universität
innsbruck

RAHMENBETRIEBSVEREINBARUNG ZUR VERARBEITUNG PERSONENBEZOGENER DATEN

universität innsbruck

Präambel

Die Universität verarbeitet in verschiedenen Bereichen personenbezogene Daten von Mitarbeiter_innen, insbesondere zu Zwecken der Personalwirtschaft und in der Kommunikation.

Die Universität und die Betriebsräte stimmen überein, dass die von der Universität eingesetzten Systeme für eine effiziente Administration, die Gewährleistung der Sicherheit an der Universität sowie für eine zeitgemäße interne und externe Kommunikation notwendig sind. Einigkeit besteht auch darüber, dass IT Systeme aufgrund der rasant fortschreitenden technologischen Entwicklung ständig einem hohen Anpassungs- bzw. Aktualisierungsbedarf unterliegen und dass die Universität daher veranlasst ist, diesem dynamischen Wandel Folge zu leisten.

Diese Rahmenbetriebsvereinbarung dient dazu, die Umsetzung von rechtlichen Bestimmungen zur Verhinderung des Datenmissbrauchs (EU-DSGVO, DSG und ArbVG) zu unterstützen. Insbesondere sollen die Mitarbeiter_innen vor einer unberechtigten Verarbeitung personenbezogener Daten und einer systematischen, die Menschenwürde des bzw. der Einzelnen berührenden Kontrolle geschützt werden. Die Systeme und Datenverarbeitungen werden nicht zu Zwecken der systematischen, kollektiven oder individuellen Leistungs- und Verhaltenskontrolle genutzt.

Gleichzeitig ist sicherzustellen, dass die Universitätsleitung die ihr in den Gesetzen übertragenen Aufgaben rechtzeitig und vollständig wahrnehmen kann.

universität innsbruck

1. Geltungsbereich und Regelungsgegenstand

Diese Betriebsvereinbarung gilt:

a) persönlich:

für alle Mitarbeiter_innen der Universität Innsbruck mitsamt ihren Außenstellen sowie für die Bediensteten des Amtes der Universität Innsbruck, dh für jede vom Rektorat verschiedene natürliche Person (zB auch für Projektmitarbeiter_innen, Ferialarbeitskräfte, Leiharbeitskräfte, „externe" Lehrbeauftragte bzw Lektor_innen etc).

Nicht vom Anwendungsbereich erfasst ist insbesondere die Verarbeitung von Studierendendaten oder von Daten sonstiger Personen, über die die Universität verfügt, auch wenn die Daten mit denselben Systemen verarbeitet werden wie die Mitarbeiter_innendaten.

b) sachlich:

für die Verarbeitung personenbezogener Mitarbeiter_innendaten durch die Universität Innsbruck.

Die Grundsätze dieser Rahmenbetriebsvereinbarung gelten sinngemäß für alle bestehenden und zukünftigen (Zusatz-)Betriebsvereinbarungen, die (auch) die Verarbeitung personenbezogener Mitarbeiter_innendaten zum Gegenstand haben.

c) zeitlich:

Die gegenständliche Betriebsvereinbarung ersetzt vollständig die bisherige „Rahmenbetriebsvereinbarung zur automationsunterstützten Verwendung personenbezogener Daten" vom 30.04.2009.

Sie gilt ab dem Datum der Unterzeichnung vorerst befristet bis 31.12.2021.

In dieser Zeit besteht eine Phase der beiderseitigen Prüfung der Anwendbarkeit dieser Vereinbarung, binnen der - auf Wunsch einer Vertragsseite - ergänzende Gespräche mit dem Ziel einer einvernehmlichen Abänderung geführt werden können.

Sollte bis acht Wochen vor Ablauf der Befristung keine Vertragsseite gegenüber der anderen Partei ausdrücklich und schriftlich auf ein Auslaufen der Betriebsvereinbarung mit Fristende bestehen, verlängert sich diese Betriebsvereinbarung jeweils um weitere zwölf Monate.

