Montanuniversität
Leoben

DATENSCHUTZRICHTLINIE DER MONTANUNIVERSITÄT LEOBEN

Dokumenteninformationen

Versionsnummer:	2.0		
Dokumententitel:	Datenschutzrichtlinie der Montanuniversität Leoben		
Compliance-Bezug:	Gesetzlich: DSGVO, DSG, FOG		
Dokumentenkoordinator:	Dr. Klaus Sapetschnig	**Datenschutzbeauftragter:**	RA Dr. Daniel Stanonik LL.M.
Freigabe:	Rektorat der MUL		
Revisionsintervall:	Jährlich	**Letzte Revision:**	-

Dokumentenverteiler

Verteilerkreis
Veröffentlichung auf der Datenschutzhomepage der MUL und im MBL

Freigabe

Die Richtlinie tritt mit dem Ablauf des Tages ihrer Kundmachung im Mitteilungsblatt der Montanuniveristät Leoben in Kraft.

Leoben, 05.Mai 2026

Univ.-Prof. Dipl.-Ing. Dr.mont. Dr.-Ing. E.h. Dr.h.c. Peter Moser

MONTANUNIVERSITÄT LEOBEN
REKTOR

Versionsverlauf

Datum, Autor	**Version**	**Beschreibung**
2022 10 31	1.0	Initiale Erstellung
2026 05 05	2.0	Überarbeitung

Montanuniversität
Leoben

INHALT

Montanuniversität
Leoben

Montanuniversität
Leoben

1. Einleitung

Die vorliegende Datenschutzrichtlinie bildet die Grundlage für die Einhaltung der gesetzlichen Datenschutzanforderungen sowie den Schutz der verarbeiteten personenbezogenen Daten der Montanuniversität Leoben.

Datenschutz ist für die Montanuniversität Leoben von wesentlicher Bedeutung, um die gesetzlichen Anforderungen im Umgang mit personenbezogenen Daten zu erfüllen. Die vorliegende Datenschutzrichtlinie ist daher allen organisationsinternen Prozessen verbindlich zu Grunde zu legen.

Die Datenschutzrichtlinie regelt den Umgang mit personenbezogenen Daten.
Insbesondere soll sie

- Verantwortlichkeiten, Aufgaben und Pflichten für alle relevanten Datenschutzthemen regeln,
- das Bewusstsein für die Notwendigkeit von strategischen, technischen und organisatorischen Maßnahmen zur Sicherstellung der Datenschutzanforderungen fördern sowie
- die Vorgehensweise im Umgang mit Data-Breach-Vorfällen festlegen.

2. Grundsätze

2.1 Verpflichtung zum Datenschutz

Das Rektorat der Montanuniversität Leoben verabschiedet hiermit die Datenschutzrichtlinie als Bestandteil ihrer langfristigen Entwicklungsstrategie.

Das Rektorat wird die Ziele und Prinzipien der Datenschutzbestimmungen in Einklang mit der Entwicklungsstrategie und den langfristigen Zielen der Universität unterstützen.

2.2 Stellenwert des Datenschutzes

Datenschutzmanagement wird – in Hinblick auf relevante rechtliche, technologische und organisatorische Belange – aktiv vom Rektorat bzw. dem hierzu vom Rektorat beauftragten Datenschutzkoordinator in Zusammenarbeit mit dem externen Datenschutzbeauftragten betrieben.

2.3 Geltungsbereich

Die vorliegende Datenschutzrichtlinie gilt für alle Standorte der Montanuniversität Leoben.

Die Inhalte der Datenschutzrichtlinie bzw. dessen integrierende und ausführende Dokumente sind allen Mitarbeiter*innen im Geltungsbereich zu kommunizieren und zugänglich zu machen. Des Weiteren sind alle Mitarbeiter*innen im Geltungsbereich sowie externe Auftragnehmer zur Einhaltung der in der Datenschutzrichtlinie festgelegten Bestimmungen verpflichtet.

