

Mitteilungsblatt

der Universität Innsbruck

www.uibk.ac.at/service/c101/mitteilungsblatt

Studienjahr 2023/2024

Ausgegeben am 02.04.2024

38. Stück

Inhalt

648. Richtlinie des Rektorates für das Datenschutzmanagement an der Universität Innsbruck

Das Mitteilungsblatt erscheint jeweils am 1. und 3. Mittwoch jeden Monats.

Eigentümer, Herausgeber, Vervielfältigung und Vertrieb: Büro der Rektorin der Universität Innsbruck, Innrain 52, A-6020 Innsbruck. Für den Inhalt verantwortlich: Mag. Johannes Weber

648. Richtlinie des Rektorates für das Datenschutzmanagement an der Universität Innsbruck

I Präambel

Die vorliegende Richtlinie bildet die Grundlage für das interne Datenschutzmanagement an der Universität Innsbruck, das die Einhaltung der gesetzlichen Anforderungen sowie den Schutz der verarbeiteten personenbezogenen Daten an der Universität Innsbruck sicherstellt.

Datenschutz ist für die Universität Innsbruck sowohl im Forschungsbetrieb, als auch bei der Studierenden- und Mitarbeiterverwaltung von wesentlicher Bedeutung. Die Universität ist bestrebt, die gesetzlichen Anforderungen im Umgang mit personenbezogenen Daten zu erfüllen.

Insbesondere soll die Richtlinie:

- sicherstellen, dass auf Universitätsebene geeignete Maßnahmen zur Einhaltung der DSGVO umgesetzt werden,
- das Bewusstsein für die Notwendigkeit von strategischen, technischen und organisatorischen Maßnahmen zur Sicherstellung der Datenschutzanforderungen schaffen sowie
- die Kernprozesse und Schwerpunkte bei der Umsetzung der Datenschutzthemen an der Universität vorgeben und entsprechende Zuständigkeiten zu deren Umsetzung zuweisen.

II Grundsätze

1. Management Commitment

Das Rektorat betrachtet einen verantwortungsvollen, maßvollen, sicheren und den gesetzlichen Vorgaben entsprechenden Umgang mit personenbezogenen Daten als einen wesentlichen Grundwert und wird die Ziele und Prinzipien der Datenschutzbestimmungen in Einklang mit der Strategie und den Zielen der Universität unterstützen.

2. Stellenwert des Datenschutzes

Um die Anforderungen des Schutzes personenbezogener Daten langfristig und universitätsweit sicherzustellen, wird an der Universität Innsbruck ein Datenschutzmanagementsystem betrieben, welches – in Hinblick auf relevante rechtliche, technologische und organisatorische Belange – aktiv vom Rektorat mit entsprechenden zeitlichen, fachlichen und finanziellen Ressourcen ausgestattet wird.

3. Geltungsbereich

Die vorliegende Richtlinie gilt für die gesamte Universität Innsbruck.

Diese Richtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter, die entsprechend den zugewiesenen Rollen und Aufgaben mit der Umsetzung des Datenschutzes an der Universität Innsbruck betraut sind, soweit keine zwingend gesetzlichen Bestimmungen, insbesondere hinsichtlich einer festgelegten Weisungsfreiheit, dagegensprechen.

Die Umsetzung dieser Richtlinie kann in Form von technischen und organisatorischen Maßnahmen erfolgen. Dazu gehören auch bereichsspezifische Richtlinien, betriebliche Regelungen oder betriebliche Anweisungen. Die Mitarbeiterinnen und Mitarbeiter sind verpflichtet, diese einzuhalten.

Die Inhalte der Richtlinie bzw. alle ausführenden Dokumente dazu sind den MitarbeiterInnen im jeweiligen Geltungsbereich zu kommunizieren. Dies geschieht über geeignete Schulungen gemäß dem internen Schulungskonzept und die dauerhafte Bereitstellung der relevanten Informationen im Intranet der Universität Innsbruck.

