MITTEILUNGSBLATT
DER
Medizinischen Universität Innsbruck

Internet: http://www.i-med.ac.at/mitteilungsblatt/

Studienjahr 2023/2024 | Ausgegeben am 7. Februar 2024 | 25. Stück

Medieninhaberin, Herstellerin, Herausgeberin und Redaktion: Medizinische Universität Innsbruck.
Anschrift, Verlags- und Herstellungsort: Innrain 52, A-6020 Innsbruck.

Medizinische Universität Innsbruck

82. BETRIEBSVEREINBARUNG

gem. §§ 91 Abs. 2, 91 Abs. 2, 96 Abs. 3 und 96a Abs. 1 Z. 1 ArbVG

über die Einführung und Nutzung elektronischer Personalakten

abgeschlossen zwischen der Medizinischen Universität Innsbruck, vertreten durch den Rektor Univ.-Prof. Dr. med. univ. W. Wolfgang Fleischhacker, einerseits und

dem Betriebsrat für das wissenschaftliche Universitätspersonal, vertreten durch seinen Vorsitzenden ao. Univ.-Prof. Dr. med. univ. Martin Tiefenthaler, sowie

dem Betriebsrat für das allgemeine Universitätspersonal, vertreten durch seinen Vorsitzenden Mathias Schaller, andererseits.

Inhaltsverzeichnis

PRÄAMBEL

Die Medizinische Universität Innsbruck strebt eine Digitalisierung und elektronische Aufbewahrung der personenbezogenen Dokumente und Unterlagen ihrer Mitarbeiter*innen an. Der elektronische Personalakt soll die bisher zentral geführten Personalakten in Papierform ablösen.

Für den elektronischen Personalakt wird als Softwarelösung das Dokumenten-Managementsystem DOXIS verwendet und an die Bedürfnisse der Medizinischen Universität Innsbruck angepasst.

Gleichzeitig muss der Schutz der Persönlichkeitsrechte unter Wahrung der Regelungen des Datenschutzes für die Mitarbeiter*innen gewährleistet sein.

I. ALLGEMEINES

1. REGELUNGSGEGENSTAND

Regelungsgegenstand der Betriebsvereinbarung ist die Einführung und Anwendung des elektronischen Personalaktes.

Der Begriff des elektronischen Personalaktes umfasst die Zusammenfassung aller schriftlich festgehaltenen Daten und Vorgänge, die sich mit den Personalien einer bestimmten Arbeitnehmerin oder eines bestimmten Arbeitnehmers und dem Inhalt und der Entwicklung ihres oder seines Arbeitsverhältnisses befassen.

2. GELTUNGSBEREICH

2.1. Persönlicher Geltungsbereich

Diese Betriebsvereinbarung gilt für alle Arbeitnehmer*innen der Medizinischen Universität Innsbruck, die dem Kollektivvertrag für die Arbeitnehmerinnen und Arbeitnehmer der Universitäten unterliegen, und die Vertragsbediensteten der Medizinischen Universität Innsbruck, nicht aber für die Beamtinnen und Beamten, die dem Amt der Medizinischen Universität Innsbruck zur Dienstleistung zugewiesen sind.

2.2. Räumlicher Geltungsbereich

Diese Betriebsvereinbarung gilt für alle Standorte bzw. Arbeitsstätten der Medizinischen Universität Innsbruck; dies auch bezogen auf die digital eingebundenen Arbeitsstätten unter einer gesicherten Datenleitung (z. B. 2-Faktor-Authentifizierung), etwa im Rahmen des „Homeoffice" laut Richtlinie über die Voraussetzungen und Modalitäten für das Arbeiten im Homeoffice und/oder Remote Work für das allgemeine Universitätspersonal.

3. ZIELE UND ZWECKE

Ziel der elektronischen Speicherung von Personaldaten ist die Erweiterung und Verbesserung der vorhandenen IT-Unterstützung für den Personaladministrationsbereich. Eine moderne und flexible Personalverwaltung benötigt einen schnellen, ortsunabhängigen und aktuellen Zugriff auf Daten und Dokumente der Mitarbeiter*innen.

Mit dem elektronischen Personalakt sollen insbesondere folgende Vorteile erreicht werden:

- ein systematisches, einheitliches Ablagesystem
- Unterstützung, Vereinfachung und Professionalisierung der Personalverwaltung
- die Sicherstellung des Zugriffs ausschließlich berechtigter Personen
- Transparenz der Personalaktenführung für die Arbeitnehmer*innen durch eine einheitliche, zentrale Aktenführung

Mit dieser Betriebsvereinbarung soll sichergestellt werden, dass die Mitarbeiter*innen vor missbräuchlicher Verwendung des Systems, insbesondere einer technisch möglichen Überwachung ihrer Leistung und/oder ihres Verhaltens, geschützt werden.