2. Zielsetzung

Die Universität und die Betriebsräte stimmen überein, dass

a) diese Betriebsvereinbarung zur Qualitätssicherung und Transparenz bei der Verwendung personenbezogener Daten durch die Universität dient,
b) die Universität personenbezogene Daten nur im gesetzlich vorgeschriebenen und betrieblich notwendigen Ausmaß verarbeitet,
c) Datenverarbeitungen durch die Universität dazu dienen, die sich aus Gesetzen, Kollektivverträgen, Betriebsvereinbarungen oder Arbeitsverträgen ergebenden Aufgaben der Personalwirtschaft zu unterstützen und zu erleichtern sowie die in der Präambel genannten Ziele umzusetzen.

universität innsbruck

3. Rechtliche Grundlagen

Die Betriebsvereinbarung wird auf der Grundlage der gesetzlichen Bestimmungen abgeschlossen, insbesondere

- den Bestimmungen des Arbeitsverfassungsgesetzes (ArbVG), im Besonderen die §§ 89, 91, 92, 96, 96a und 97 sowie
- den Bestimmungen der EU-Datenschutzgrundverordnung (EU-DSGVO) und des Datenschutzgesetzes (DSG).

4. Funktionen im Bereich Datenschutz und Informationssicherheit

An der Universität Innsbruck gibt es zum Zeitpunkt des Abschlusses dieser Betriebsvereinbarung vier offizielle Funktionen im Bereich des Datenschutzes und der Informationssicherheit:

a) Datenschutzbeauftragte_r iSd EU-DSGVO

Die Aufgaben der/des Datenschutzbeauftragte_n ergeben sich unmittelbar aus Art. 39 der EU-DSGVO. Die/der Datenschutzbeauftragte ist die zentrale Kontrollinstanz iS Datenschutz und Informationssicherheit an der Universität Innsbruck. Zu ihren/seinen Aufgaben zählen insbesondere:

- Überwachung der Einhaltung der EU-DSGVO
- Auf Anfrage Beratung im Zusammenhang mit Datenschutz-Folgenabschätzungen
- Zusammenarbeit mit der und erste Anlaufstelle für die Aufsichtsbehörde

Die/der Datenschutzbeauftragte ist in der Ausübung ihrer/seiner Funktion weisungsfrei.

b) Datenschutzkoordinator_in als interne Ansprechperson

Ein/e Datenschutzkoordinator_in sorgt universitätsintern für die Umsetzung der EU-DSGVO und hat damit eine operative Funktion. Ihre/seine Aufgaben sind im Wesentlichen:

- Aufbau und Weiterentwicklung eines Datenschutzmanagementsystems
- Aufbau/Führen des Verarbeitungsverzeichnisses
- Erste Anlaufstelle für Auskunftsbegehren und Koordination der Maßnahmen zur Gewährleistung der Betroffenenrechte
- Koordination von Datenschutz-Folgenabschätzungen
- Universitätsinterne Schulungen und Information

c) Informationssicherheitsbeauftragte_r

Die/Der Informationssicherheitsbeauftragte plant und koordiniert die Umsetzung von Maßnahmen zur Gewährleistung der Informationssicherheit.

- Aufbau eines Informationssicherheitsmanagementsystems
- Planung und Koordination der Umsetzung von technischen und organisatorischen Sicherheitsmaßnahmen
- Operative Sicherstellung der Informationssicherheit
- Operative Umsetzung des Data-Breach-Prozesses

universität innsbruck

- Universitätsinterne Schulungen und Information

d) Datenschutzgremium

Das Datenschutzgremium setzt sich aus Mitgliedern der Betriebsräte und des Rektorats zusammen und hat eine beratende Funktion. Seine Aufgaben und Rechte ergeben sich aus dieser Betriebsvereinbarung.

5. Datenschutzgremium

Zur Beratung aller Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten wird an der Universität Innsbruck ein Datenschutzgremium eingerichtet. Die Entscheidungskompetenzen des Rektorats und der Betriebsräte gemäß ArbVG bleiben davon unberührt.

Die Beratungen und Ergebnisse des Datenschutzgremiums dienen dem Rektorat und den Betriebsräten als Entscheidungsgrundlagen und als Information für die Ausübung der gesetzlich geregelten Mitwirkungs- bzw. Zustimmungsrechte.