4. Ziele der Richtlinie

Übergeordnetes Ziel der Universität Innsbruck bei der Einführung des Datenschutzmanagements ist die Sicherstellung der Einhaltung der Bestimmungen der EU-Datenschutz-Grundverordnung (EU-DSGVO, kurz DSGVO) bzw. der nationalen Datenschutzvorschriften) bei allen Abläufen, die personenbezogene Daten verarbeiten. Oberste Priorität neben der Sicherstellung der Datenschutzgrundsätze (gemäß Art. 5 DSGVO) haben dabei:

- Die Sicherung der Exzellenz bei Forschung mit personenbezogenen Daten
- Transparenter, sicherer und auf das zwingend erforderliche Ausmaß beschränkter Umgang mit personenbezogenen Daten Studierender, Mitarbeiter:innen und weiteren natürlichen Personen
- Die zeitnahe und faire Behandlung von Anfragen im Rahmen von Betroffenenrechten
- Gezielte Prüfroutinen beim Einsatz von Anwendungen (Hard und Softwaresysteme), die personenbezogene Daten verarbeiten

5. Konsequenzen bei Verstößen

Verstöße gegen gültige datenschutzrelevante Vorgaben durch Mitarbeiter:innen und / oder externe Auftragnehmer:innen können arbeitsrechtliche Sanktionen zur Folge haben bzw. zu straf- oder zivilrechtlichen Konsequenzen führen.

6. Gesetzliche Grundlagen

Bezugnehmend auf die Inhalte dieser Richtlinie dienen insbesondere folgende Rechtsnormen als Basis:

- EU-Datenschutz-Grundverordnung – EU-DSGVO
- Datenschutzgesetz – DSG
- Arbeitsverfassungsgesetz – ArbVG

III Datenschutzorganisation

Nachfolgend werden die Zuständigkeiten für die Umsetzung der Datenschutzmaßnahmen der Universität Innsbruck definiert.

1. Rektorat

Das Rektorat trägt die Gesamtverantwortung in Bezug auf die Einhaltung der gesetzlichen Bestimmungen des Datenschutzes. Durch entsprechende universitätsinterne Vorgaben, die vorliegende Datenschutzrichtlinie, Bereitstellung der notwendigen technischen, finanziellen und personellen Ressourcen und nachfolgende Setzung von Maßnahmen zur kontinuierlichen Sicherstellung der Angemessenheit kommt das Rektorat dieser Verantwortung nach. Das Managementsystem für Datenschutz wird als Prozess der kontinuierlichen Verbesserung mit dem Ziel implementiert, die einzelnen Maßnahmen in den Bereichen Datenschutz und Informationssicherheit so zu koordinieren, dass die Ziele dieser Richtlinie erreicht werden.

Durch regelmäßige Kontrollen und Berichte durch den Datenschutzbeauftragten und das interne Kontrollsystem überwacht das Rektorat die Umsetzung der Bestimmungen der Datenschutzrichtlinie und fördert das Bewusstsein der Mitarbeiterinnen und Mitarbeiter hinsichtlich Datenschutz.

Das Rektorat stellt Folgendes sicher:

- Sicherstellung der Einhaltung der gesetzlichen Bestimmungen der DSGVO sowie nationaler Datenschutzvorschriften
- Ordnungsgemäße und frühzeitige Einbindung der bzw. des Datenschutzbeauftragten in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen
- Ordnungsgemäße und frühzeitige Einbindung des Datenschutzgremiums entsprechend der Rahmenbetriebsvereinbarung zur Verarbeitung personenbezogener Daten sowie der Betriebsräte in den gesetzlich vorgesehenen Fällen
- Sicherstellung, dass ein Verzeichnis aller Verarbeitungstätigkeiten (Verfahrensverzeichnis) gemäß Art. 30 DSGVO geführt wird.

- Unterstützung der bzw. des Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben, insbesondere durch Zurverfügungstellung von Informationen zu personenbezogenen Daten und Verarbeitungsvorgängen.
- Sicherstellung, dass die bzw. der Datenschutzbeauftragte bei der Erfüllung ihrer bzw. seiner Aufgaben keine Anweisungen bzgl. der Ausübung dieser Aufgaben erhält.
- Sicherstellung, dass die Kontaktdaten der bzw. des Datenschutzbeauftragten veröffentlicht sind und an die Aufsichtsbehörde mitgeteilt werden
- Sicherstellung, dass die bzw. der Datenschutzbeauftragte wegen der Erfüllung ihrer bzw. seiner Aufgaben nicht abberufen oder benachteiligt wird.

