Montanuniversität
Leoben

Rahmenbetriebsvereinbarung für die Verarbeitung von personenbezogenen Daten in Informations- und Kommunikationstechnologie-Systemen

Abgeschlossen zwischen dem Rektorat und den Betriebsräten für das wissenschaftliche und das allgemeine Universitätspersonal der Montanuniversität Leoben

Juli 2026

Versetz' Berge

1 Präambel

Diese Rahmenbetriebsvereinbarung regelt die Verarbeitung personenbezogener Daten von Mitarbeiter:innen an der Montanuniversität Leoben, die im Zuge des Einsatzes und Betriebs von Informations- und Kommunikationstechnologie-Systemen (IKT-Systemen) entstehen. Unter IKT-Systemen sind nicht nur interne, sondern insbesondere auch externe, z.B. cloudbasierte Anwendungen, Dienste und Plattformen (Cloud-Services) zu verstehen, unabhängig davon, ob diese durch die Universität selbst oder durch externe Anbieter bereitgestellt und betrieben werden.

Die vorliegende Rahmenbetriebsvereinbarung schützt die Persönlichkeitsrechte aller Angehörigen der Montanuniversität und stellt sicher, dass Daten nur rechtmäßig, transparent und zweckgebunden verarbeitet werden. Ziel ist es, den Anforderungen der Datenschutz-Grundverordnung (DSGVO), des Datenschutzgesetzes (DSG) sowie weiterer anwendbarer gesetzlicher Bestimmungen, Kollektivverträge und universitärer Regelungen gerecht zu werden. Gleichzeitig legt die Vereinbarung klare Grundsätze in der Verarbeitung von personenbezogenen Daten fest. Damit wird ein verbindlicher Rahmen für die datenschutzkonforme Nutzung und den Betrieb von IKT-Systemen an der Montanuniversität geschaffen und Transparenz und Nachvollziehbarkeit für alle Beteiligten gewährleistet. Die vorliegende Betriebsvereinbarung bildet auch einen Rahmen für zukünftig abzuschließende Einzel- Betriebsvereinbarungen, die sachbezogene, detaillierte Regelungen für einzelne konkrete IKT-Anwendungen im Arbeitsprozess betreffen.

Die Montanuniversität Leoben und die Betriebsräte stimmen darin überein, dass IKT-Systeme für die genannten Zwecke erforderlich sind. Einvernehmen besteht darüber, dass diese Systeme aufgrund ihrer hohen Dynamik und Wichtigkeit einer kontinuierlichen Weiterentwicklung und Aktualisierung bedürfen. Die Universität trägt diesem Wandel Rechnung und gewährleistet die notwendige Anpassung der eingesetzten IKT-Systeme.

Im gegenseitigen Vertrauen werden klare betriebliche Regelungen geschaffen, die beiden Seiten dienen und das Verfahren zur Einführung oder Erweiterung von IKT-Systemen verlässlich gestalten. Sie ersetzt nicht in jedem Fall spezifische Vereinbarungen zu einzelnen Systemen, bildet jedoch einen verbindlichen Rahmen.

Diese Vereinbarung wird zwischen der Montanuniversität Leoben und den Betriebsräten des Wissenschaftlichen Universitätspersonals und des Allgemeinen Universitätspersonals abgeschlossen.

2 Rechtliche Grundlagen

Diese Betriebsvereinbarung wird auf Grundlage der gesetzlichen Bestimmungen abgeschlossen, insbesondere unter Bezugnahme auf

1) das Arbeitsverfassungsgesetz (ArbVG),
2) das Arbeitnehmer:innenschutzgesetz (ASchG),
3) der Datenschutz-Grundverordnung (DSGVO),
4) das Datenschutzgesetz (DSG).

3 Geltungsbereich

3.1 Sachlich

Die vorliegende Betriebsvereinbarung regelt die digitalisierte und automatisierte Verarbeitung personenbezogener Daten der Mitarbeiter:innen der Montanuniversität im Zusammenhang mit der Planung, Einführung, Verwendung und Veränderung der bestehenden und zukünftigen IKT-Systeme.