Das Rektorat und die Betriebsräte verpflichten sich, im Konfliktfall erst dann den Rechtsweg zu beschreiten, wenn nach Beratung im Datenschutzgremium keine Einigung zustande gekommen bzw. ein innerbetrieblicher Schlichtungsversuch erfolglos geblieben ist. Dies ist dann der Fall, wenn im Zuge der Beschlussfassung keine Einigung erfolgt oder ein Beschluss innerhalb von zwei Monaten ab der ersten Befassung im Datenschutzgremium nicht zustande gekommen ist.

a) Zusammensetzung

Dem Datenschutzgremium gehören an:

- vier durch das Rektorat zu benennende Vertreter_innen (ordentliche Mitglieder),
- jeweils zwei Vertreter_innen der beiden Betriebsräte (ordentliche Mitglieder),
- die/der Datenschutzkoordinator_in als Mitglied ohne Stimmrecht (außerordentliches Mitglied).

Das Datenschutzgremium kann bei Bedarf Fachpersonal seiner Wahl zur Beratung beiziehen.

b) Geschäftsordnung

Zur Bewältigung der organisatorischen Abläufe hat das Datenschutzgremium eine Geschäftsordnung mit folgendem Mindestinhalt festzulegen:

- Vorsitzführung
- Protokollführung
- Art der Beschlussfassung
- Art der Einberufung
- Sitzungsintervall
- Regelung der internen Informationsweitergabe.

universität innsbruck

c) Konstituierung

Die Konstituierung des Datenschutzgremiums und die Wahl einer/eines Vorsitzenden aus dem Kreis der ordentlichen Mitglieder haben innerhalb von drei Monaten nach Abschluss dieser Betriebsvereinbarung zu erfolgen.

d) Vertretung nach außen

Das Datenschutzgremium wird nach außen durch die/den Vorsitzende_n vertreten.

e) Beschlussfähigkeit

Das Datenschutzgremium ist beschlussfähig, wenn von Seiten des Rektorats zwei und von Seiten der beiden Betriebsräte je ein Mitglied anwesend sind. Gültige Beschlüsse können nur einhellig gefasst werden und sind zu protokollieren.

f) Sitzungen

Das Datenschutzgremium tagt in regelmäßigen Intervallen, die in der Geschäftsordnung festzulegen sind.

Zwischenzeitliche Einberufungen durch die/den Vorsitzende_n sind möglich.

Die/der Vorsitzende hat auch auf begründetes Verlangen eines Mitglieds des Datenschutzgremiums binnen fünf Arbeitstagen eine Sitzung einzuberufen. Jede Einberufung hat eine schriftliche Tagesordnung zu enthalten und ist spätestens zwei Arbeitstage vor der Sitzung allen Mitgliedern des Datenschutzgremiums zu übergeben.

6. Rechte des Datenschutzgremiums

a) Information zu Datenverarbeitungen

Das Datenschutzgremium ist über alle Verarbeitungen personenbezogener Mitarbeiter_innendaten in allgemein verständlicher Form zu informieren. Die Information hat so zu erfolgen, dass das Datenschutzgremium in der Lage ist, die Art, den Umfang und die Auswirkungen der Datenverarbeitung zu beurteilen. Dies umfasst insbesondere die in Anhang 1 angeführten Informationen.

Sofern personenbezogene Daten mittels Informations- und Kommunikationstechnik (IKT) verarbeitet werden, ist bereits in der Planungsphase, dh vor Einführung bzw Veränderung des IKT-Systems, das Datenschutzgremium einzubinden. Dabei sind zusätzlich zu den in Anhang 1 angeführten Punkten folgende Informationen zur Verfügung zu stellen:

- Zielsetzung und geplante Auswirkungen des Projektes (zB Personalaufwand, Veränderung von Arbeitsabläufen)
- Zeitplan des Projektablaufes bis zur Umsetzung
- Projektleiter_in, System-Verantwortliche und involvierte Projekt-Team-Mitglieder
- externe Berater_innen
- externe Programmierer_innen

Die Information an das Datenschutzgremium hat noch vor der Implementierung, dh vor der Einführung bzw wesentlichen Veränderung der Datenverarbeitung zu erfolgen, dies jedenfalls so

rechtzeitig, dass eine Beratung über die Einführung bzw Veränderung der Verarbeitung noch durchgeführt werden kann. In den gesetzlich vorgesehenen Fällen ist die Zustimmung der Betriebsräte zu erwirken.