2. Datenschutzbeauftragte:r

Die bzw. der Datenschutzbeauftragte wird vom Rektorat benannt, berichtet unmittelbar diesem und nimmt die Aufgaben gemäß Art. 39 DSGVO wahr.

Er bzw. sie führt die laufende Beratung und Unterrichtung des Rektorats, der Datenschutzkoordination, aller für die Umsetzung Zuständigen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten und hinsichtlich der rechtlichen Auslegungen nach der DSGVO sowie allen anwendbaren Datenschutzvorschriften durch.

Dabei erhält er bzw. sie angemessene Unterstützung durch Finanzmittel, Infrastrukturen sowie gegebenenfalls Personal.

Betroffene Personen können die bzw. den Datenschutzbeauftragte:n zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte im Zusammenhang stehenden Fragen zu Rate ziehen. Die bzw. der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

Die bzw. der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben, insbesondere seiner Überwachungsaufgaben durch Audits und andere Maßnahmen, dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie bzw. er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

3. Datenschutzkoordination

Die an der Universität Innsbruck eingerichtete Datenschutzkoordination setzt die Vorgaben des Rektorates hinsichtlich des Datenschutzmanagements an der Universität um. Die Datenschutzkoordination unterstützt die weiteren für die Umsetzung Zuständigen bei ihren definierten Datenschutzaufgaben.

Die Datenschutzkoordination ist insbesondere zuständig für:

- Die Führung und regelmäßige Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO.
- Beratung und Unterstützung beim Aufbau des Datenschutzmanagementsystems (Aufgaben, Prozesse, Dokumente)
- Beratung und Unterstützung im Zusammenhang mit der Bearbeitung von Anfragen im Zusammenhang mit Betroffenenrechten
- Die Planung und Durchführung des internen Schulungskonzepts zum Datenschutz. Sie arbeitet bei der Durchführung mit anderen Dienstleistungseinheiten zusammen.

4. Zentraler Informatikdienst

Der zentrale Informatikdienst sorgt für die Umsetzung der informationssicherheitsrelevanten Anforderungen des Datenschutzes in seinem Zuständigkeitsbereich.

Der zentrale Informatikdienst ist durch die Zuständigen für Verarbeitungstätigkeiten frühzeitig in alle Projekte und Prozesse einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.

5. Leiter:innen von Organisationseinheiten, Instituten und Forschungsprojekten (Bereichszuständige)

Die Leiter:innen von Organisationseinheiten und Instituten sowie von Forschungsprojekten sind zuständig für die ordnungsgemäße Datenverarbeitung in ihrem Zuständigkeitsbereich (Bereichszuständige). Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in dieser Richtlinie enthaltenen Anforderungen des Datenschutzes in Ihrem Zuständigkeitsbereich entsprechend berücksichtigt und umgesetzt werden.

Die Aufgabe aller Bereichszuständigen ist es, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung der internen Vorgaben sicherzustellen und entsprechend definierten Prozesse einzuführen.

Insbesondere ist von den Bereichszuständigen sicherzustellen, dass alle MitarbeiterInnen in ihrem Zuständigkeitsbereich die einschlägigen Richtlinien und Vorgaben dazu zur Kenntnis genommen haben.

Die Bereichszuständigkeit für eine Verarbeitungstätigkeit und die vollständige Dokumentation gemäß DSGVO liegt bei der Leitung der bei einem internen Verwaltungsprozess / Projekt für die Durchführung und Ausgestaltung federführenden Dienstleistungseinheit bzw. bei der Leitung eines Forschungsprojekts und kann nicht delegiert werden. Die jeweils zuständige Leitung trägt, in Abstimmung mit der Datenschutzkoordination, dafür Sorge, dass die Dokumentation und die regelmäßige Aktualisierung der Verarbeitungen personenbezogener Daten und der technischen und

organisatorischen Maßnahmen (TOM) im Verzeichnis der Verarbeitungstätigkeiten erfolgt und die Mitarbeiterinnen und Mitarbeiter, an die diese Aufgabe delegiert wird, entsprechende zeitliche Ressourcen haben.