Ziel dieser Betriebsvereinbarung ist es schließlich, die Vorteile des elektronischen Personalaktes unter Berücksichtigung der Datenschutzbestimmungen für die betroffenen Arbeitnehmer*innen zu nutzen.

4. GRUNDSÄTZE DER DATENVERARBEITUNG UND DES DATENSCHUTZES

Jede Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der Mitarbeiter*innen ist erstens nur im Rahmen der Zweckbestimmung des Arbeitsverhältnisses zulässig, wenn sich zweitens die Berechtigung unmittelbar aus gesetzlichen oder aus kollektiv- und arbeitsvertraglichen Bestimmungen ergibt und drittens im hierfür notwendigen Ausmaß.

Die Medizinische Universität Innsbruck stellt bei der Verarbeitung personenbezogener Daten der Mitarbeiter*innen die Einhaltung der Bestimmungen des Datenschutzgesetzes (DSG) und der Datenschutzgrundverordnung (DSGVO) sicher. Insbesondere achtet die Medizinische Universität Innsbruck darauf, personenbezogene Daten gegen Verlust, Zerstörung, Verfälschung, unbeabsichtigte Schädigung und den Zugriff Unbefugter zu sichern.

Es sind insbesondere technische und/oder organisatorische Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind:

- Unbefugten den Zutritt zu IT-Systemen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
- zu verhindern, dass IT-Systeme von Unbefugten genutzt werden können (Zugangskontrolle),
- zu gewährleisten, dass die zur Benutzung eines IT-Systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle / Anlage 2),
- zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft sowie festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob, wann und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- zu gewährleisten, dass personenbezogene Daten gegen Zerstörung, Verlust und Offenlegung gegenüber unbefugten Dritten geschützt sind (Verfügbarkeitskontrolle),

- zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können,
- zu gewährleisten, dass personenbezogenen Daten nur so lange verarbeitet werden, als dies für die Zweckerreichung vorbehaltlich allfälliger öffentlichrechtlicher Aufbewahrungspflichten und zivilrechtlicher Aufbewahrungserfordernisse notwendig ist,
- zu gewährleisten, dass personenbezogene Daten am aktuellen Stand und richtig sind,
- zu gewährleisten, dass personenbezogene Daten langfristig speicherbar und lesbar sind; dies in Verbindung mit Punkt III. Z. 12.

5. RECHTLICHE GRUNDLAGEN

Die Betriebsvereinbarung wird auf Grundlage der gesetzlichen Bestimmungen, insbesondere der §§ 91 Abs. 2, 91 Abs. 2, 96 Abs. 3 und 96a Abs. 1 Z. 1 ArbVG, abgeschlossen. Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten gemäß dieser Betriebsvereinbarung sind insbesondere das Arbeitsverfassungsgesetz (ArbVG), das Datenschutzgesetz (DSG) und die Datenschutz-grundverordnung (DSGVO).

II. TECHNISCHE BESCHREIBUNG

6. SYSTEMBESCHREIBUNG

Als Software für den elektronischen Personalakt kommt das Dokumentenmanagementsystem DOXIS der Firma SER zum Einsatz. Konkret wird die Standardoberfläche des DOXIS Lösungspakets Personalakte verwendet, in der elektronische Personaldokumente pro Mitarbeiter*in systematisch, revisionssicher und datenschutzkonform abgelegt, verwaltet und abgerufen werden können.

Das DOXIS Lösungspaket Personalakte bietet folgende Funktionen:

• Vordefinierte Aktenstruktur, Belegarten und Aufbewahrungsfristen
• Vergabe permanenter oder temporärer Zugriffsrechte auf Personalakten und -dokumente für die Mitarbeiter*innen über Portalrollen
• Vordefinierter Workflow für Antrag auf Akteneinsicht eines Mitarbeiters/einer Mitarbeiterin
• Automatisches Ausführen von Workflows für Personaldokumente
• Verwendung von Dokumentvorlagen
• Automatische Synchronisierung von unbedingt erforderlich Personaldaten aus SAP

Die konkreten Einstellungen des DOXIS Lösungspakets Personalakte an der Medizinischen Universität Innsbruck sind in den folgenden Punkten und in den Anlagen dieser Betriebsvereinbarung detailliert beschrieben:

Anlage 1: Aktenstruktur und Aufbewahrungsdauer elektronischer Personalakt

Anlage 2: Überblick Portalrollen mit Zugriffsberechtigungen

Anlage 3: Schnittstellenverzeichnis: Beschreibung des Datenimports aus SAP HCM in den DOXIS Personalakt

Die Speicherung und Archivierung des elektronischen Personalakts erfolgt am Datenbank-Server der Medizinischen Universität Innsbruck.