Die/der Vorsitzende des Datenschutzgremiums ist verpflichtet, alle ihr/ihm von Seiten der Universität übermittelten Informationen binnen zwei Arbeitstagen an die Mitglieder des Datenschutzgremiums weiterzuleiten.

b) Information zu Richtlinien und Maßnahmen

Das Datenschutzgremium ist laufend über wesentliche Änderungen im Bereich Datenschutz und Informationssicherheit zu informieren, insbesondere bei Einführung oder Änderung von Richtlinien oder Maßnahmen in den Bereichen Schulung, Sensibilisierung und Wahrung der Betroffenenrechte.

c) Einsicht in das Verarbeitungsverzeichnis

Den Mitgliedern des Datenschutzgremiums ist auf Verlangen Einsicht in das Verarbeitungsverzeichnis der Universität zu gewähren.

d) Information zu Datenschutzverletzungen

Das Datenschutzgremium ist über Verletzungen des Schutzes personenbezogener Daten („data breach") inklusive der getroffenen Maßnahmen zu informieren.

e) Mitwirken an der Beurteilung von Risiken und Datenschutz-Folgenabschätzung

Das Datenschutzgremium ist bei der allgemeinen Beurteilung von Risiken, die durch die Verarbeitung personenbezogener Daten entstehen, sowie bei der Durchführung der Datenschutz-Folgenabschätzung beratend hinzuzuziehen.

f) Recht auf Hinzuziehung externer Berater_innen

Das Datenschutzgremium hat das Recht, bei Bedarf externe Berater_innen beizuziehen.

g) Berichte zu Datenschutz und Informationssicherheit

Dem Datenschutzgremium sind jährlich Berichte zu den Themen Datenschutz und Informationssicherheit vorzulegen. Diese behandeln den aktuellen Stand und die wesentlichen Problembereiche in Bezug auf Datenschutz und Informationssicherheit und umfassen zumindest folgende Punkte:

- Übersicht über neue oder geänderte Datenverarbeitungen des letzten Jahres bzw seit dem letzten Bericht
- aktuelle Entwicklungen
- ggf geänderte rechtliche Rahmenbedingungen
- Datenschutz- und Informationssicherheitszwischenfälle
- umgesetzte und geplante Maßnahmen und Projekte
- erstellte oder geänderte Konzepte und Richtlinien (zB Schulungskonzept oder Informationssicherheitsrichtlinie)
- quantitative Leistungsindikatoren zur Dokumentation der Wirksamkeit von Datenschutz und Informationssicherheit (zB durchgeführte Schulungen und Beratungsgespräche, Anzahl von Zwischenfällen, Anzahl neuer oder geänderter Datenverarbeitungen etc). Die verwendeten

universität innsbruck

Indikatoren sind vorab mit dem Datenschutzgremium zu beraten und nach Möglichkeit über längere Zeit unverändert zu verwenden.

h) Beratung durch die/den Datenschutzbeauftragte_n

Das Datenschutzgremium wird einmal jährlich von der/dem Datenschutzbeauftragten über die Wahrnehmung ihrer/seiner Pflichten und Aufgaben informiert. Auf Verlangen des Datenschutzgremiums kann die/der Datenschutzbeauftragte zu weiteren Sitzungen des Datenschutzgremiums hinzugezogen werden.

i) Einbindung in die Bestellung und Abberufung der Datenschutzkoordinatorin/des Datenschutzkoordinators

Das Datenschutzgremium wird rechtzeitig über eine (Neu)Bestellung der Datenschutzkoordinatorin/des Datenschutzkoordinators informiert und hat das Recht, ein Mitglied zu benennen, das durch die ausschreibende Stelle in den Bestellungsprozess eingebunden wird und diesen in beratender Funktion begleitet. Die Einbindung umfasst jedenfalls die Einsichtnahme in die Bewerbungsunterlagen und in den Besetzungsvorschlag. Das ausgewählte Mitglied darf dem Datenschutzgremium pauschal über das Auswahlverfahren Auskunft erteilen, jedoch keine personenbezogenen Informationen der Bewerber_innen weitergeben.

