstaben ist jedoch zu bevorzugen.	**Falsch:** Weisungen Nutzung IT-Mittel.docx **Besser:** Weisung_Nutzung_IT-Mittel.docx **Richtig:** WeisungNutzungIT-Mittel.docx
Umlaute Umlaute in Datei- und Ordnernamen sind zulässig.	**Falsch:** Bestaetigung.docx **Richtig:** Bestätigung.docx
Sprache Die verwendete Sprache für Datei- und Ordnernamen ist Deutsch. Dateien, welche in mehreren Sprachen vorliegen, werden mit dem jeweiligen Sprachkürzel (_it bzw. _rm) am Ende des Dateinamens gekennzeichnet. Dateien in deutscher Sprache werden nicht gekennzeichnet.	WeisungNutzungIT-Mittel.docx WeisungNutzungIT-Mittel_rm.docx WeisungNutzungIT-Mittel_it.docx
Erstelldatum und Version Erstelldatum und Version eines Dokumentes dürfen nicht im Dateinamen angegeben werden. Diese werden in Form von Metadaten zu jeder Datei automatisch hinterlegt und können, wenn nötig, abgerufen werden. Die letzten 100 Versionen der entsprechenden Datei werden vom System automatisch gespeichert.	**Falsch:** WeisungNutzungIT-Mittel_20170602.docx **Richtig:** WeisungNutzungIT-Mittel.docx
Jahres- und Semesterzahlen Jahres- und Semesterzahlen sind zulässig. Jahreszahlen werden im Format (yyyy) und Semesterzahlen im Format (yyyy-yy) angegeben.	**Richtig:** Budget2018.docx **Richtig:** Studierende2017-18.docx
Maximale Zeichenzahl Für Ordnerbenennungen sind maximal 30 Zeichen, für Dateinamen exkl. Dateiendung (Bspw. .docx) 50 Zeichen zulässig.	-

Anhang IV – WEISUNG DATENSCHUTZ UND DATENSICHERHEIT 210.100 – Negativliste

Die untenstehenden Dokumente müssen bei der Archivierung aus dem Dossier entfernt und gem. Weisung entsorgt werden. Sie sind in der Regel nicht geschäftsrelevant.

- Entwürfe und überholte Versionen von Unterlagen (ausser diese wären zum Verständnis einer Diskussion notwendig)
- Kopien sowie Doppel- und Mehrfachexemplare (Exemplar mit Originalunterschrift aufbewahren)
- Notizen ohne Relevanz für den Geschäftsprozess
- Reservationen (von Sitzungszimmer usw.)
- Begleitschreiben ohne geschäftsrelevanten Inhalt
- Offerten, die nicht berücksichtigt wurden (inkl. Absageschreiben)
- Unterlagen Dritter (z.B. Broschüren, Kataloge, Angebote die keine Reaktion auslösen)
- Unterlagen übergeordneter Stellen (Kanton, Bund) die sich nicht auf ein Geschäft zwischen dem Amt und der jeweiligen Stelle beziehen

Anhang V – WEISUNG DATENSCHUTZ UND DATENSICHERHEIT 210.100 – Struktur Dossier

Ordnungssystemposition	Titel/ Bezeichnung	Ordnerstruktur
1.1	Sitzungsprotokoll HSL [STUDIENJAHR]	1.1.1 Beilagen 1.1.2 Einladung 1.1.3 Protokoll 1.1.4
1.2	Sitzungsprotokoll HSR [STRATEGIEPERIODE]	1.2.1 Beilagen 1.2.2 Einladung 1.2.3 Protokoll 1.2.4
5.1	Studiengang [BEZEICHNUNG_REVISIONNUMMER]	5.1.1 Planung 5.1.2 Durchführung 5.1.3 Qualitätssicherung 5.1.4 Entwicklung
5.2	Studienjahr [BEZEICHNUNG]	5.2.1 Planung 5.2.2 Durchführung 5.2.3 Qualitätssicherung 5.2.4 Entwicklung
5.3	Studierendenakte [NAME_VORNAME_MATNR]	5.3.1 Personalien 5.3.2 Korrespondenz 5.3.3 Studierendenleistung 5.3.4 Mobilität
6.1	Lehrgang/Kurse [BEZEICHNUNG_JAHR]	6.1.1 Planung 6.1.2 Durchführung 6.1.3 Qualitätssicherung 6.1.4 Entwicklung

Ordnungssystemposition	Titel/ Bezeichnung	Ordnerstruktur
8.1	Projektdokumentation [BEZEICHNUNG / PROJEKTNUMMER]	8.1.1 Planung 8.1.2 Durchführung 8.1.3 Qualitätssicherung 8.1.4 Entwicklung
8.2	Tagungsdokumentation [BEZICHNUNG_JAHR]	8.2.2 Planung 8.2.3 Durchführung 8.2.4 Qualitätssicherung 8.2.5 Entwicklung
11.1	Publikationen [BEZEICHNUNG_JAHR]	11.1.1 Planung 11.1.2 Durchführung 11.1.3 Qualitätssicherung 11.1.4 Entwicklung
12.1	Personalakte [NACHNAME_VORNAME_PERSNR]	12.1.1 Planung 12.1.2 Durchführung 12.1.3 Qualitätssicherung 12.1.4 Entwicklung
13.1	Rechtsgrundlagen [NUMMER_BEZEICHNUNG]	13.1.1 Planung 13.1.2 Durchführung 13.1.3 Qualitätssicherung 13.1.4 Entwicklung
13.2	Beschlussprotokoll [BEZEICHNUNG]	13.2.1 Planung 13.2.2 Durchführung 13.2.3 Qualitätssicherung 13.2.4 Entwicklung

phGR

Anhang VI – Weisung Datenschutz und Datensicherheit 210.100

DATENSCHUTZERKLÄRUNG

Version:1.0
Autor: Martin Berger
Letzte Änderung: 01.07.2024
Klassifizierung: Öffentlich
Status: Aktiv

1 WORUM GEHT ES IN DER DATENSCHUTZERKLÄRUNG?

Datenschutz ist Vertrauenssache, und Ihr Vertrauen ist uns wichtig. In dieser Datenschutzerklärung informieren wir Sie deshalb, wie und wozu wir Ihre Personendaten erheben, bearbeiten und verwenden. Sie erfahren in dieser Datenschutzerklärung unter anderem:

- welche Personendaten wir erheben und bearbeiten;
- zu welchen Zwecken wir Ihre Personendaten verwenden;
- wer Zugang zu Ihren Personendaten hat;
- welchen Nutzen unsere Datenbearbeitung für Sie hat;
- wie lange wir Ihre Personendaten bearbeiten;
- welche Rechte Sie mit Bezug auf Ihre Personendaten haben; und
- wie Sie uns kontaktieren können.