6. Datenschutzdelegierte

Es wird pro Organisationseinheit der Universität Innsbruck ein:e Datenschutzdelegierte:r durch die Leitung der Organisationseinheit ernannt, wobei die Leitung diese Funktion auch selbst übernehmen kann. In Ausnahmefällen können kleinere, eng verzahnte Organisationseinheiten eine:n gemeinsame:n Datenschutzdelegierte:n ernennen. Die Datenschutzdelegierten unterstützen die Datenschutzkoordination unter deren Anleitung und Schulung in der Umsetzung von Datenschutzvorgaben auf Ebene der Organisationseinheiten und stellen sicher, dass wichtige Datenschutzthemen an die Datenschutzkoordination herangetragen und institutsübergreifend gelöst werden.

7. Datenschutzgremium

Die Aufgaben und Kompetenzen des Datenschutzgremiums werden in der Rahmenbetriebsvereinbarung zur Verarbeitung personenbezogener Daten beschrieben und beruhen insbesondere auf den gesetzlichen Bestimmungen zur betrieblichen Mitbestimmung und zum Datenschutz für Arbeitnehmerinnen und Arbeitnehmer. Dem Datenschutzgremium kommen allgemeine Beratungsaufgaben und Aufgaben bei der Protokolleinsicht zu.

8. Anwender:innen

Mitarbeiter:innen sind zur Einhaltung der vorgegebenen Regeln im Umgang mit personenbezogenen Daten, soweit diese sie oder ihn betreffen, verpflichtet. Sie haben die Pflicht, sich aktiv an den internen Schulungsmaßnahmen zu beteiligen und alle übergeordneten sowie bereichsspezifischen Datenschutz- und Datensicherheitsmaßnahmen einzuhalten, die ihnen auf geeigneten Wegen zur Kenntnis gebracht wurden.

IV Grundsätzliches zur Verarbeitung von personenbezogenen Daten

Die Bestimmungen der DSGVO sowie der nationalen Datenschutzvorschriften in den jeweils geltenden Fassungen sind uneingeschränkt von allen Mitarbeiter:innen, Auftragsverarbeiter:innen und sonstigen externen Auftragnehmer:innen einzuhalten. Die Bereichszuständigen stellen dies in ihrem Zuständigkeitsbereich sicher.

Alle Mitarbeiter:innen sind mit Dienstantritt schriftlich zur Wahrung des Datengeheimnisses gemäß § 6 DSG zu verpflichten. Diese Verpflichtung hat Verschwiegenheit über alle Umstände, die den Mitarbeiterinnen und Mitarbeitern aufgrund ihrer Tätigkeit bekannt werden, zu beinhalten. Das Datengeheimnis hat über das Ende des Dienstverhältnisses hinaus zu gelten.

V Verzeichnis der Verarbeitungstätigkeiten

Die Datenschutzkoordination ist dafür zuständig, ein Verzeichnis gemäß Art. 30 DSGVO aller Verarbeitungstätigkeiten (Verfahrensverzeichnis) zu führen. Art. 30 DSGVO definiert, welche Inhalte in das Verzeichnis aufzunehmen sind. Das Verfahrensverzeichnis ist schriftlich zu führen und der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Werden neue Verarbeitungstätigkeiten personenbezogener Daten begonnen (z.B. im Rahmen neuer Projekte, Verfahren) oder bestehende geändert, sind diese im Voraus der Datenschutzkoordination zu melden. Die Meldung hat entsprechend den universitätsinternen Vorgaben zu erfolgen, insbesondere sind auch die geltenden Betriebsvereinbarungen und Richtlinien zu beachten.

Alle Bereichszuständigen, die für die Einrichtung, Durchführung oder Änderung von Verarbeitungstätigkeiten personenbezogener Daten im Sinne der DSGVO zuständig sind, sind verpflichtet, diese Meldungen zeitgerecht durchzuführen und in Abstimmung mit der Datenschutzkoordination entsprechende Routinen in ihrem Zuständigkeitsbereich einzuführen. Alle Unterlagen zur Dokumentation und Nachbearbeitung im Verfahrensverzeichnis sind der Datenschutzkoordination zeitgerecht bereitzustellen.