Der Begriff IKT-System umfasst alle Instrumente und Anwendungen, die der elektronischen Kommunikation und der elektronischen Informationsverarbeitung dienen und die den Mitarbeiter:innen vom Arbeitgeber für die Durchführung der universitären Aufgaben als Betriebsmittel zur Verfügung gestellt werden oder die vom Arbeitgeber zur Verarbeitung von Mitarbeiter:innendaten (z.B. SAP) genutzt werden. Beispiele hierfür sind Serversysteme, Arbeitsplatzrechner, Notebooks, interne sowie externe Kommunikationsnetzwerke (Internet, Telefon, Mobiltelefon und sonstige mobile Geräte sowie die darauf befindlichen Applikationen und Daten) und Softwaresysteme.

Die vorliegende Betriebsvereinbarung gilt für alle IKT-Systeme, mit welchen personenbezogene Daten und insbesondere vertrauliche oder sensible personenbezogene Daten der Mitarbeiter:innen im Sinne der DSGVO verarbeitet werden.

3.2 Persönlich und örtlich

Diese Rahmenbetriebsvereinbarung gilt für alle Mitarbeiter:innen der Montanuniversität im Sinne des § 36 ArbVG. Erfasst sind ebenso Bundesbedienstete, die dem Amt der Montanuniversität zugeordnet sind oder Personen, die an der Montanuniversität Nebentätigkeiten ausüben.

Die Betriebsvereinbarung gilt an allen Standorten der Montanuniversität, sowie an sämtlichen auswärtigen Arbeitsstellen. Personenbezogene Daten dieser Personengruppen werden in der Folge als Mitarbeiter:innendaten bezeichnet.

3.3 Zeitlich

Die Betriebsvereinbarung tritt am 15.Juli.2026 in Kraft und ist auf unbestimmte Zeit abgeschlossen.

Jede der Vertragsparteien kann diese Betriebsvereinbarung unter Einhaltung einer Kündigungsfrist von drei Monaten zum Monatsletzten kündigen.

4 Datenkategorisierung

Zur systematischen Erfassung und Verarbeitung personenbezogener Daten von Mitarbeiter:innen werden die folgenden zwei Kategorien entsprechend der DSGVO definiert:

Kategorie A: Allgemeine personenbezogene Mitarbeiter:innendaten

Diese Kategorie umfasst alle regulären personenbezogenen Daten (gem. Art. 6 DSGVO), die zur Begründung, Durchführung und Beendigung des Arbeitsverhältnisses, zur betrieblichen

Kommunikation sowie zur Berechtigungssteuerung in den IT-Systemen erforderlich sind. Ebenso fallen inhaltliche Arbeitsergebnisse darunter. Für diese Daten gilt das Prinzip der Zweckbindung und der minimalen Rechtevergabe („Need-to-Know-Prinzip").

Beispiele: Stammdaten (Name, Adresse, Organisationseinheit), Kontaktdaten (Telefonnummer, E-Mail), organisatorische Daten (Berechtigungsrollen, Arbeitszeit, Urlaub), administrative Daten (Gehaltsdaten, Pfändungen) sowie Inhaltsdaten (Inhalte von E-Mails, Chats oder Dokumenten).

Kategorie B: Besondere Kategorien personenbezogener Daten (Sensible Daten)

Diese Daten unterliegen dem erhöhten Schutzregime des Art. 9 DSGVO. Eine Verarbeitung in IT-Systemen darf nur auf Basis einer ausdrücklichen gesetzlichen Grundlage oder einer expliziten, freiwilligen Einwilligung für eindeutige und berechtigte Zwecke erfolgen. Der Zugriff auf diese Daten ist streng auf den zwingend erforderlichen Personenkreis (z.B. HR-Abteilung, Betriebsärztlicher Dienst) zu beschränken.

Beispiele: Gesundheitsdaten (Krankenstände, ärztliche Atteste), biometrische Daten (z.B. Fingerabdruck für Zutritt), Daten über die Gewerkschaftszugehörigkeit, Religionsbekenntnis oder ethnische Herkunft.

5 Grundsätze der Datenverarbeitung und des Datenschutzes

Zweck dieser Rahmenbetriebsvereinbarung ist es, die rechtskonforme Verarbeitung personenbezogener Daten von Mitarbeiter:innen bei der Nutzung von IKT-Systemen sicherzustellen.