7. AKTENSYSTEMATIK

7.1 Aktenstruktur

Die elektronische Speicherung des Personalaktes erfolgt in einer einheitlichen Aktenstruktur. Die Personalakten werden personenbezogen geführt.

Die Personalakte wird gemäß der in Anlage 1 beigefügten Struktur in Register, Unterregister und Dokumenttyp unterteilt. Innerhalb der Dokumenttypen erhalten die Dokumente unterschiedliche, vordefinierte Namen, wodurch eine weitere Unterscheidung der Dokumentarten möglich ist.

7.2 Aktenzugriff

Die elektronischen Personalakten werden von den zuständigen Mitarbeiterinnen und Mitarbeitern der Abteilung Personal (siehe dazu Pkt. 8) geführt. Dies umfasst das Hinzufügen, Verschieben und Löschen von Dokumentverknüpfungen.
Innerhalb eines einzelnen Aktes ist eine Volltextsuche und Attributsuche (nach erfassten Informationen) möglich.

7.3 Aktenerfassung und Aktenablage

Die in Papier geführten Altakten werden durch ein Scanverfahren in den elektronischen Personalakt überführt (Initialscan).

Für den Initialscan werden die Papierakten zunächst von Mitarbeiterinnen und Mitarbeitern der Abteilung Personal technisch vorbereitet.

Der Initialscan erfolgt von einem ISO-zertifizierten Scandienstleister unter Einhaltung der datenschutzrechtlichen Bestimmungen. Die Papierakten werden vom Scanstandort in Österreich wieder an die Medizinische Universität Innsbruck zurücktransportiert und dort nach einer Übergangsphase archiviert.

Für alle Personen mit Dienstverhältnis zur Medizinischen Universität Innsbruck wird ein elektronischer Personalakt angelegt.

Für folgende Mitarbeiter*innen-Gruppen wird kein elektronischer Personalakt angelegt, soweit kein Dienstverhältnis mit der Universität besteht:

- Beamtinnen und Beamte
- Gastprofessorinnen und Gastprofessoren
- Ferialpraktikantinnen und -praktikanten
- Praktikantinnen und Praktikanten
- Personen in Universitätslehrgängen
- Volontariate
- Personen mit Lehrbefugnis ohne Dienstverhältnis
- Personen mit Werkverträgen

Im Tagesgeschäft erfolgt die Ergänzung des elektronischen Personalaktes durch Hochladen von Dokumenten, die bereits digital in der Abteilung Personal einlangen oder von befugten Mitarbeiter*innen der Abteilung Personal eingescannt wurden. Die Dokumente werden damit im

elektronischen Akt abgelegt. Die Originale werden danach fachgerecht vernichtet, sofern die Aufbewahrung rechtlich nicht erforderlich ist. Im Falle, dass die originalen Dokumente aufzubewahren sind, werden diese analog zu den Personalakten der Beamtinnen und Beamten sicher verwahrt.

8. ZUGRIFFSBERECHTIGUNGEN

Die Mitarbeiter*innen der Abteilung Personal haben permanenten Zugriff auf den elektronischen Personalakt. Weiters wird eine Zugriffsmöglichkeit für dasjenige Rektoratsmitglied inklusive der Vertretung für die Dauer dessen Abwesenheit angelegt, das für das Personal zuständig ist.

Darüber hinaus ist die Einrichtung eines temporären Zugriffs für externe Prüfer*innen zur Erfüllung gesetzlicher Vorschriften (z. B. GPLB-Prüfung) vorgesehen.

Die Zugriffsrechte sind je nach Rolle (z. B. HR-Leitung, HR-Administration, externe Prüfer etc.) auf jene Teile des Personalakts beschränkt, die im Rahmen der Aufgabenerfüllung benötigt werden.

Die Struktur der Berechtigungsrollen ist Anlage 2 zu entnehmen.

Nur die Mitarbeiter*innen der Abteilung Personal können Dokumente entgegennehmen, welche in den elektronischen Personalakt gespeichert werden. Sie können die Daten des elektronischen Personalaktes entsprechend ihrer Berechtigungsrolle lesen, bearbeiten und ausdrucken.

Alle Mitarbeiter*innen, die Zugriff auf den elektronischen Personalakt haben, haben sicherzustellen, dass die datenschutzrechtlichen Bestimmungen eingehalten werden. Die in der Personalakte enthaltenen Informationen sind vertraulich zu behandeln.