2 WER IST FÜR DIE DATENBEARBEITUNG VERANTWORTLICH?

Datenschutzrechtlich verantwortlich für eine bestimmte Datenbearbeitung ist jeweils die Institution, die festlegt, ob diese Bearbeitung erfolgen soll, zu welchen Zwecken sie erfolgt und wie sie ausgestaltet ist. Für die Datenbearbeitungen nach dieser Datenschutzerklärung ist grundsätzlich die Pädagogische Hochschule Graubünden, Scalärastrass 17, 7000 Chur ("PH Graubünden", "wir" oder "uns"), verantwortlich.

3 BEGRIFFE

- **Personendaten** sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.
- Eine **betroffene Person** ist eine Person, von der Personendaten bearbeitet werden.
- **Bearbeiten** umfasst jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, beispielsweise das Abfragen, Abgleichen, Anpassen, Archivieren, Aufbewahren, Auslesen, Bekanntgeben, Beschaffen, Erfassen, Erheben, Löschen, Offenlegen, Ordnen, Organisieren, Speichern, Verändern, Verbreiten, Verknüpfen, Vernichten und Verwenden von Personendaten.
- **Profiling** meint jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
- **Cookies** sind Dateien, die gewisse technische Daten enthalten und über einen Internetbrowser auf einem Computersystem abgelegt und gespeichert werden. Die betroffene Person kann das Speichern von Cookies durch unsere Internetseite jederzeit mittels einer entsprechenden Einstellung des genutzten Internetbrowsers verhindern und damit der Setzung von Cookies dauerhaft widersprechen. Ferner können bereits gesetzte Cookies jederzeit über einen Internetbrowser oder andere Softwareprogramme gelöscht werden.
- Zu den **technischen Daten** gehören u.a.

- die IP-Adresse Ihres Geräts und weitere Geräte-IDs (z.B. MAC-Adresse);
- Kennnummern, die Ihrem Gerät von Cookies und ähnlichen Technologien (z.B. Pixel Tags) zugewiesen werden;
- Angaben über Ihr Gerät und dessen Konfiguration, z.B. Betriebssystem oder Spracheinstellungen;
- Angaben zum Browser, mit dem Sie auf das Angebot zugreifen, und dessen Konfiguration;
- Informationen über Ihre Bewegungen und Aktionen auf unseren Webseiten und in unseren Apps;
- Angaben über Ihren Internetprovider;
- Ihr ungefährer Standort und der Zeitpunkt der Nutzung;
- systemseitige Aufzeichnungen von Zugriffen und anderen Vorgängen (Log-Daten);
- Randdaten aus dem Fernmeldeverkehr.

4 WELCHE QUELLEN UND DATEN NUTZEN WIR?

Wir bearbeiten Daten, die im Rahmen der Nutzung unserer Webseiten, Apps oder Wi-Fi-Netzwerke anfallen (technische Daten), die Sie uns zur Verfügung stellen (z.B. im Rahmen von Newsletter-Anmeldungen, Anmeldungen zu Veranstaltungen, Ausfüllen von Webformularen oder sonstigen Bestellungen) oder die im Rahmen des Vertragswesens anfallen. Dies kann insbesondere im Zusammenhang mit Studium, Weiterbildung, Forschung oder Dienstleistungen stehen.
Wir erheben Ihre personenbezogenen Daten insbesondere, wenn Sie mit uns in Kontakt treten, zum Beispiel über unsere Webseiten, als Interessent:in, Antragsteller:in, Kundin oder Kunde, Bewerber:in, usw. Wir bearbeiten personenbezogene Daten, die wir im Rahmen unserer Geschäftsbeziehung von unseren Kundinnen und Kunden erhalten. Zudem bearbeiten wir - soweit für die Erbringung unserer Dienstleistungen erforderlich - personenbezogene Daten, die wir aus öffentlich zugänglichen Quellen zulässigerweise gewinnen.
Relevante personenbezogene Daten sind Personalien (Name, Adresse und andere Kontaktdaten, Geburtstag und -ort und Staatsangehörigkeit) und Legitimationsdaten (z.B. Ausweisdaten). Darüber hinaus können dies auch Auftragsdaten, Daten aus der Erfüllung unserer vertraglichen Verpflichtungen, Werbe- und Vertriebsdaten, Dokumentationsdaten sowie andere mit den genannten Kategorien vergleichbare Daten sein.
Wir können zu Schulungs-, Beweis- und Qualitätssicherungszwecken Telefon- oder Videokonferenzen mithören oder aufzeichnen. In solchen Fällen weisen wir Sie gesondert darauf hin (z.B. durch eine Anzeige oder Ansage) und es steht Ihnen frei, uns mitzuteilen, falls Sie keine Aufzeichnung wünschen, oder die Kommunikation zu beenden (falls Sie lediglich keine Aufzeichnung Ihres Bildes wünschen, stellen Sie bitte Ihre Kamera aus). Ausserdem können wir Personendaten für die Organisation, die Durchführung und die Nachbereitung von Anlässen bearbeiten, wie insbesondere Teilnehmerlisten und Inhalte von Referaten und Diskussionen, aber auch Bild- und Audioaufnahmen, die während diesen Anlässen erstellt werden.
Bei der rein informatorischen Nutzung unserer Webseiten, also wenn Sie keine Webformulare ausfüllen und sich nicht für einen Event registrieren oder uns sonst Informationen übermitteln, erheben wir folgende technische Daten, die Ihr Browser übermittelt. Eine Zusammenführung dieser Daten mit anderen Datenquellen wird nicht vorgenommen. Diese Datenerhebungen dienen lediglich der Optimierung und Verbesserung der Nutzerfreundlichkeit unserer Webseiten. Wir behalten uns vor, diese

Daten nachträglich zu prüfen, wenn uns konkrete Anhaltspunkte für eine rechtswidrige Nutzung bekannt werden.