Der Einsatz von IKT-Systemen soll der Universität dabei helfen, ihre gesetzlichen Aufgaben bestmöglich zu erfüllen und organisatorisch leistungsstark sowie wettbewerbsfähig zu bleiben.

Jede Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der Mitarbeiter:innen ist ausschließlich unter folgenden Bedingungen zulässig:

a) im Rahmen der Zweckbestimmung des Arbeitsverhältnisses,
b) wenn sich die Berechtigung unmittelbar aus gesetzlichen oder aus kollektiv- und arbeitsvertraglichen Bestimmungen ergibt und
c) nur im hierfür notwendigen Ausmaß.

Im Einklang mit der DSGVO wird festgelegt, dass personenbezogene Mitarbeiter:innendaten insbesondere nicht für folgende Zwecke herangezogen werden dürfen:

a) für Zwecke der unberechtigten Leistungskontrolle
b) für Zwecke der Verhaltenskontrollen,
c) zur Erstellung von unerlaubten personenbezogenen Profilen der Mitarbeiter:innen (Profiling),
d) zur unberechtigten Speicherung, Auslagerung und Übermittlung von personenbezogenen Daten,
e) zur systematischen Kontrolle, die die Menschenwürde der Mitarbeiter:innen beeinträchtigen könnte.

Unrechtmäßig durchgeführte personenbezogene Leistungs- oder Verhaltenskontrollen durch Auswertungen personenbezogener Daten, die entgegen den Bestimmungen dieser Betriebsvereinbarung, einer Zusatzvereinbarung oder gesetzlichen Vorgaben von der Montanuniversität als Arbeitgeber durchgeführt werden, dürfen nicht als gerichtliche oder außergerichtliche Beweismittel zum Nachteil von Mitarbeiter:innen, die von dieser Betriebsvereinbarung erfasst sind, verwendet werden. Es besteht ein außergerichtliches, gerichtliches und behördliches Beweismittel- und Beweisverwertungsverbot.

5.1 Prinzipien der Verarbeitung personenbezogener Daten

Dezentrale Systeme zur Verarbeitung personenbezogener Daten dürfen nur unter Einbindung des Betriebsrates und im Rahmen der DSGVO eingesetzt werden. Die Systeme müssen mindestens die gleichen Datensicherheits- und Verfügbarkeitsstandards wie zentrale Systeme gewährleisten. Dies gilt für Systeme in akademischen und administrativen Einheiten, bei Universitätsorganen sowie für Systeme, die von Einzelpersonen genutzt werden. Regelungen in dieser Betriebsvereinbarung sind für dezentrale Systeme inklusive externer Systeme (z.B. Cloud Systeme Dritter) jedenfalls einzuhalten.

Die Verarbeitung erfolgt ausschließlich auf den dafür vorgesehenen zentralen oder zulässigen dezentralen Systemen, zweckgebunden, verhältnismäßig und unter Beachtung von Datenschutz, Datensicherheit und Transparenz.

Dezentrale Systeme, externe Dienste oder Kopien personenbezogener Daten dürfen nur unter Einhaltung der DSGVO und dokumentierter Verfahren verwendet werden.

Die Serviceabteilung ICT und Digitalisierung ist nur berechtigt, personenbezogene Daten im Rahmen der technischen Sicherstellung der IKT-Infrastruktur zu verarbeiten, wobei jede Verarbeitung dokumentiert und nicht länger als erforderlich gespeichert wird.

5.2 Fernwartung

Beim Einsatz von Fernwartung (etwa im Rahmen von Wartungsverträgen) ist dafür Sorge zu tragen, dass personenbezogene Daten nicht missbräuchlich verwendet werden. Sollte eine Hilfestellung durch Aufschalten in die aktuelle Arbeitsumgebung (Bildschirmmaske) erfolgen, ist dies nur nach Aufforderung durch die Anwenderinnen und Anwender und deren Zustimmung für jeden einzelnen Fall erlaubt.

Der Einstieg sowie der Ausstieg der Supporttechnikerin bzw. des Supporttechnikers in eine fremde Anwendung sind anzuzeigen und zu protokollieren.