Über die Abberufung der Datenschutzkoordinatorin/des Datenschutzkoordinators ist das Datenschutzgremium unverzüglich zu informieren.

7. Aufgaben des Datenschutzgremiums

Aufgabe des Datenschutzgremiums ist es, einen Interessenausgleich zwischen dem Rektorat und den beiden Betriebsräten herbeizuführen. Das Datenschutzgremium ist auch zu befassen, wenn bei Fragen im Zusammenhang mit dieser Betriebsvereinbarung und darauf beruhenden Betriebsvereinbarungen keine Einigung erzielt werden kann.

a) Allgemeine Beratungsaufgaben

Das Datenschutzgremium berät das Rektorat und die Betriebsräte bzgl der gemeldeten Datenverarbeitungen, zur Umsetzung und Einhaltung dieser Betriebsvereinbarung sowie der jeweils geltenden gesetzlichen Bestimmungen, insbesondere der Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten (Art 5 EU-DSGVO).

Das Datenschutzgremium hat alle nach Punkt 6 lit. a gemeldeten Datenverarbeitungen umgehend zu behandeln und kann dazu eine Stellungnahme abgeben, in der es technische oder organisatorische Maßnahmen vorschlagen und allenfalls von der Verwendung personenbezogener Daten abraten kann.

Weiters unterstützt das Datenschutzgremium die/den Datenschutzkoordinator_in bei der allgemeinen Bewertung von Risiken von Datenverarbeitungen und Maßnahmen zur Risikobehandlung sowie bei der Durchführung der Datenschutz-Folgenabschätzung (Art 35 EU-DSGVO).

Das Datenschutzgremium kann Stellungnahmen zu Data-Breach-Berichten und insbesondere daraus abzuleitenden Empfehlungen zur Verbesserung von Datenschutz und Informationssicherheit abgeben.

universität innsbruck

Das Datenschutzgremium kann zu Datenschutz- und Informationssicherheitsberichten der Universität Stellungnahmen abgeben, insbesondere zu den darin vorgeschlagenen technischen und organisatorischen Maßnahmen zur laufenden Verbesserung von Datenschutz und Informationssicherheit im Allgemeinen sowie zu spezifischen Datenverarbeitungen oder mit Bezug auf konkrete Datenschutz- und Informationssicherheitszwischenfälle.

b) Protokolleinsicht

Das Datenschutzgremium ist gem. Punkt 11 in die Einsichtnahme in Protokolldaten bei begründetem Missbrauchsverdacht einzubinden.

8. Informations- und Kontrollrechte der Betriebsräte

a) Informationsrechte

Alle Informationen gem § 91 Abs 2 ArbVG werden seitens der Universität Innsbruck an das Datenschutzgremium übermittelt. Informationen, die auf diesem Weg den Betriebsräten zukommen, gelten als Mitteilung iSd § 91 Abs 2 ArbVG.

b) Kontrollrechte

Die Betriebsräte haben das Recht, im Rahmen der ihnen vom Gesetz eingeräumten Befugnisse im Beisein einer qualifizierten Ansprechperson in personenbezogene Datenverarbeitungen Einsicht zu nehmen.

Darüber hinaus veranlasst die/der Datenschutzkoordinator_in mindestens einmal jährlich eine Stichprobenkontrolle der Protokolldaten ausgewählter Datenverarbeitungen. Den Betriebsräten kommt hinsichtlich der Auswahl der Datenverarbeitungen und der Aufbereitung der Protokolldaten ein Vorschlagsrecht zu.

Zudem wird den Betriebsräten das Recht eingeräumt, auf Verlangen einer Mitarbeiterin/eines Mitarbeiters im Einzelfall die Richtigstellung und Löschung personenbezogener Daten zu kontrollieren.