Unter Umständen können Sie sich bei einzelnen Online-Angeboten mit dem Login eines Drittanbieters anmelden (z.B. Switch edu-ID). In diesem Fall erhalten wir Zugriff auf bestimmte beim betreffenden Anbieter hinterlegte Daten, z.B. Ihr Name und Ihre E-Mail-Adresse. Informationen dazu finden Sie in der Datenschutzerklärung des betreffenden Anbieters.

5 WIE BEARBEITEN WIR BESONDERS SCHÜTZENSWERTE PERSONENDATEN?

Bestimmte Arten von Personendaten gelten datenschutzrechtlich als «besonders schützenswert», z.B. Angaben über die Gesundheit und biometrische Merkmale. Je nach Konstellation können Personendaten auch solche besonders schützenswerten Personendaten umfassen. Wir bearbeiten besonders schützenswerte Personendaten in der Regel aber nur, wenn es für die Erbringung einer Leistung erforderlich ist, Sie uns diese Daten von sich aus bekannt gegeben haben oder Sie in die Bearbeitung eingewilligt haben. Wir können besonders schützenswerte Personendaten ausserdem bearbeiten, wenn dies zur Rechtswahrung oder Einhaltung von in- oder ausländischen Rechtsvorschriften erforderlich ist, die entsprechenden Daten von der betroffenen Person offensichtlich öffentlich bekanntgegeben wurden oder das anwendbare Recht ihre Bearbeitung sonst zulässt.

6 AUF WELCHER RECHTSGRUNDLAGE UND WOFÜR BEARBEITEN WIR IHRE DATEN (ZWECK DER BEARBEITUNG)?

Als öffentlich-rechtliche Anstalt bearbeiten wir personenbezogene Daten auf der Rechtsgrundlage des kantonalen Gesetzes über Hochschulen und Forschung (GHF, BR 427.200) im Einklang mit den Bestimmungen des kantonalen Datenschutzgesetzes (KDSG, BR 171.100) des Kantons Graubünden, des Schweizerischen Bundesgesetzes über den Datenschutz (DSG, SR 235.1) sowie der Europäischen Datenschutz-Grundverordnung (DSGVO, Verordnung 2016/679), soweit die entsprechenden Regelungen anwendbar sind. Da die DSGVO verlangt, dass wir diese einzeln aufführen, werden nachfolgend diejenigen Rechtsgrundlagen genannt, auf welche wir unsere Bearbeitung stützen, sofern die DSGVO zur Anwendung gelangt. Bei einer Bearbeitung von Personendaten nach KDSG oder DSG stützen wir uns jeweils auf die vergleichbaren Rechtsgrundlagen in diesen Gesetzen.

6.1 Zur Erfüllung von vertraglichen Pflichten (Art. 6 Abs. 1 b DSGVO)

Die Bearbeitung von Daten erfolgt zur Erbringung von Dienstleistungen der PH Graubünden im Rahmen der Erfüllung unserer Verträge (bspw. in den Bereichen Aus- und Weiterbildung und betreffend unsere Dienstleistungen) mit unseren Kundinnen und Kunden oder zur Durchführung vorvertraglicher Massnahmen, die auf Anfrage hin erfolgen. Die Zwecke der Datenbearbeitung richten sich in erster Linie nach der konkreten Dienstleistung und können unter anderem Tätigkeiten wie Schulungen oder Beratung umfassen. Die Vertragsunterlagen und Geschäftsbedingungen können weitere Einzelheiten zu den Datenbearbeitungszwecken enthalten.

6.2 Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 f DSGVO)

Soweit erforderlich bearbeiten wir Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen unsererseits oder von Dritten. Beispiele:

- Forschung
- Werbung oder Markt- und Meinungsforschung, soweit Sie der Nutzung Ihrer Daten nicht widersprochen haben,
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten,
- Newsletter, Eventanmeldungen und Bestellungen (sofern Zusendung von der betroffenen Person erwartet werden kann)
- Gewährleistung der IT-Sicherheit und des IT-Betriebs,
- zur Analyse des Internetverkehrs auf unseren Webseiten, zur Verbesserung der Funktionalität unserer Webseiten
- Verhinderung und Aufklärung von Straftaten,
- Massnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten

Auch die Wahrung weiterer berechtigter Interessen, die sich nicht abschliessend nennen lassen, gehören dazu.

6.3 Aufgrund Ihrer Einwilligung (Art. 6 Abs. 1 a DSGVO)

Soweit Sie uns eine Einwilligung zur Bearbeitung von personenbezogenen Daten für bestimmte Zwecke (z.B. Weitergabe von Daten, Auswertung personenbezogener Daten für Forschungs- und Marketingzwecke; Newsletter, soweit keine Rechtsgrundlage hierfür gestützt auf lit. b besteht) erteilt haben, ist die Rechtmässigkeit dieser Bearbeitung auf Basis Ihrer Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der DSGVO, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind. Der Widerruf der Einwilligung berührt nicht die Rechtmässigkeit der bis zum Widerruf bearbeiteten Daten.

6.4 Aufgrund gesetzlicher Vorgaben (Art. 6 Abs.1 c DSGVO) oder im öffentlichen Interesse (Art. 6 Abs. 1 e DSGVO)

Zudem unterliegen wir als PH Graubünden neben den Vorschriften des Hochschulförderungs- und -koordinationsgesetz (HFKG, SR 414.20) sowie dem kantonalen Gesetz über Hochschulen und Forschung (GHF, BR 427.200) auch den sonstigen rechtlichen Vorgaben des schweizerischen Gesetzgebers, so dass eine Bearbeitung personenbezogener Daten auch dann erfolgen kann, wenn dies aufgrund gesetzlicher Vorgaben erforderlich ist oder wenn die Bearbeitung im öffentlichen Interesse liegt. Grundlage hierfür ist, insbesondere für Studium und Weiterbildung, u.a. Art. 24 HFKG und Art. 2, 9 GHF.