5.3 Dienstleistungen durch Dritte

Die Einsicht in personenbezogene Daten von Mitarbeiter:innen der Montanuniversität durch Dritte ist nur erlaubt für:

a) berechtigte Personen des SAP-Supportteams des Bundesrechenzentrums (BRZ), für die Dauer der Supportleistung,
b) externe Dienstleister, die eine ausreichende Gewähr für die rechtmäßige und sichere Datenverwendung im Sinne der DSGVO bieten, wobei zu prüfen ist, ob eine

Vertraulichkeitsvereinbarung (NDA) erforderlich ist (z.B. bei Zugriff auf personenbezogene oder vertrauliche Geschäftsdaten),

c) Auftragsverarbeiter im Sinne der DSGVO,

d) weitere Personengruppen im Rahmen gesetzlicher Vorgaben (z.B. Behörden, Gerichte etc.).

Alle zum Einsatz kommenden Auftragsverarbeiter müssen eine ausreichende Gewähr für die rechtmäßige und sichere Datenverarbeitung im Sinne des Art 28 Abs 3 DSGVO bieten.

Die Montanuniversität als Arbeitgeber hat dazu mit jedem Auftragsverarbeiter eine Vereinbarung zu treffen und, sofern von diesem personenbezogene Daten verarbeitet werden, auf die Regelungen dieser Betriebsvereinbarung und betreffenden Zusatzvereinbarungen hinzuweisen.

5.4 Protokolldaten

Aufzeichnungen von Benutzeraktivitäten (Protokolle) dürfen nur unter Einhaltung der Bestimmungen des Datenschutzrechts zu folgenden Zwecken personenbezogen ausgewertet werden:

a) Gewährleistung der Sicherheit und Funktion von IT-Systemen,

b) Analyse und Korrektur von technischen Fehlern in den IT-Systemen,

c) Optimierung der IT-Systeme,

d) Leistungsverrechnung der IT-Systeme,

e) Einhaltung von betrieblich getroffenen technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung (Datensicherheit),

f) bei begründetem Verdacht auf regelwidriges Verhalten entsprechend den Bestimmungen in Punkt 6.4,

g) zur Überprüfung der Einhaltung von Betriebsvereinbarungen, insbesondere wenn der Betriebsrat diese Überprüfung fordert.

Unzulässig ist die Verwendung zum Zweck einer Leistungs- und Verhaltenskontrolle sowie zur Erstellung von personenbezogenen Profilen von Mitarbeiter:innen ohne die vorherige Zustimmung des zuständigen Betriebsrats.

Zugriffe durch die ICT-Abteilung sind zu protokollieren, damit tatsächlich durchgeführte Verarbeitungsvorgänge im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.

6 Rechte und Pflichten im Rahmen der Betriebsvereinbarung

6.1 Informationsrechte der Betriebsräte

Die Betriebsräte erhalten den Zugang zu einem Verzeichnis der verwendeten IKT-Systeme, insbesonders mit folgenden Informationen:

a) Systembeschreibungen,

b) Verwendungszwecke,

c) betriebliche(r) Verantwortliche(r) / Ansprechperson(en),

d) Standorte (inklusive dezentraler Systeme),

e) Schnittstellenverzeichnisse (Datenübertragungen zwischen Systemen),

f) beabsichtigte Beiziehung oder vertragliche Verpflichtung von Auftragsverarbeitern.

Fristen für die Löschung von Daten (grundsätzlich nach 30 Tagen) und weitere Informationen zu den IKT-Systemen sind den Betriebsräten zur Verfügung zu stellen.

6.2 Kontrollrechte des Betriebsrats

Dem Betriebsrat ist unter Einhaltung der gesetzlichen Bestimmungen, die mitunter im Einzelfall die Zustimmung der betroffenen Mitarbeiter:innen erfordern, in sämtliche IT-Systemprotokolle und Auswertungen (insbesondere personenbezogene Auswertungen) binnen 3 Werktagen in technisch adäquater Form Einsicht zu geben.