Alle Berechtigten sind verpflichtet, die Zugriffsrechte nur im Rahmen ihrer konkreten Aufgabenstellung zu nutzen. Zuwiderhandeln kann (arbeits-)rechtliche Folgen nach sich ziehen. Zur Erteilung der Zugriffsrechte ist die Verpflichtungserklärung zur Wahrung des Datengeheimnisses und von Geschäfts- und Betriebsgeheimnissen zu unterzeichnen (siehe Anlage 4).

Berechtigungen, sowie alle Zugriffe (schreibend und lesend) auf den elektronischen Personalakt werden mit Zeitpunkt des Zugriffs protokolliert.

Die Systemadministration hat keinen Zugriff auf Daten außer zur Störungsbehebung bzw. zur Servicierung auf Anfrage der Abteilung Personal.

9. AUSWERTUNGEN

Personenbezogene Auswertungen, insbesondere Verhaltens- oder Leistungskontrollen werden nicht durchgeführt. Die Abfragen des eigenen Personalakts werden nicht ausgewertet.

10. PROTOKOLLIERUNG UND DOKUMENTATION

Alle Berechtigungen sowie Berechtigungsänderungen werden gesondert dokumentiert und laufend aktualisiert.

Darüber hinaus wird jeder Zugriff auf den elektronischen Personalakt protokolliert.

Der Zugriff auf das Zugriffsprotokoll und die Dokumentation über die Berechtigung darf nur bei vermuteter missbräuchlicher Verwendung des Systems von einer Mitarbeiterin oder einem Mitarbeiter der Abteilung Personal gemeinsam mit je einer Vertreterin oder einem Vertreter

desjenigen Betriebsrats, dem die Mitarbeiterin oder der Mitarbeiter zuzuordnen ist, sowie unter Beisein einer Mitarbeiterin oder einem Mitarbeiter der IT-Abteilung und des Fachbereiches Datenschutzes erfolgen und keinesfalls zu routinemäßigen Kontroll- oder Überwachungszwecken.

11. AUFBEWAHRUNGSFRISTEN

Die Speicherdauer des elektronischen Personalaktes wird entsprechend den gesetzlichen, insbesondere den arbeits-, abgaben- und datenschutzrechtlichen Vorgaben auch im Einklang mit kollektivvertraglichen Regelungen und gemäß den Betriebsvereinbarungen sichergestellt (siehe Anlage 1). Die Löschung wird gemäß DSG und DSGVO automatisch bzw. durch die Abteilung Informationstechnologie durchgeführt und systemkonform protokolliert.

III. AUSKUNFTSRECHTE UND WEITERGABE VON PERSONALDATEN

12. EINSICHTNAHME UND AUSKUNFTSRECHT FÜHRUNGSKRÄFTE

Leiter*innen von Organisationseinheiten haben ein Auskunftsrecht zu Inhalten aus dem elektronischen Personalakt jener Mitarbeiter*innen, deren Dienstvorgesetzte*r sie sind, soweit dies für die Erfüllung ihrer Dienstpflichten und/oder den Betrieb erforderlich und zweckmäßig ist. Ein entsprechender Antrag ist zu begründen und der Leitung der Abteilung Personal zur Entscheidung vorzulegen.

13. WEITERGABE AN DRITTE

Eine Weitergabe von Personaldaten aus dem elektronischen Personalakt an Dritte ist nur zur Erfüllung gesetzlicher Vorschriften (z.B. GPLB-Prüfung, Rechnungshof) oder mit vorheriger Zustimmung der Mitarbeiterin oder des Mitarbeiters zulässig.

14. RECHTE DER MITARBEITERINNEN UND MITARBEITER

Jede Mitarbeiterin und jeder Mitarbeiter hat das Recht, mit einem formlosen Ansuchen ohne Angabe von Gründen an die Abteilung Personal Einsicht in ihren oder seinen Personalakt zu nehmen. Zu diesem Zweck wird den Mitarbeiter*innen innerhalb von zwei Wochen für die Dauer von zwei Wochen über einen bereitzustellenden Link eine temporäre Zugriffsmöglichkeit auf den eigenen Personalakt zur Verfügung gestellt. Im Rahmen des temporären Zugriffs haben die Mitarbeiter*innen gleichzeitig auch Einsicht in die Zugriffshistorie bei ihrem Personalakt und den dort gespeicherten Dokumenten als objektbezogener Audittrail. Das Einsichtsrecht steht den Mitarbeiter*innen einmal halbjährlich zu.

Das Auskunftsrecht sowie das Recht auf Richtigstellung gemäß Datenschutzgesetz (DSG) i.V.m. der Datenschutzgrundverordnung (DSGVO) sind zu beachten.