7 WER BEKOMMT IHRE DATEN?

Innerhalb der PH Graubünden erhalten diejenigen Stellen Zugriff auf Ihre Daten, welche diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten brauchen. Auch von uns eingesetzte Dienstleister können zu diesen Zwecken Daten erhalten. Dies sind u.a. Unternehmen in den Kategorien IT-Dienstleistungen, Logistik, Druckdienstleistungen, Telekommunikation, Beratung und Consulting sowie Vertrieb und Marketing.

Alle diese Kategorien von Empfängern können ihrerseits Dritte beiziehen, so dass Ihre Daten auch diesen zugänglich werden können. Die Bearbeitung durch bestimmte Dritte können wir beschränken (z.B. IT-Provider), jene anderer Dritter aber nicht (z.B. Behörden, Banken etc.).

Weitere Empfänger personenbezogener Daten können z.B. sein:

- Öffentliche Stellen und Institutionen (z.B. Behörden und Gerichte) bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung.
- Einrichtungen innerhalb der PH Graubünden zur Risikosteuerung aufgrund gesetzlicher oder behördlicher Verpflichtung.
- Diejenigen Stellen, für die Sie uns Ihre Einwilligung zur Datenübermittlung erteilt haben bzw. für die Sie uns von der Verschwiegenheitspflicht gemäss Vereinbarung oder Einwilligung befreit haben.

Wir ermöglichen bestimmten Dritten, auf unserer Website und bei Anlässen von uns ihrerseits Personendaten von Ihnen auch in eigener Verantwortung zu erheben (z.B. Medienfotografen, Anbieter von Tools, die wir auf unserer Website eingebunden haben (siehe Abschnitt 13.4), etc.). Soweit wir nicht in entscheidender Weise an diesen Datenerhebungen beteiligt sind, sind diese Dritten allein dafür verantwortlich. Bei Anliegen und zur Geltendmachung Ihrer Datenschutzrechte wenden Sie sich bitte direkt an diese Dritten.

8 WERDEN DATEN IN EIN DRITTSTAAT ÜBERMITTELT?

Eine Datenübermittlung an Stellen in Staaten ausserhalb der Schweiz (sogenannte Drittstaaten) findet statt (bspw. im Rahmen der Forschungskooperationen mit ausländischen Hochschulen/Organisationen), soweit

- es gesetzlich vorgeschrieben ist oder
- Sie uns Ihre Einwilligung erteilt haben, oder
- wir durch entsprechende Mechanismen (bspw. Verträge) geeignete Garantien vorgesehen haben.

9 SIND IHRE DATEN SICHER?

Wir treffen den Risiken angemessene technische und organisatorische Massnahmen zum Schutz Ihrer Daten vor unberechtigtem Zugriff und Missbrauch.
Unsere Mitarbeitenden und die von uns beauftragten Dienstleister sind der Datensicherheit und zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet. Überdies wird diesen der Zugriff auf die persönlichen Daten nur soweit notwendig gewährt.

10 WIE LANGE WERDEN IHRE DATEN BEARBEITET?

Wir bearbeiten Ihre Daten grundsätzlich so lange, wie es unsere Verarbeitungszwecke und gesetzliche Aufbewahrungsfristen, insbesondere zu Dokumentations- und Beweiszwecken, erfordern oder eine Speicherung technisch notwendig ist (z.B. bei Backups). Sofern keine gesetzlichen, vertraglichen oder technischen Gründe entgegenstehen, löschen oder anonymisieren wir Ihre Daten grundsätzlich nach Ablauf der Aufbewahrungsfrist im Rahmen unserer üblichen Prozesse.

Als öffentlich-rechtliche Anstalt sind wir gem. Gesetz über die Aktenführung und Archivierung (GAA, BR 490.200) des Kantons Graubünden verpflichtet, alle Unterlagen nach Ablauf der Aufbewahrungsfrist dem Staatsarchiv anzubieten. Die vom Staatsarchiv verwalteten Unterlagen unterliegen einer Schutzfrist von 30 Jahren, bei besonders schützenswerten Personendaten von 50 Jahren, und sind erst nach Ablauf dieser Frist zugänglich.

11 WELCHE RECHTE HABEN SIE IM ZUSAMMENHANG MIT DER BEARBEITUNG IHRER PERSONENDATEN?

Sie haben das Recht, Datenbearbeitungen zu widersprechen, besonders wenn wir Ihre Personendaten auf Basis eines berechtigten Interesses bearbeiten und die weiteren anwendbaren Voraussetzungen erfüllt sind. Sie können ausserdem Datenbearbeitungen im Zusammenhang mit Direktmarketing (z.B. Werbe-E-Mails) jederzeit widersprechen. Dies gilt auch für ein Profiling, soweit dieses mit solchem Direktmarketing in Verbindung steht.
Soweit die jeweils anwendbaren Voraussetzungen erfüllt und keine gesetzlichen Ausnahmen anwendbar sind, haben Sie zudem folgende Rechte:

- das Recht, Auskunft über Ihre bei uns gespeicherten Personendaten zu verlangen;
- das Recht, unrichtige oder unvollständige Personendaten korrigieren zu lassen;
- das Recht, die Löschung oder Anonymisierung Ihrer Personendaten zu verlangen;
- das Recht, die Einschränkung der Bearbeitung Ihrer Personendaten zu verlangen;
- das Recht, bestimmte Personendaten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten;
- das Recht, eine Einwilligung mit Wirkung für die Zukunft zu widerrufen, soweit eine Bearbeitung auf einer Einwilligung beruht. Bearbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

Bitte beachten Sie, dass diese Rechte im Einzelfall ggf. eingeschränkt oder ausgeschlossen sein können, z.B. wenn Zweifel an der Identität bestehen oder dies zum Schutz anderer Personen, zur Wahrung von schutzwürdigen Interessen oder zur Einhaltung gesetzlicher Verpflichtungen erforderlich ist. Die Bearbeitung Ihres Rechtsanspruchs beginnt in jedem Fall erst nach erfolgreicher Identitätsprüfung.
Sofern die DSGVO anwendbar ist, gilt Folgendes: Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Bearbeitung nach Art. 18 DSGVO, das Recht auf Widerspruch aus Art. 21 DSGVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO. Darüber hinaus besteht ein Beschwerderecht bei einer zuständigen Datenschutzaufsichtsbehörde (Art. 77 DSGVO).
Begehren für die Ausübung Ihrer Rechte stellen Sie bitte schriftlich an den Kontakt unter Ziffer 13.
Es steht Ihnen auch frei, bei einer zuständigen Aufsichtsbehörde Beschwerde einzureichen, wenn Sie Bedenken haben, ob die Bearbeitung Ihrer Personendaten rechtskonform ist.