Alle insbesondere für Mitarbeiter*innen relevanten datenschutzrechtlichen Bestimmungen sind in der Benutzerrichtlinie Datenschutz geregelt, die separat veröffentlicht werden wird.

2.4 Datenschutzziele

Übergeordnetes Ziel der Montanuniversität Leoben in Bezug auf Datenschutz ist die Einhaltung der Bestimmungen der EU-Datenschutz-Grundverordnung (EU-DSGVO, kurz DSGVO) bzw. den nationalen Datenschutzvorschriften (DSG) sowie dem Forschungsorganisationsgesetz (FOG). Oberste Priorität hat dabei die Sicherstellung folgender Datenschutzziele / Datenschutzgrundsätze (gemäß Art. 5 DSGVO):

- Sicherstellung der Rechtmäßigkeit der Verarbeitung
- Sicherstellung der Datenverarbeitung nach Treu und Glauben
- Sicherstellung der Transparenz der Datenverarbeitung
- Sicherstellung des Zweckbindungsprinzips
- Sicherstellung der Datenminimierung
- Sicherstellung der Speicherbegrenzung
- Sicherstellung der Richtigkeit, Integrität, Vertraulichkeit und Verfügbarkeit der verarbeiteten Daten
- Sicherstellung der Rechenschaftspflicht

Alle personenbezogenen Daten von natürlichen Personen (z. B. Personaldaten, Studentendaten, Kundendaten usw.) unterliegen der DSGVO bzw. den nationalen Datenschutzvorschriften (DSG) in den jeweils geltenden Fassungen und dürfen nicht unbefugt verarbeitet, genutzt oder weitergegeben werden. Die Bestimmungen der DSGVO sowie die nationalen Datenschutzvorschriften in den geltenden Fassungen sind uneingeschränkt von allen Mitarbeiter*innen, Auftragsverarbeiter*innen und sonstigen externen Auftragnehmer*innen einzuhalten.

Die DSGVO hat besondere Kategorien personenbezogener Daten unter besonderen Schutz gestellt. Art. 9 Abs. 1 DSGVO definiert diese als personenbezogene Daten, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen" sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Weiters unterliegen nach Art. 10 DSGVO auch personenbezogene Daten über strafrechtliche Verurteilungen besonderen Regelungen.

Vorstehende besondere Kategorien personenbezogener Daten dürfen nur unter noch engeren Voraussetzungen verarbeitet werden und unterliegen unter Umständen einer vorherigen Datenschutz-Folgenabschätzung des*der Datenschutzbeauftragten nach Art. 35 Abs. 1, 2, 3 lit. b DSGVO (siehe dazu Punkt 9).

2.5 Konsequenzen bei Verstößen

Verstöße gegen gültige Vorgaben, Vereinbarungen, Normen und Gesetze in Bezug auf Datenschutz durch Mitarbeiter*innen und / oder externe Auftragnehmer*innen können arbeitsrechtliche Sanktionen zur Folge haben bzw. zu straf- oder zivilrechtlichen Konsequenzen führen.

2.6 Gesetzliche Basis

Bezugnehmend auf die Inhalte dieser Richtlinie dienen folgende Gesetze inkl. aller Verordnungen als Basis:

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

Montanuniversität
Leoben

3. Verantwortlichkeiten und Organisation für Datenschutz

Nachfolgend werden die Verantwortlichkeiten für Datenschutz der Montanuniversität Leoben definiert.

3.1 Datenschutzverantwortlicher

Die Montanuniversität Leoben vertreten durch das Rektorat trägt die Gesamtverantwortung in Bezug auf die Einhaltung der gesetzlichen Bestimmungen, der unternehmensinternen Vorgaben und der vorliegenden Datenschutzrichtlinie sowie betreffend der daraus resultierenden Maßnahmensetzung und Kontrolle.
Das Rektorat hat die Herrn RA Dr. Daniel Stanonik LL.M., Porzellangasse 37/13, 1090 Wien zum externen Datenschutzbeauftragten bestellt und nominiert intern Hrn. Dr. Klaus Sapetschnig, Referent des Rektorates, zum internen Datenschutzkoordinator.
Das Rektorat setzt die Datenschutzrichtlinie durch Veröffentlichung auf der DS Homepage der MUL und im Mitteilungsblatt offiziell in Kraft, überwacht die Umsetzung der Bestimmungen der Datenschutzrichtlinie und fördert das Bewusstsein der Mitarbeiter*innen hinsichtlich Datenschutz.