15. RECHTE DES BETRIEBSRATES

Der Betriebsrat hat das Recht, unter Wahrung der Datenschutzbestimmungen sowie der Persönlichkeitsrechte der Mitarbeiter*innen die Einhaltung dieser Betriebsvereinbarung zu

kontrollieren. Zu diesem Zweck wird ihm insbesondere gestattet, Einsicht in das Programm Doxis und die Systemeinstellungen sowie die hinterlegten Berechtigungen zu nehmen.

Auf Wunsch werden dem Betriebsrat die entsprechenden Dokumentationen zur Verfügung gestellt, soweit die Medizinische Universität Innsbruck darauf Zugriff hat. Nötigenfalls sind fachkundige Personen auch von der Firma, von der DOXIS bezogen wird, zur Beantwortung der Fragen des Betriebsrats beizuziehen.

Die Abteilung Personal der Medizinischen Universität Innsbruck wird den Betriebsräten für das wissenschaftliche und allgemeine Universitätspersonal am Ende eines jeden Quartals eine Liste über die Zugriffsberechtigten der Abteilung Personal und deren Berechtigungsrollen schriftlich übermitteln.

Über Änderungen im Rahmen der Systembeschreibung gemäß Punkt II. 6. nach Abschluss dieser Betriebsvereinbarung sind die Betriebsräte für das wissenschaftliche und allgemeine Universitätspersonal umgehend von der Abteilung Personal schriftlich zu informieren. Langt binnen zwei Wochen keine widersprechende schriftliche Stellungnahme in der Abteilung Personal ein, gilt die Änderung als im Rahmen dieser Betriebsvereinbarung angenommen, andernfalls darüber zwischen den Vertragsparteien zu verhandeln und das Ergebnis gefordertenfalls im Mitteilungsblatt der Medizinischen Universität Innsbruck zu veröffentlichen ist.

IV. SCHLUSSBESTIMMUNGEN

16. INKRAFTTRETEN UND GELTUNGSDAUER

Diese Betriebsvereinbarung wird auf unbestimmte Zeit abgeschlossen. Sie kann von jeder der beiden Parteien unter Einhaltung einer Kündigungsfrist von sechs Monaten zum 31. Jänner eines Jahres schriftlich aufgekündigt werden.

Diese Betriebsvereinbarung tritt am Tag nach ihrer Veröffentlichung im Mitteilungsblatt der Medizinischen Universität Innsbruck in Kraft.

17. ANLAGEN

Nachstehende Anlagen bilden einen integrierenden Bestandteil dieser Betriebsvereinbarung:

Anlage 1: Aktenstruktur und Aufbewahrungsdauer elektronischer Personalakt

Anlage 2: Überblick Portalrollen mit Zugriffsberechtigungen

Anlage 3: Schnittstellenverzeichnis: Beschreibung des Datenimports aus SAP HCM in den DOXIS Personalakt

Anlage 4: Verschwiegenheitserklärung

Innsbruck, am 16.01.2024

Für die Medizinische Universität Innsbruck

Univ.-Prof. Dr. W. Wolfgang Fleischhacker eh

Rektor

Für den Betriebsrat für das wissenschaftliche Universitätspersonal

ao. Univ.-Prof. Dr. Martin Tiefenthaler eh
Vorsitzender

Für den Betriebsrat für das allgemeine Universitätspersonal

FOI Mathias Schaller eh
Vorsitzender

Anlage 1: Aktenstruktur und Aufbewahrungsdauer elektronischer Personalakt

Das fristauslösende Ereignis der Aufbewahrungsdauer ist der Austritt des Mitarbeiters/der Mitarbeiterin.