- Zuständige Aufsichtsbehörden in der Schweiz:
    - Datenschutzbeauftragter des Kantons Graubünden;
    - Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB).
- Zuständige Aufsichtsbehörde im Fürstentum Liechtenstein ist die Datenschutzstelle des Fürstentums Liechtenstein.

12 GIBT ES FÜR SIE EINE PFLICHT ZUR BEREITSTELLUNG VON DATEN?

Im Rahmen unserer Geschäftsbeziehung müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme und Durchführung einer Geschäftsbeziehung und der Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir in der Regel nicht in der Lage sein, einen Vertrag mit Ihnen zu schliessen oder diesen auszuführen.

13 TRACKING, PROFILING, IT-SYSTEMPROTOKOLLE UND EXTERNE INHALTE

Sowohl die von uns erhobenen technischen Daten als auch Cookies enthalten in der Regel keine Personendaten. Allerdings können Personendaten, die wir oder von uns beauftragte Drittanbieter von Ihnen speichern (z.B., wenn Sie ein Benutzerkonto bei uns oder diesen Anbietern haben), mit den technischen Daten bzw. mit den in Cookies gespeicherten und aus ihnen gewonnenen Informationen und damit möglicherweise mit Ihrer Person verknüpft werden.

13.1 Tracking

Wir nutzen Tools sowie Dienste von Drittanbietern (welche ihrerseits Cookies einsetzen können) auf unserer Webseite, insbesondere um die Funktionalität oder den Inhalt unserer Website zu verbessern (z.B. Integration von Videos oder Karten), Statistiken zu erstellen sowie Werbung zu schalten.
Das Tracking kann durch die Do-Not-Track-Einstellung in gängigen Internet-Browsern verhindert werden. Diese Einstellung bewirkt, dass in der Browseranfrage im Headerblock der Tag «Do-Not-Track» mitgesendet wird und die Aktionen des Besuchers nicht ausgewertet werden.

13.2 Profiling

Wir bearbeiten Ihre Daten aus der Nutzung unserer Webseiten oder Apps teilweise automatisiert, um bestimmte persönliche Aspekte auszuwerten (Profiling). Wir können Profiling beispielsweise einsetzen, um:

- unsere Angebote laufend zu verbessern und besser auf individuelle Bedürfnisse auszurichten;
- Ihnen unsere Inhalte und Angebote, inkl. eLeanring Angebote, bedarfsgerecht zu präsentieren;
- Ihnen möglichst nur Werbung und Angebote zu unterbreiten, die für Sie wahrscheinlich relevant sind.

13.3 IT-Systemprotokolle

Bei jeder Nutzung der Webseiten, Apps oder Wi-Fi-Netze, bspw. beim Aufruf von Websites und beim Versand von E-Mails, werden automatisch Daten übermittelt, welche teilweise als Personendaten klassifiziert werden könnten und von uns in sogenannten Systemprotokollen gespeichert werden. Die Systemprotokolle werden von der PH Graubünden zur Ermittlung von Störungen und aus Sicherheitsgründen gespeichert. Sind die Daten für die Erfüllung betrieblicher oder gesetzlicher Pflichten nicht mehr erforderlich, werden diese gelöscht.

13.4 Externe Inhalte

Auf den Webseiten werden externe Inhalte von z.B. YouTube, Vimeo, SRF, Moodle, Flowpaper, Google Maps, Mapbox, MazeMap, Doubleclick, Microsoft Captcha, Instagram, Facebook, LinkedIn und TikTok angezeigt oder auf externe Inhalte verlinkt. Dabei wird die IP-Adresse übermittelt und die Inhaltanbieter können Cookies etc. setzen. Ist der Webseiten-Besucher gleichzeitig im Netzwerk des jeweiligen Drittanbieters angemeldet, kann der Besuch auf der Webseite je nach Anbieter seinem Benutzerkonto zugeordnet werden. Die Kontaktdaten und weitere Informationen zu den einzelnen Datenbearbeitungen dieser Dienstleister sind in der jeweiligen Datenschutzerklärung abrufbar. Die PH Graubünden hat ein berechtigtes Interesse an der Einbindung dieser externen Inhalte oder der Verlinkung zu solchen, jedoch keinen Einfluss auf die Art und Weise der Datenübermittlung.

14 MOODLE

Die folgenden Datenschutzhinweise geben einen Überblick über die Erhebung und Bearbeitung Ihrer Daten im Learning Management System (https://moodle.phgr.ch) der PH Graubünden (nachfolgend «Moodle»). Moodle ist ein Open Source Learning Management System (LMS) und wird an der PH Graubünden als zentrale Lernplattform eingesetzt. Die Kurse dienen den Studierenden als Informations- und Lernressource, zudem wird Moodle für Leistungsnachweise verwendet. Diese Datenschutzhinweise richten sich an alle Nutzer:innen von Moodle, insbesondere an die Studierenden und Lehrenden.

14.1 Bearbeitung zur Erfüllung der Aufgaben als Hochschule mit kantonaler Trägerschaft

Die Bearbeitung der Daten durch die PH Graubünden erfolgt zur Erfüllung der Aufgaben, die den Hochschulen mit kantonaler Trägerschaft gemäss Gesetz über die Art. 9 GHF gesetzlich übertragen sind. Der Leistungsauftrag der PH Graubünden umfasst unter anderem das Erbringen von Lehre, Weiterbildung, Forschung und Dienstleistungen (Art. 2 GHF).