6.3 Rechte und Pflichten der Mitarbeiter:innen

Information über Rechte und Pflichten

Alle Mitarbeiter:innen sind über ihre Rechte und Pflichten in Bezug auf die elektronische Datenverarbeitung und diese Betriebsvereinbarung zu informieren.

Maßnahmen bei Verdacht auf unzulässige Verarbeitung

Sind Mitarbeiter:innen über die Zulässigkeit einer Verarbeitung oder Übermittlung im Zweifel, sind sie angehalten, die oder den Dienstvorgesetzte:n vor Durchführung in Kenntnis zu setzen, den Arbeitsauftrag und ggf. dessen Durchführung schriftlich zu dokumentieren und den/die Datenschutzbeauftragte/n umgehend zu informieren. Der/dem Mitarbeiter:in dürfen hierdurch keine Nachteile entstehen.

Informations-, Auskunfts-, Richtigstellungs- und Löschungsrechte

Die durch das Gesetz den Mitarbeiter:innen eingeräumten Rechte bleiben unberührt. Dies umfasst insbesondere

- das Recht auf Auskunft über die sie betreffenden personenbezogenen Daten (Art. 15 DSGVO),
- das Recht auf Berichtigung unrichtiger Daten (Art. 16 DSGVO),
- das Recht auf Löschung („Recht auf Vergessenwerden“) im Rahmen der gesetzlichen Vorgaben (Art. 17 DSGVO),
- das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie
- das Recht auf Widerspruch gegen eine Verarbeitung im Rahmen von Art. 21 DSGVO.

Qualifizierung

Alle mit und an IKT-Systemen arbeitenden Beschäftigten sind ihrer Aufgabe entsprechend zu schulen. Dafür kann jeweils systembezogen in Zusatzvereinbarungen ein Qualifizierungskonzept definiert werden.

Private Nutzung

Die Mitarbeiter:innen können auf ihren, vom Arbeitgeber zur Verfügung gestellten, Computersystemen einen Ordner „privat" anlegen, dessen Inhalte ohne ausdrückliche Zustimmung der betroffenen Person weder eingesehen noch ausgewertet werden dürfen. Von den Mitarbeiter:innen sind betriebliche Regelungen zur Daten- und Netzwerksicherheit zu beachten.

6.4 Einsichtnahme in Protokolldaten bei begründetem Verdacht auf regelwidriges Verhalten

1) Bei einem konkreten Verdacht auf die Verletzung gesetzlicher, vertraglicher oder dienstlicher Pflichten (z.B. private Telefongespräche ins Ausland) durch eine Mitarbeiterin oder einen Mitarbeiter wird dieser bzw. diesem zunächst Gelegenheit gegeben, sich persönlich zu den Vorwürfen zu äußern. Auf Wunsch der betroffenen Person kann eine Vertrauensperson oder ein Mitglied des Betriebsrats hinzugezogen werden.

2) Lässt sich die Angelegenheit nicht klären, wird mit Zustimmung der betroffenen Mitarbeiterin/des betroffenen Mitarbeiters und unter Hinzuziehung der/des Datenschutzbeauftragten sowie des zuständigen Betriebsrats Einsicht in die entsprechenden Protokoll- bzw. Logdaten genommen.

Die Einsichtnahme beschränkt sich auf den konkreten Verdacht des Missbrauchs. Protokoll- bzw. Logdaten dürfen im erforderlichen Umfang auch über bestehende Löschfristen hinaus gesichert werden. Die/Der Datenschutzbeauftragte und der zuständige Betriebsrat sind in diesem Fall beizuziehen.

7 Schluss- und Übergangsbestimmungen

Sollten einzelne Bestimmungen dieser Betriebsvereinbarung unwirksam sein oder werden, so bleiben die anderen Teile davon unberührt.

Für das Rektorat:

Vizerektor Univ.-Prof. Dipl.-Ing. Dr.techn. Thomas Prohaska

Für den Betriebsrat für das Wissenschaftliche Universitätspersonal:

Dipl.-Ing. Dr. Eva Wegerer, MBA Vorsitzende

Für den Betriebsrat für das Allgemeine Universitätspersonal:

ADir. Jürgen Edlinger Vorsitzender

Leoben, am 15.07.2026