Die Universitätsleitung verpflichtet sich, durch geeignete Maßnahmen die Kontrolle der Einhaltung dieser Rahmenbetriebsvereinbarung durch die Betriebsräte zu ermöglichen.

9. Anleitung, Information und Rechte der Mitarbeiter_innen

Die Universitätsleitung und die Betriebsräte tragen dafür Sorge, das Bewusstsein der Mitarbeiter_innen der Universität hinsichtlich eines sicheren und verantwortungsvollen Umgangs mit elektronischen Medien im Allgemeinen und mit personenbezogenen Daten im Besonderen zu fördern. Dazu erlässt und kommuniziert die Universität Benutzungsrichtlinien zu Datenschutz und Informationssicherheit, deren Inhalt von allen Mitarbeiter_innen als Dienstanweisung zwingend zu beachten ist.

Alle Mitarbeiter_innen sind über ihre Rechte und Pflichten in Bezug auf die Verarbeitung personenbezogener Daten, die dazu abgeschlossenen Betriebsvereinbarungen sowie die ergänzenden Richtlinien zu informieren.

universität innsbruck

Die Informationen müssen sowohl in schriftlicher Form vorliegen als auch im Wege von Schulungen (inkl Online-Schulungen) vermittelt werden, die innerhalb der Arbeitszeit angeboten und besucht werden können.

Die Planung von Schulungen erfolgt im Rahmen eines Datenschutz-Schulungskonzeptes, das eine systematische Information der Mitarbeiter_innen zeitnah zum Arbeitsbeginn an der Universität sicherstellt.

Sind Mitarbeiter_innen über die Zulässigkeit einer Verarbeitung personenbezogener Daten in begründetem Zweifel, ist der Arbeitsauftrag schriftlich zu dokumentieren. Die/der Mitarbeiter_in kann eine Auskunft der Datenschutzkoordinatorin/des Datenschutzkoordinators bzgl der Zulässigkeit einholen. Der/dem Mitarbeiter_in darf hierdurch kein Nachteil entstehen (siehe auch § 6 Abs 4 DSG). Auf Wunsch der Mitarbeiterin/des Mitarbeiters ist der zuständige Betriebsrat über die Anfrage sowie die erteilte Auskunft zu informieren.

10. Umgang mit Protokolldaten

Protokolldaten (Logdaten) betreffend Benutzer_innenaktivitäten dürfen ohne Einwilligung der betroffenen Mitarbeiterin/des betroffenen Mitarbeiters ausschließlich zu folgenden Zwecken aufgezeichnet und ausgewertet werden:

a. Einhaltung der Bestimmungen der EU-DSGVO zu Datenschutz und Informationssicherheit
b. Kontrolle der Zulässigkeit der Datenverarbeitung
c. Überprüfung der Einhaltung von Betriebsvereinbarungen
d. Gewährleistung der Systemfunktionalität und Systemsicherheit
e. Analyse und Korrektur von technischen Fehlern
f. Planung und Optimierung von IT Systemen und IT Services
g. Leistungsverrechnung für den Betrieb der Systeme und Anwendungen.

Im Sinne der Datenminimierung ist sicherzustellen, dass personenbezogene Systemaufzeichnungen zum ehestmöglichen Zeitpunkt pseudonymisiert, anonymisiert bzw. gelöscht werden.

Davon ausgenommen sind die Auswertung und Einsichtnahme bei Vorliegen eines hinreichend begründeten Verdachts der Verletzung gesetzlicher, dienstlicher oder vertraglicher Pflichten und bei Verdacht des Datenmissbrauchs durch eine/n Mitarbeiter_in.

11. Vorgehen bei Verdacht auf Verletzung gesetzlicher, dienstlicher oder vertraglicher Pflichten und Datenmissbrauch

Der Verdacht der Verletzung gesetzlicher, dienstlicher oder vertraglicher Pflichten oder der missbräuchlichen Verwendung von personenbezogenen Daten ist der/dem Datenschutzkoordinator_in zu melden. Sie/er veranlasst bis zur Klärung der Vorgehensweise die Sicherung aller notwendigen Protokolldaten und unterrichtet das zuständige Rektoratsmitglied und die Betriebsräte. Dabei ist strikt die Verhältnismäßigkeit zu wahren und der/dem Mitarbeiter_in vorab Gelegenheit zur Stellungnahme zu geben, wenn dadurch der Prüfzweck nicht vereitelt wird.

universität innsbruck

Das Datenschutzgremium hat auf Antrag eines seiner Mitglieder oder des zuständigen Rektoratsmitglieds über eine Einsichtnahme in die betreffenden Protokolle umgehend zu beraten und eine Empfehlung abzugeben.