EBENE 1	EBENE 2	Dokumentarten	Aufbewahrung (Jahre)
Persönliche Dokumente	Bewerbungsunterlagen	Bewerbungsunterlagen	7
	Eintrittsunterlagen	Eintrittsunterlagen	7
	Dienstzeugnisse und Ähnliches	Dienstzeugnisse und Ähnliches	7
	Persönliche Dokumente	Persönliche Dokumente	7
	Familie	Familie	7
	Änderung Stammdaten	Änderung Stammdaten	7
	Sonstiges	Sonstiges	7
	Pers. Dokumente Altdaten gesamt	Pers. Dokumente Altdaten gesamt	7
Zeugnisse & Zertifikate	Zeugnisse & Diplome	Zeugnisse & Diplome	7
	Zertifikate & Eintragungen	Zertifikate & Eintragungen	7
	Sonstiges	Sonstiges	7
	Zeugnisse Altdaten gesamt	Zeugnisse Altdaten gesamt	7
Personalaufnahme & -änderung	Besetzungsverfahren	Besetzungsverfahren	7
	Arbeitsplatzbeschreibung	Arbeitsplatzbeschreibung	7
	Vordienstzeiten	Vordienstzeiten	7
	Basisausbildung	Basisausbildung	7
	Dienstzeitregelung	Dienstzeitregelung	7
	Arbeitsvertrag	Arbeitsvertrag	30
	Nebentätigkeit	Nebentätigkeit	7
	Vereinbarungen	Vereinbarungen	7
	Sonstiges	Sonstiges	7
	Pers.aufnahme Altdaten gesamt	Pers.aufnahme Altdaten gesamt	7
Personalentwicklung	Mitarbeitergespräche	Mitarbeitergespräche	7
	Sonstiges	Sonstiges	7
	Pers.entwicklung Altdaten ab 2016	Pers.entwicklung Altdaten ab 2016	7
An-/Abwesenheiten	Krankheit/Unfall/Kur	Krankheit/Unfall/Kur	7
	Pflegefreistellung	Pflegefreistellung	3
	Dienstverhinderungen	Dienstverhinderungen	3
	Dienstreise	Dienstreise	3
	Freistellungen	Freistellungen	3
	Elternschaft	Elternschaft	3
	Sonstige Karenzen	Sonstige Karenzen	3
	Sonstiges	Sonstiges	3
	An-/Abwesenh. Altdaten ab 2016	An-/Abwesenh Altdaten ab 2016	7
Abrechnungsrelevante Daten	Zulagen	Zulagen	7
	Pendlerpauschale	Pendlerpauschale	7
	Jobticket	Jobticket	7
	Freibetragsbescheid	Freibetragsbescheid	7
	Familienbonus	Familienbonus	7
	Kinderzulage	Kinderzulage	7
	Mehrarbeit/Überstunden	Mehrarbeit/Überstunden	7
	Prämien	Prämien	7
	Jubiläumszuwendung	Jubiläumszuwendung	7
	Mitgliedschaften (GÖD)	Mitgliedschaften (GÖD)	7
	Pensionskasse	Pensionskasse	7
	Meldungen BVAEB	Meldungen BVAEB	7
	KV/MSchG 2. Jahr	KV/MSchG 2. Jahr	7
	Geldaushilfe	Geldaushilfe	7
	Sonstiges	Sonstiges	7
	Abrechnung Altdaten gesamt	Abrechnung Altdaten gesamt	7
	Abrechnung Altdaten ab 2016	Abrechnung Altdaten ab 2016	7
Lehre	Externe Lehre	Externe Lehre	3
	Interne Lehre	Interne Lehre	3
	ULG	ULG	3
	Sonstiges	Sonstiges	3
	Lehre Altdaten ab 2016	Lehre Altdaten ab 2016	3
Berechnungen	§ 109 UG	§ 109 UG	7
	Vorrückungsstichtag VBG	Stichtag VBG	7
	Stichtag Jubiläum	Stichtag Jubiläum	7
	Besoldungsreform	Besoldungsreform	7
	Sonstiges	Sonstiges	7
	Berechnungen Altdaten gesamt	Berechnungen Altdaten gesamt	7
Ende Dienstverhältnis	Austrittsschreiben	Austrittsschreiben	7
	Urlaubsersatzleistung	Urlaubsersatzleistung	7
	Dienstzeugnis MUI	Dienstzeugnis MUI	30
	Sonstiges	Sonstiges	7
	Ende DV Altdaten gesamt	Ende DV Altdaten gesamt	7
Internes	Vertrauliches	Vertrauliches	3
	Sensibles	Sensibles	7
	Internes Altdaten gesamt	Internes Altdaten gesamt	7