14.2 Welche Quellen und Daten nutzen wir?

Wir bearbeiten Daten, die Sie selbst aktiv eingeben, wie z.B. Forenbeiträge, Wiki-Beiträge, gelöste Aufgaben und Prüfungsantworten oder Ergänzungen zu Ihrem Profil. Sodann Daten über Bewertungen von Tests, Aufgaben und Leistungsnachweisen, welche entweder automatisch generiert oder aktiv durch Ihre:n Kursbetreuer:in eingegeben werden. Darüber hinaus erfassen wir, welche Kurse Sie nutzen und was Sie wann in diesen Kursen tun (z.B. welche Seiten Sie besucht haben). Sodann werden Stammdaten wie Ihr Name und Ihre E-Mail-Adresse bearbeitet. Diese können sowohl aus anderen internen Systemen als auch aus externen Diensten wie der SWITCH edu-ID stammen. Jeder Zugriff auf Moodle wird in Logfiles protokolliert. Dazu gehören technische Daten wie IP-Adresse, Informationen zum Browsertyp, Datum und Uhrzeit des Zugriffs.

14.3 Wofür bearbeiten wir Ihre Daten?

Die Daten werden bearbeitet, um die E-Learning-Angebote der PH Graubünden in den Bereichen Lehre und Weiterbildung zur Verfügung zu stellen und den Hochschulbetrieb zu gewährleisten. Dabei wird die Interaktion untereinander in verschiedenen Aktivitäten wie Chats, Foren, Umfragen oder Tests ermöglicht.

Ihre Daten werden bearbeitet, um Sie für die Nutzung von Moodle zu authentifizieren und zu autorisieren sowie die von Ihnen definierten Einstellungen in Moodle bei einer erneuten Anmeldung in gleicher Form wieder zur Verfügung zu stellen.

Die Speicherung der Logfiles erfolgt einerseits zu statistischen Zwecken, zur Sicherung des Dienstes, zur Analyse von Angriffen und zur Gewährleistung der technischen Stabilität. Zum anderen kann im Rahmen von Prüfungen und Leistungsnachweisen auf Logfiles zugegriffen werden, um zu überprüfen, ob Unredlichkeiten begangen wurden.

Moodle verfügt über eine Learning Analytics Funktion. Ziel dieser Funktion ist es, basierend auf Nutzungsdaten aus der Vergangenheit und dem gegenwärtigen Nutzungsverhalten Vorhersagen über den Lernerfolg einzelner Nutzer/innen zu machen und Diagnosen und Empfehlungen abzugeben. Derzeit wird diese Funktion an der PH Graubünden nur in ausgewählten Projekten zu internen Forschungs- und Entwicklungszwecken eingesetzt.

15 MIAPHGR

Die folgenden Datenschutzhinweise geben einen Überblick über die Erhebung und Bearbeitung Ihrer Daten in miaPHGR (https://mia.phgr.ch) der PH Graubünden (nachfolgend «miaPHGR»). miaPHGR wird an der PH Graubünden als Online-Self-Service-Tool für Hochschulangehörige eingesetzt. Es dient neben der Verwaltung der persönlichen Daten, der Registrierung für Angebote und Dienstleistungen der PH Graubünden sowie zu Informationszwecke. Diese Datenschutzhinweise richten sich an alle Nutzer:innen von miaPHGR, insbesondere an die Studierenden und Lehrenden.

15.1 Bearbeitung zur Erfüllung der Aufgaben als Hochschule mit kantonaler Trägerschaft

Die Bearbeitung der Daten durch die PH Graubünden erfolgt zur Erfüllung der Aufgaben, die den Hochschulen mit kantonaler Trägerschaft gemäss Gesetz über die Art. 9 GHF gesetzlich übertragen sind. Der Leistungsauftrag der PH Graubünden umfasst unter anderem das Erbringen von Lehre, Weiterbildung, Forschung und Dienstleistungen (Art. 2 GHF).

15.2 Welche Quellen und Daten nutzen wir?

Wir bearbeiten Daten, die Sie selbst aktiv eingeben, wie z.B. Ergänzungen und Aktualisierungen Ihrer Adress- und Kontaktdaten, erweiterte Personendaten und persönliche Dokumente wie Leistungsnachweise. Darüber hinaus erfassen wir, welche Angebote und Services Sie gebucht haben. Diese Informationen können sowohl aus anderen internen Systemen als auch aus externen Diensten wie der SWITCH edu-ID stammen. Jeder Zugriff auf miaPHGR wird in Logfiles protokolliert. Dazu gehören technische Daten wie IP-Adresse, Informationen zum Browsertyp, Datum und Uhrzeit des Zugriffs.

15.3 Wofür bearbeiten wir Ihre Daten?

Die Daten werden bearbeitet, um Ihnen einen zeitunabhängigen Zugriff auf Ihre Daten sowie Angebote und Services zu ermöglichen und damit den Betrieb der Hochschule kundenfreundlicher und effizienter zu gestalten.

Wir bearbeiten Ihre Daten, um Sie für die Nutzung von miaPHGR zu authentifizieren und zu autorisieren und um die von Ihnen definierten Einstellungen in miaPHGR bei einer erneuten Anmeldung in gleicher Form wieder zur Verfügung zu stellen. Bei der Erstregistrierung wird Ihre AHV-Nummer mit unseren Daten abgeglichen, um Sie eindeutig zu identifizieren und die Datenqualität zu gewährleisten. Ihre Kontaktdaten und die erweiterten Personendaten werden zur Sicherstellung des Hochschulbetriebs bearbeitet, insbesondere für Kommunikationszwecke, z.B. bei ausserordentlichen Ereignissen, oder für die Rechnungsstellung.

Die Speicherung der Logfiles erfolgt zu statistischen Zwecken, zur Sicherung des Dienstes, zur Analyse von Angriffen und zur Gewährleistung der technischen Stabilität.