Das Rektorat stellt folgende Maßnahmen sicher:

- Einhaltung der gesetzlichen Bestimmungen der DSGVO sowie nationaler Datenschutzvorschriften
- Ordnungsgemäße und frühzeitige Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen
- Zur Verfügungstellung
    - der erforderlichen Ressourcen
    - des Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie
    - die Erhaltung des notwendigen Fachwissens der Mitarbeiter*innen
- Sicherstellung, dass der Datenschutzbeauftragte und Datenschutzkoordinator bei der Erfüllung seiner Aufgaben keine Anweisungen bzgl. der Ausübung dieser Aufgaben erhält
- Sicherstellung, dass der Datenschutzbeauftragte und der Datenschutzkoordinator wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt wird
- Sicherstellung, dass durch andere durch den Datenschutzbeauftragten und durch den Datenschutzkoordinator wahrgenommene Aufgaben und Pflichten kein Interessenskonflikt herbeigeführt wird
- Sicherstellung, dass die Kontaktdaten des Datenschutzbeauftragten und Datenschutzkoordinators veröffentlicht sind

3.2 Datenschutzbeauftragter

Der Datenschutzbeauftragte wird direkt vom Rektorat bestellt, berichtet auf Anforderung direkt und ist für folgende Aufgaben gemäß Art. 39 DSGVO verantwortlich:

- Unterrichtung und Beratung der Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO sowie den nationalen Datenschutzvorschriften
- Überwachung der Einhaltung gesetzlicher Vorgaben
- Überwachung der Einhaltung der Strategien des Rektorates für den Schutz personenbezogener Daten
- Sensibilisierung und Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeiter*innen

- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung
- Zusammenarbeit mit der Aufsichtsbehörde
- Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen
- Anlaufstelle für Betroffene nach Absprache mit dem Datenschutzkoordinator

Zusätzlich sorgt der Datenschutzbeauftragte für das regelmäßige Update, die Weiterentwicklung und die kontinuierliche Verbesserung der im laufenden Betrieb notwendigen Datenschutzprozesse.
Zudem initiiert der Datenschutzbeauftragte regelmäßige Datenschutz-Termine in Abstimmung mit dem Datenschutzkoordinator.

3.3 Datenschutzkoordinator

Der Datenschutzkoordinator ist primäre Ansprechperson aller Organisationseinheiten der Montanuniversität Leoben zum Thema Datenschutz und koordiniert die Beantwortung dieser Anfragen mit dem Datenschutzbeauftragten.

Die Aufgaben des Datenschutzkoordinators sind:

- Regelmäßige Aktualisierung und kontinuierliche Verbesserung der Datenschutzunterlagen
- Durchführung von regelmäßigen Awareness-Trainings zu Themen des Datenschutzes in Abstimmung mit dem Datenschutzbeauftragten
- Sicherstellung der regelmäßigen Pflege und Aktualisierung des Verarbeitungsverzeichnisses
    - Laufende, strukturierte Erhebung von Datenanwendungen, mit denen personenbezogene Daten verarbeitet werden und Befüllung des Verarbeitungsverzeichnisses
    - Regelmäßige risikotechnische Bewertung der identifizierten Datenanwendungen im Verarbeitungsverzeichnis
    - Durchführung der Datenschutz-Folgenabschätzung
- Regelmäßige Dokumentation der technischen und organisatorischen Maßnahmen (TOMs) und Identifikation von priorisierten Verbesserungsmaßnahmen
- Regelmäßige Aktualisierung, Dokumentation und Verbesserung der Betroffenenrechte
    - Recht auf Auskunft
    - Recht auf Berichtigung
    - Recht auf Löschung / Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Mitteilungspflichten bei Berichtigung, Löschung oder Einschränkung
    - Recht auf Datenübertragbarkeit
    - Recht auf Widerspruch
    - Einwilligung und Informationspflicht
- Regelmäßige Aktualisierung, Dokumentation und Verbesserung des Data-Breach-Prozesses
- Regelmäßige Aktualisierung, Dokumentation und Verbesserung der Datenschutzrichtlinie