Anlage 2: Überblick Portalrollen mit Zugriffsberechtigungen

Rolle	Zugriff auf	Zielgruppe
HR-Leitung	alles	Personalleitung + Stellvertreter*in
HR-Personaljuristen	alles	Personaljurist*innen ohne Leitungsfunktion
HR-Sekretariat	Persönliche Dokumente, Zeugnisse & Zertifikate, Personalaufnahme & -änderung, Personalentwicklung, An-/Abwesenheiten	Sekretariat Personalabteilung
HR-Administration	alles außer „Internes"	Personaladministration, Teamleiter*innen
HR-Personalverrechnung	Personalaufnahme & -änderung, An-/Abwesenheiten, Abrechnungsrelevantes, Berechnungen, Ende Dienstverhältnis, Sensibles	Personalverrechnung
HR-Reisekostenabrechnung	Arbeitsplatzbeschreibungen, Arbeitsvertrag, An-/Abwesenheiten	Sachbearbeiter*innen Reisekostenabrechnung
HR-Zeitwirtschaft	Personalaufnahme/-änderung, An-/Abwesenheit, Mehr-/Überstunden, Ende Dienstverhältnis	Sachbearbeiter*innen Zeitwirtschaft
HR-Stellenmanagement	Persönliche Dokumente, Zeugnisse & Zertifikate, Personalaufnahme & -änderung	Bearbeiter*innen Bewerbungs- und Stellenmanagement
HR-Personalentwicklung	Personalentwicklung, Zeugnisse und Zertifikate	Personalentwicklung
PersRektorat/Vizerektorat	alles, nur Leserechte	Rektor*innen/Vizerektor*innen für Personal und ihre Stellvertreter*innen im Falle der Abwesenheit
Jeder	Temporäre Einsicht der MUI-Mitarbeiter*innen in eigenen Personalakt	Mitarbeiter*innen
Management	-	nicht verwendet! Standardrolle des DOXIS-Systems, kann aus technischen Gründen nicht gelöscht werden
Externe Prüfer	nur temporär auf benötigte Dokumente	Rechnungshof, Sozialversicherung

Anlage 3: Schnittstellenverzeichnis: Beschreibung des Datenimports aus SAP HCM in den DOXIS Personalakt

Die Stammdaten der Mitarbeiter*innen werden ausschließlich in SAP HCM als führendem Personalverwaltungssystem angelegt. Da manche Stammdaten für die Verwaltung und Suche der elektronischen Personaldokumente in DOXIS unbedingt erforderlich sind, werden diese über eine Schnittstelle von SAP HCM in das DOXIS Lösungspaket Personalakte übertragen.

Der Export von SAP HCM nach DOXIS findet täglich statt und übermittelt zwischenzeitliche Datenänderungen. Umgekehrt findet kein Datenaustausch vom DOXIS Personalakt nach SAP HCM statt.

Konkret handelt es sich um Stammdaten aus folgenden SAP HCM-Feldgruppen:

Feldgruppe	SAP Infotyp	Beschreibung
Schlüsselwerte	-	Personalnummer
Maßnahmen	0000	Eintrittsdatum, Austrittsdatum, Status Beschäftigung
Organisatorische Zuordnung	0001	Personal-Teilbereich, Mitarbeiterkreis, Mitarbeitergruppe, Kostenstelle, Organisationseinheit
Daten zur Person	0002	Anrede, Nachname, Vorname, Geburtsname, Geburtsdatum, Staatsangehörigkeit
Behinderung	0004	Behindertengruppe
Anschriften	0006	Straße und Hausnummer, Postleitzahl, Ort, Land
Sollarbeitszeit	0007	Wochenstunden
Sozialversicherung A	0044	SV-Nummer
Kommunikation	0105	q-Kennung

Anlage 4: Verschwiegenheitserklärung

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Verpflichtungserklärung
zur Wahrung des Datengeheimnisses
und von Geschäfts- und Betriebsgeheimnissen für Mitarbeiter*innen
der Abteilung Personal

Vorname, Familienname, Titel:

Organisationseinheit: Abteilung Personal

Sehr geehrte Mitarbeiterin!
Sehr geehrter Mitarbeiter!

In Ausübung Ihrer beruflichen Tätigkeit an der Medizinischen Universität Innsbruck erlangen Sie Kenntnisse über personenbezogene Daten sowie über Geschäfts- und Betriebsgeheimnisse. Alle diese Informationen sind absolut vertraulich zu behandeln und unterliegen den einschlägigen rechtlichen Bestimmungen, wie beispielsweise dem österreichischen Datenschutzgesetz (DSG), dem europäischen Datenschutzrecht (EU-DSGVO) sowie dem Wettbewerbsrecht (UWG).

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") beziehen (zB Name, Adresse, Telefonnummer). Besondere Kategorien personenbezogener Daten umfassen alle personenbezogenen Daten natürlicher Personen über kulturelle und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, die Verarbeitung von genetischen Daten, die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, die Verarbeitung von Gesundheitsdaten sowie die Verarbeitung von Daten zum Sexualleben oder der sexuellen Orientierung.

Geschäfts- oder Betriebsgeheimnisse sind Tatsachen und Erkenntnisse kommerzieller oder technischer Art, die bloß einer bestimmten und begrenzten Zahl von Personen bekannt sind, nicht über diesen Kreis hinausdringen sollen und an deren Geheimhaltung ein wirtschaftliches Interesse besteht.