16 WIE KÖNNEN SIE UNS KONTAKTIEREN?

Bei Fragen zu dieser Datenschutzerklärung oder zur Bearbeitung Ihrer Personendaten können Sie uns unter den folgenden Angaben kontaktieren.
PH Graubünden
Martin Berger
Datenschutzberater
Scalärastrasse 17
7000 Chur
datenschutz@phgr.ch

17 ÄNDERUNGEN DIESER DATENSCHUTZERKLÄRUNG

Diese Datenschutzerklärung ist nicht Bestandteil eines Vertrags mit Ihnen. Wir können diese Datenschutzerklärung jederzeit anpassen. Die auf dieser Website veröffentlichte Version ist die jeweils aktuelle Fassung. Wir behalten uns das Recht vor, Personen deren Kontaktangaben bei uns registriert sind, bei erheblichen Änderungen aktiv zu informieren. Generell gilt für Datenbearbeitungen jeweils die Datenschutzerklärung in der bei Beginn der betreffenden Bearbeitung aktuellen Fassung.
Diese Datenschutzerklärung wird von der Hochschulleitung in der Weisung Datenschutz und Datensicherheit (BR 210.100) als Anhang geführt. Bei Abweichungen gilt die Weisung.

Anhang VII – Weisung Datenschutz und Datensicherheit 210.100

DATENSCHUTZ IM UMGANG MIT BILD-, TON- UND VIDEOAUFZEICHNUNGEN

Version: 1.0
Autor: Martin Berger
Letzte Änderung: 01.07.2024
Klassifizierung: Öffentlich
Status: Aktiv

1 Zweck

1.1 Zweck dieses Anhangs ist es, Rechtssicherheit im Umgang mit personenbezogenen Bild-, Ton- und Videoaufzeichnungen (Aufzeichnungen), die an der PH Graubünden im Rahmen ihres vierfachen Leistungsauftrags erhoben werden, zu schaffen. Insbesondere soll deren Beschaffung, Aufbewahrung, Veränderung, Verwendung, Weitergabe und Löschung geregelt werden. Damit soll sichergestellt werden, dass die Rechte der Person, deren Personendaten aufgezeichnet werden, gewahrt bleiben.

2 Geltungsbereich

2.1 Diese Weisung gilt für alle Personen, die im Rahmen des vierfachen Leistungsauftrags der PH Graubünden Aufzeichnungen vornehmen und verwenden, d.h.

a) Mitarbeitende und Studierende der PH Graubünden (Hochschulangehörige);
b) Personen im Honorarverhältnis (Lehrbeauftragte, Praxislehrpersonen, u.a.);
c) Teilnehmende an Weiterbildungsveranstaltungen und -lehrgängen;
d) allfällige weitere Personen, die im Auftrag der PH Graubünden handeln.

3 Gegenstand

3.1 Der vorliegende Anhang zur Weisung Datenschutz und Datensicherheit (WDD) 210.100 regelt den Umgang mit Bild-, Ton- und Videoaufzeichnungen (Aufzeichnungen), die Personendaten enthalten und im Kontext des vierfachen Leistungsauftrags der PH Graubünden entstanden sind. Analog zu handhaben sind schriftliche Interviews und Gesprächsprotokolle, die Personendaten enthalten und den Rückschluss auf Personen erlauben.

3.2 Aufzeichnungen sind im Sinne dieses Anhangs als relevant einzustufen, wenn die aufgezeichnete Person bestimmbar ist. Dazu zählen insbesondere folgende Sachverhalte:

a) Bild-, Ton- und Video-Aufzeichnungen von Unterrichts- und Schulsituationen;
b) Bild-, Ton- und Video-Aufzeichnungen im Rahmen von Veranstaltungen der PH Graubünden;
c) Bild-, Ton- und Video-Dokumentationen von Ereignissen ausserhalb des Unterrichts (z.B. Förder-, Therapie- und Beratungssituationen in schulischen und ausserschulischen Kontexten);
d) Dokumentation von Arbeiten namentlich bezeichneter Schülerinnen und Schülern in Praktikumsklassen;
e) Video- oder Audio-Interviews mit Mitarbeitenden der PH Graubünden oder Dritten;
f) Schriftliche Interviews, Beobachtungen oder Gesprächsprotokolle mit namentlich bezeichneten Schülerinnen und Schülern, Studierenden, Praxislehrpersonen, Fach-/Förderlehrpersonen oder Mitarbeitenden.

3.3 Aufzeichnungen fallen nicht unter diesen Anhang, wenn die aufgezeichnete Person nicht bestimmbar ist. Dazu zählen insbesondere folgende Sachverhalte:

a) Video-Aufzeichnungen, auf denen Einzelpersonen nicht erkenn- und bestimmbar sind (z.B. Rückenansichten oder Aufzeichnungen mit verpixelten Gesichtern);
b) Audio-Aufzeichnungen von Gesprächen, bei denen Einzelpersonen nicht erkenn- und bestimmbar sind (z.B. ohne Namensnennung, unkenntliche oder nachgesprochen Stimme);
c) Anonymisierte Transkriptionen von video- oder audiographierten Gesprächen (Für die Erhebung selbst als ersten Prozessschritt ist jedoch eine Einverständniserklärung erforderlich siehe Ziffer 6);
d) Anonyme oder bereits bei der Erstellung anonymisierte schriftliche Interviews, Beobachtungen oder Gesprächsprotokolle;

e) Aufzeichnungen, die nur für das betreffende Setting verwendet werden (z.B. Video-Aufzeichnungen im Rahmen des Sportunterrichts zur Verbesserung von Bewegungsabläufen), nicht an Drittpersonen weitergegeben werden oder einsehbar sind und unmittelbar anschliessend an die Verwendung gelöscht werden.

3.4 Ausgenommen von den Bestimmungen dieser Weisung sind Gesprächsprotokolle, die im Rahmen eines Beschwerdegesprächs, einer internen Untersuchung, einer Schlichtung, eines Ausschlussgesprächs, der Gewährung rechtlichen Gehörs oder anderen gesetzlichen Verpflichtungen aufgezeichnet werden.

3.5 In jedem Fall müssen die Betroffenen über die Aufzeichnungen informiert werden.

4 Verantwortlichkeit

4.1 Die Verantwortung für die Einhaltung dieser Weisung trägt, soweit nichts anderes bestimmt ist, diejenige Person, welche die Aufzeichnung vornimmt.