Soweit die Universität als Auftragsverarbeiterin i.S.d. Art. 30 Abs. 2 DSGVO tätig ist, führt die Datenschutzkoordination auch ein entsprechendes Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter. Dieses umfasst alle Dienstleistungen, die die Universität für Dritte erbringt und bei denen personenbezogene Daten für einen Auftraggeber verarbeitet werden. Entsprechende Meldungen sind von den Bereichszuständigen an die Datenschutzkoordination zu erstatten.

VI Risikobewertung und Datenschutz-Folgeabschätzung

Bei der Einführung oder wesentlichen Änderung von Verarbeitungstätigkeiten von personenbezogenen Daten ist durch die Bereichszuständigen eine Risikobewertung durchzuführen. Dabei ist zu ermitteln, ob diese Verarbeitung nach Art, Umfang, Kontext und Zweck ein hohes Risiko für die Betroffenen darstellt. Die Datenschutzkoordination und der bzw. die Datenschutzbeauftragte unterstützen die Bereichszuständigen bei der Risikobewertung. Ergibt die Risikobewertung das Vorliegen eines mittleren, hohen oder sehr hohen Risikos, ist der Sachverhalt inklusive der Risikobewertung dem zuständigen Rektoratsmitglied zur Entscheidung vorzulegen. Abhängig vom festgestellten Risiko sind nachfolgend angemessene technische und organisatorische Datensicherheitsmaßnahmen festzulegen und zu ergreifen.

Besteht bei einer Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen, ist der Bereichszuständige verpflichtet, vorab eine Datenschutz-Folgeabschätzung durchzuführen. Hierbei sind die bzw. der

Datenschutzbeauftragte sowie die Datenschutzkoordination beizuziehen und das Datenschutzgremium zu informieren. Das Ergebnis ist schriftlich festzuhalten und im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

VII Bewusstsein und Schulungen

Die Datenschutzkoordination sorgt in Abstimmung mit der Personalentwicklung für die Erstellung eines Schulungskonzeptes und die regelmäßige Durchführung von Schulungen.

VIII Datenschutzvorfälle

Die Universität ist im Fall einer Verletzung des Schutzes personenbezogener Daten verpflichtet unverzüglich zu reagieren und entsprechende Meldungen und Maßnahmen entsprechend Art. 33 und 34 DSGVO zu treffen bzw. durchzuführen. Die Bearbeitung von Datenschutzvorfällen wird in einem separaten Prozess geregelt.

Durch Bekanntgabe der universitätsinternen Vorgaben sowie durch Schulung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter wird die unverzügliche Meldung sichergestellt.

IX Betroffenenrechte

Die Universität Innsbruck ist verpflichtet, die Rechte der Betroffenen zu wahren und sicherzustellen, dass diese bei Geltendmachung fristgerecht erfüllt werden.

Dies betrifft insbesondere folgende Betroffenenrechte:

- Recht auf Auskunft (gemäß Art. 15 DSGVO)
- Recht auf Berichtigung (gemäß Art. 16 DSGVO)
- Recht auf Löschung / Recht auf Vergessenwerden (gemäß Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (gemäß Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (gemäß Art. 20 DSGVO)
- Recht auf Widerspruch (gemäß Art. 21 DSGVO)

Da ab dem Zeitpunkt von eingehenden Anfragen, welche die Betroffenenrechte adressieren, gesetzliche Fristen zu laufen beginnen, haben die Bereichszuständigen bei Kenntnisnahme dafür Sorge zu tragen, dass solche Anfragen unverzüglich an die Datenschutzkoordination weitergeleitet werden. Die Datenschutzkoordination übernimmt, gegebenenfalls in Abstimmung mit den Bereichsverantwortlichen, dem Datenschutzbeauftragten sowie dem zuständigen Rektoratsmitglied, die Bearbeitung.