Ihnen sind folgende Punkte bewusst bzw. verpflichten Sie sich zur Einhaltung folgender Punkte:

- Personenbezogene Daten unterliegen einem besonderen Schutz und deren Verarbeitung (Verwendung) ist nur unter besonderen Voraussetzungen zulässig.
- Mit personenbezogenen Daten, die Ihnen auf Grund Ihrer beruflichen Tätigkeit anvertraut oder zugänglich gemacht wurden, ist sorgfältig umzugehen.
- Es ist untersagt, sich unbefugt personenbezogene Daten zu beschaffen oder diese unbefugt zu verarbeiten.
- Es ist untersagt, unbefugten Personen oder unzuständigen Stellen – intern wie extern – personenbezogene Daten zu übermitteln, mitzuteilen, zugänglich zu machen oder Kenntnis davon zu verschaffen.
- Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden.
- Anvertraute Benutzerkennwörter, Passwörter und sonstige Zugangsberechtigungen sind sorgfältig zu verwahren, geheim zu halten und anderen Personen nicht zugänglich zu machen. Benutzerkennwörter, Passwörter und sonstige Zugangsberechtigungen anderer Personen dürfen nicht verwendet werden. Das betrifft insbesondere die Mitarbeiterkennung, die KIS-Zugangsberechtigung und den ELGA-Zugang.
- Datenträger jeglicher Art, auf denen personenbezogene Daten gespeichert sind, sind zu verschlüsseln. Personenbezogene Daten dürfen nicht auf privaten Datenträgern gespeichert werden.
- Es dürfen ohne ausdrückliche Genehmigung keine Bild-, Ton- und Videoaufzeichnungen angefertigt werden.
- Allfällige weiterreichende andere Bestimmungen über die Geheimhaltungspflichten sind ebenfalls zu beachten, sofern sie mit dem europäischen und nationalen Datenschutzrecht nicht im Widerspruch stehen.
- Diese Verpflichtungen bestehen nach Beendigung Ihrer beruflichen Tätigkeit an der Medizinischen Universität Innsbruck fort.
- Verstöße gegen die hier genannten Verpflichtungen haben nicht nur arbeitsrechtliche Folgen (zB Entlassung), sondern ziehen auch (verwaltungs-)strafrechtliche und zivilrechtliche (zB Schadenersatz) Konsequenzen nach sich.

Aktuelle Informationen, Dokumente sowie Kontaktdaten zum Datenschutz an der Medizinischen Universität Innsbruck sind im Intranet unter folgendem Link abrufbar: https://www.i-med.ac.at/datenschutzkoordinator/intranet/unterlagen.html
Hier finden Sie auch die Kontaktdaten des Datenschutzkoordinators der Medizinischen Universität Innsbruck, der Ihnen im Falle von Rückfragen zur Verfügung steht.

Bitte wenden!

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

§ 6 DSG – Datengeheimnis

(1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

Art 32 Abs 4 DSGVO

Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

§ 11 UWG – Verletzung von Geschäfts- oder Betriebsgeheimnissen.
Mißbrauch anvertrauter Vorlagen

(1) Wer als Bediensteter eines Unternehmens Geschäfts- oder Betriebsgeheimnisse, die ihm vermöge des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des Wettbewerbes mitteilt, ist vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen. (BGBl. Nr. 120/1980, Art. I Z 6)

(2) Die gleiche Strafe trifft den, der Geschäfts- oder Betriebsgeheimnisse, deren Kenntnis er durch eine der im Abs. 1 bezeichneten Mitteilungen oder durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbes unbefugt verwertet oder an andere mitteilt.

(3) Die Verfolgung findet nur auf Verlangen des Verletzten statt.

(4) Aufgrund der technischen vollständigen Protokollierung aller Zugriffe auf elektronische Datenablagen und -verarbeitungen und Einsichtnahme sowie die Überlassung der diesbezüglichen Logfiles an die erfassten MitarbeiterInnen ist mit Transparenz über Zugriffe auf personenbezogene Daten zu rechnen und auch mit der leichteren allfälligen Feststellung unberechtigter Zugriffe. Ich nehme mit Unterfertigung diese Situation zur Kenntnis.

Hiermit erkläre ich, dass ich die obige Erklärung samt Verpflichtungen gelesen und verstanden habe, von der Medizinischen Universität Innsbruck über die entsprechenden (datenschutzrechtlichen) Bestimmungen, insbesondere über das Datengeheimnis nach § 6 DSG idgF, über die Sicherheit der Verarbeitung nach Art 32 Abs 4 DSGVO idgF und über die Verschwiegenheitsverpflichtungen nach § 11 UWG idgF belehrt worden bin und verpflichte mich ausdrücklich zur Einhaltung des geltenden Datenschutzrechts, einschließlich entsprechender betrieblicher Anordnungen und zur Wahrung der Geschäfts- und Betriebsgeheimnisse.

Innsbruck, am

_____
Unterschrift der Mitarbeiterin/des Mitarbeiters