4.2 Werden die Daten anschliessend an eine andere Person weitergegeben, geht die Verantwortung auf diese über.

5 Dokumentation zum Datenschutz

5.1 Es liegt im Ermessen der verantwortlichen Person im Sinne von Ziffer 4, in welcher Form sie sich vor der Beschaffung von Personendaten mit den folgenden Punkten vertraut macht und deren Einhaltung sicherstellt:

a) die Verwendung der Daten (Art und Zweck der Verwendung, Personenkreis, der Zugang zu den Daten hat, etc.);

b) den vollständigen Aufzeichnungs-, Nutzungs- und Bearbeitungsprozess bis zur Entfernung;

c) in welcher Form die gemäss Ziffer 6 erforderliche Einverständniserklärung eingeholt wird.

5.2 Die verantwortliche Person muss in der Lage sein, bei der Ausübung der Rechte der betroffenen Personen oder bei Datenschutzvorfällen Auskunft zu erteilen. Wird die Verantwortung gemäss Ziffer 4.2 übertragen, so geht die Verantwortung auf die neue Person über.

5.3 Ist in einer Lehr- oder Weiterbildungsveranstaltung die Aufzeichnung und Nutzung von Bild-, Ton- und Videoaufzeichnungen durch Studierende oder Weiterbildungsteilnehmende vorgesehen, so trägt die für die Veranstaltung zuständige Person die Verantwortung für die korrekte Anleitung der Studierenden oder Teilnehmenden bezüglich der Punkte gemäss Ziffer 5.1.

6 Einverständniserklärung

6.1 Vor der Erhebung von Personendaten ist die schriftliche Einverständniserklärung der betroffenen Personen bzw. der Erziehungsberechtigten einzuholen. Hierfür stehen auf der Datenschutzwebseite Vorlagen zur Verfügung.

6.2 Mit der Einverständniserklärung muss die verantwortliche Person gemäss Ziffer 4 die betroffenen Personen über mindestens folgende Punkte informieren:

a) den Verwendungszweck der Daten;

b) den Kreis der Personen, die Einblick in die Daten haben;

c) die Dauer der Datenspeicherung;

d) die allfällige Weiterverwendung der Daten nach Abschluss des Vorhabens oder deren Löschung und Vernichtung.

6.3 Bei einer Veränderung der in Ziffer 6.2 erwähnten Punkte ist eine neue Einverständniserklärung einzuholen.

6.4 Das Einverständnis von Hochschulangehörigen zur Erhebung von Personendaten im Anwendungsbereich dieser Weisung kann vorausgesetzt werden, solange es sich nicht um Personendaten im Sinne von Ziffer 3.4 oder besonders schützenswerte Personendaten im Sinne von Art. 5 Abs. 1 lit. b WDD handelt. Sie müssen jedoch gemäss Ziffer 3.5 über die Datenerhebung informiert und auf ihr Widerspruchsrecht hingewiesen werden.

6.5 Bei Kindern unter 14 Jahren erfolgt die schriftliche Einverständniserklärung in jedem Fall durch die Erziehungsberechtigten. Je nach Risikograd, der sich aus dem Verwendungszweck und der Verbreitung ergibt, können Kinder und Jugendliche zwischen 14 und 18 Jahren die Einverständniserklärung allein unterzeichnen. Die Information der Erziehungsberechtigten ist in jedem Fall sicherzustellen.

6.6 Wenn sich Kinder und Jugendliche unter 18 Jahren im Sinne von Ziffer 6.2 gegen eine Datenerhebung entscheiden, so muss dies unabhängig von ihrem Alter respektiert werden.

6.7 Eine Einverständniserklärung ist mindestens so lange aufzubewahren, wie die Aufzeichnung oder Teile davon existieren.

6.8 Personen, die ihr Einverständnis nicht erteilen, dürfen auf den Aufzeichnungen nicht bestimmbar sein.

7 Umgang mit Aufzeichnungen

7.1 Eine Bearbeitung personenbezogener Daten ist nur zulässig, wenn sie im Einklang mit den gesetzlichen Datenschutzbestimmungen erfolgt.

7.2 Personendaten sind so weit wie möglich zu anonymisieren oder zu pseudonymisieren. Nicht anonymisierte Aufzeichnungen sind unmittelbar nach der Aufzeichnung an einem sicheren Speicherort, zu dem nur die zur Einsichtnahme berechtigten Personen Zugang haben, zu speichern und an allen anderen Speicherorten (einschliesslich Papierkorb) zu löschen.

7.3 Die Weitergabe von Daten innerhalb und ausserhalb der PH Graubünden darf ausschliesslich physisch auf Datenträgern oder über die von der PH Graubünden zur Nutzung zur Verfügung gestellten IT-Applikationen/Speicherorte erfolgen (vgl. Weisung Verwaltung 610.110). Der Zugriff darf nur durch die in der Einwilligungserklärung genannten Zugriffsberechtigten erfolgen. Dies ist technisch sicherzustellen.

7.4 Soweit Daten der PH Graubünden von Dritten eingesehen oder weitergegeben werden, ist dies nur mit ausdrücklicher Einwilligung der betroffenen Person bzw. der/des Erziehungsberechtigten zulässig. Ausnahmen sind zulässig, soweit die Voraussetzungen von Ziffer 7.7 erfüllt sind oder eine gesetzliche Grundlage für die Weitergabe besteht.

7.5 Die in Ziffer 2 genannten Personen sind zur Verschwiegenheit über die aus den Personendaten gewonnenen Erkenntnisse ausserhalb des berechtigten Personenkreises verpflichtet. Die Verantwortlichen von Veranstaltungen, bei denen Personendaten bekannt gegeben werden, sind verpflichtet, die Anwesenden auf die Schweigepflicht hinzuweisen.

7.6 Im Falle einer Archivierung der Aufzeichnungen richtet sich diese nach den Bestimmungen des Art. 14 WDD.

7.7 Erfolgt die Bearbeitung durch Dritte (Auftragsbearbeiter), so ist im entsprechenden Vertragsverhältnis sicherzustellen, dass die Vorgaben gem. Art. 8 WDD eingehalten werden. Hierfür steht auf der Datenschutzwebseite eine Vorlage Auftragsdatenbearbeitungsvertrag (ADV) zur Verfügung.