X Informationspflichten

Die Bereichszuständigen haben für Verarbeitungen von personenbezogenen Daten in ihrem Zuständigkeitsbereich gemeinsam mit der Datenschutzkoordination dafür Sorge zu tragen,

dass den Betroffenen alle notwendigen Informationen in geeigneter Weise zur Verfügung gestellt werden. Dies betrifft vor allem die Übermittlung von Informationen gemäß folgenden Artikeln:

- Art. 13 DSGVO (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person)
- Art. 14 DSGVO (Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden)

XI Technische und organisatorische Maßnahmen (TOMs) Privacy by Design / Privacy by Default

Die Bereichszuständigen haben, in Abstimmung mit dem zentralen Informatikdienst und der Datenschutzkoordination, geeignete technische und organisatorische Maßnahmen (TOMs) zur Sicherung der in ihrem jeweiligen Zuständigkeitsbereich verarbeiteten personenbezogenen Daten zu treffen, abhängig

- vom Stand der Technik,
- den Implementierungskosten,
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Diese Maßnahmen haben jedenfalls die Erfordernisse des Art. 32 DSGVO zu erfüllen und ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Hinsichtlich der Definition des Stands der Technik erfolgt die Orientierung an den Leitlinien des Europäischen Datenschutzausschusses, (inter-)nationalen Normen und Best-Practice-Ansätzen wie z. B. ISO/IEC 27001 oder BSI IT-Grundschutz.

Weiters stellen die Bereichszuständigen sicher, dass die Datenschutzerfordernisse bereits von vornherein in Gesamtkonzeptionen von Datenverarbeitungen miteinbezogen werden (z.B. bei der Einführung neuer Anwendungen) (Privacy by Design) und tragen dafür Sorge, dass Produkte oder Dienstleistungen standardmäßig datenschutzfreundlich konfiguriert sind (Privacy by Default). Sie werden dabei von der Datenschutzkoordination, dem Datenschutzbeauftragten und den jeweils für die IT-Systeme zuständigen Personen unterstützt.

XII Rahmenbedingungen für die Auftragsverarbeitung

Die Bereichszuständigen stellt, ggf. in Abstimmung mit der Datenschutzkoordination und den Zeichnungsberechtigten, sicher, dass bei der Auswahl und Beauftragung von Auftragsverarbeiter:innen die Rahmenbedingungen gemäß Art. 28 und Art. 29 DSGVO eingehalten und in dokumentierter Form vereinbart werden. Dazu ist mit jedem bzw. jeder Auftragsverarbeiter:in (z.B. Dienstleister:innen), die bzw. der personenbezogene Daten im

Auftrag der Universität Innsbruck verarbeitet, ein Vertrag zur Auftragsdatenverarbeitung abzuschließen.

Bereichszuständige müssen Verarbeitungen personenbezogener Daten, die im Auftrag für Dritte erfolgen, zeitgerecht vor Aufnahme der Dienstleistung der Datenschutzkoordination melden, damit diese dokumentiert und im Verzeichnis der Verarbeitungstätigkeiten der Universität als Auftragsverarbeiterin erfasst werden.

XIII Rahmenbedingungen für gemeinsam Verantwortliche

Für den Fall, dass gemeinsam mit externen Partner:innen die Mittel und Zwecke der Verarbeitung personenbezogener Daten festgelegt werden (Joint Controller), ist es Aufgabe des Bereichszuständigen, ggf. in Zusammenarbeit mit der Datenschutzkoordination und dem Zeichnungsberechtigten, eine Vereinbarung abzuschließen, in der die Aufgaben und Verantwortlichkeiten gemäß DSGVO der Universität und der Vertragspartner (Joint Controller) insbesondere gegenüber den Betroffenen, deren Daten sie verarbeiten, festgelegt sind. Die wesentlichen Bestimmungen daraus sind den Betroffenen zur Verfügung zu stellen. Dabei sind die internen Vorgaben zu beachten.

XIV Überprüfung und Aufrechterhaltung des Datenschutzmanagementsystems (DSMS)

Das Datenschutzmanagement an der Universität Innsbruck wird als kontinuierlicher Prozess verstanden, der laufend zu überprüfen, aufrecht zu erhalten und im Bedarfsfall anzupassen oder zu verbessern ist.

Insbesondere sind dazu regelmäßige Audits zur Überprüfung der Vollständigkeit, Korrektheit und Wirksamkeit der umgesetzten Prozesse und implementierten Maßnahmen und Berichte der Ergebnisse an das Rektorat (Jour Fixe, Managementmeetings) durchzuführen.

Für das Rektorat

Univ.-Prof. Dr. Veronika Sexl

Rektorin