Sofern die Kontrolle als rechtlich zulässig und für die Aufklärung des Verdachts als zielführend bewertet wird, können sowohl die/der Verantwortliche gem. Art. 4 Z 7 EU-DSGVO als auch die Betriebsräte einen Kontrolltermin durch die/den Datenschutzkoordinator_in initiieren. Die/der Datenschutzkoordinator_in hat den Termin sowohl mit den Betriebsräten als auch mit dem zuständigen Rektoratsmitglied zu koordinieren, wobei jede Seite das Recht hat, einen oder mehrere Vertreter_innen zur Kontrolle zu entsenden.

Wenn sich der Verdacht auf Regelverstöße oder unberechtigte Verarbeitungsvorgänge durch die Einsichtnahme in die Protokolldaten bestätigt, so sind die vom Verdacht betroffenen Personen unverzüglich zur Stellungnahme aufzufordern. Die Stellungnahmen sind an das zuständige Rektoratsmitglied und die Mitglieder des Datenschutzgremiums weiterzuleiten.

Innsbruck, am 07. Sep. 2020

Für die Universität:

.....

Rektor
Univ.-Prof. i. R. Dr. Dr. h. c. mult. Tilmann Märk

.....

Vizerektorin für Personal
Univ.-Prof. Dipl.-Psych. Dr. Anna Buchheim
Universität Innsbruck
6020 Innsbruck, Innrain 52

Für den Betriebsrat für das wissenschaftliche Personal:

.....

OR Mag. Christoph Bedenbecker (Vorsitzender)

Für den Betriebsrat der allgemeinen Universitätsbediensteten:

.....

ADir. RgR. Erwin Vones (Vorsitzender)

universität innsbruck

ANHANG 1: Information zu IKT-Systemen

Je Informations- und Kommunikationssystem (IKT-System) sind, sofern vorhanden, folgende Informationen zur Verfügung zu stellen:

- Name des IKT-Systems (Datenverarbeitung), Versionsbezeichnung und Anbieter
- Verwendungszweck der Datenverarbeitung
- die jeweiligen Systembeschreibungen / Benutzerhandbücher
- betriebliche verantwortliche Ansprechperson(en)
- Dokumentation aus dem Verarbeitungsverzeichnis nach Art 30 EU-DSGVO inkl. Informationen zu externen Dienstleister_innen und Dienstleistungsverträgen
- Mandant_innen, die personenbezogene Echtdaten verwenden (z.B. Testsystem, Konsolidierungssystem, Produktivsystem)
- eingesetzte Systemteile / Module
- Ort der Datenhaltung/-verwaltung (bei Dienstleister_in, nähere Angaben zur/zum Dienstleister_in)
- betroffene Personengruppe
- Standort und Art der Datenerfassungsgeräte (zB Terminals, Kameras, Automaten, ...)
- die verwendeten Datenarten und Datenkategorien
- ein Verzeichnis personenbezogener Auswertungen mit Beispielen
- Schnittstellen (Import und Export) zu anderen IKT-Systemen
- Zugriffsberechtigungsverzeichnis und mögliche Empfänger_innenkreise
- Löschfristen
- technische und organisatorische Maßnahmen gemäß Art 32 Abs 1 EU-DSGVO
- automatisierte Auswertungen von Inhaltsdaten
- Ergebnisse der allfällig durchgeführten Datenschutz-Folgenabschätzung sowie der Konsultation der Datenschutzbehörde (gem Art 35 f EU-DSGVO)
- Auflistung der allfällig getroffenen Maßnahmen im Zusammenhang mit Datenschutz durch Technik und allfällig eingeführte datenschutzfreundliche Voreinstellungen
- Form und Umfang der Protokollierung