3.4 Anwender

Jede*r Mitarbeiter*in ist für die Einhaltung der vorgegebenen Regeln im Umgang mit personenbezogenen Daten, soweit diese ihn betreffen, verantwortlich.

Montanuniversität
Leoben

4. Umgang mit personenbezogenen Daten

4.1 Verarbeitung von Daten

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden. Sie dürfen also nur soweit verarbeitet werden, soweit sie für den Zweck der Datenanwendung wesentlich sind. Die Verarbeitung darf nicht über diesen Zweck hinausgehen. Bei der Verarbeitung von personenbezogenen Daten ist die Einhaltung der Datenschutzgrundsätze (siehe Kapitel 2.4) sicherzustellen.

4.2 Aufbewahrung von anvertrauten Dokumenten

Die Mitarbeiter*innen haben die ihnen anvertrauten Dokumente mit personenbezogenem Inhalt vor dem Zugriff Unbefugter geschützt aufzubewahren.

4.3 Papierkörbe

Papierkörbe zählen zu den unter Datenschutzgesichtspunkten sensiblen Einrichtungen. Die Entsorgung von schutzwürdigen personenbezogenen Informationen darf nicht im Papierkorb erfolgen, sondern ist in dafür gesondert vorgesehenen, verschlossenen Entsorgungsbehältern oder mit einem geeigneten Schredder vorzunehmen.

4.4 Entsorgung elektronischer Datenträger und Daten

Mit personenbezogenen Daten beschriebene elektronische Datenträger (etwa CDs, DVDs, externe Festplatten, Speicherkarten, USB-Sticks, Laptops und PCs) dürfen nicht im Hausmüll entsorgt werden. Vielmehr sind die eben genannten Datenträger und Geräte von fachkundigen Personen bzw. Unternehmen zu vernichten. Informationen erhalten Sie durch den Datenschutzkoordinator.

4.5 Clean Desk

Soweit Mitarbeiter*innen kein eigenes und in ihrer Abwesenheit durchgängig verschlossenes Büro haben, ist darauf zu achten, dass schutzwürdige personenbezogene sowie besondere Kategorien (§ 9 Abs. 1 DSGVO, siehe Kapitel 2.4) personenbezogener Daten angemessen geschützt werden.

4.6 Bildschirme, Drucker und Kopierer

Bildschirme und Drucker sind so aufzustellen, dass ein unberechtigter Einblick und Zugriff Dritter nach Maßgabe des baulich Möglichen ausgeschlossen ist. Hierzu zählt auch eine Sperre des Arbeitsplatzrechners bzw. Notebooks beim Verlassen des Arbeitsplatzes. Ausdrucke mit personenbezogenen Daten dürfen nicht unbeaufsichtigt im Drucker verbleiben, sondern müssen direkt nach dem Ausdruck aus dem Drucker entnommen werden. Gleiches gilt für Kopiergeräte, worin auch keine Fehlkopien oder Originaldokumente mit schutzwürdigen personenbezogenen Daten unbeaufsichtigt verbleiben dürfen.

4.7 Nutzung von Hard- und Software

Mobile Geräte, etwa Notebooks, Smartphones oder Tablets, mit denen personenbezogene Daten verarbeitet werden, sind nach aktuellem Stand der Technik zu verschlüsseln und mit Passwort/PIN für das Login zu versehen. Unterstützung bei der Verschlüsselung leisten die EDV-Beauftragten der jeweiligen Organisationseinheit.

Montanuniversität
Leoben

Bei der Nutzung von mobilen Endgeräten ist sicherzustellen, dass unbefugte Dritte personenbezogene Daten nicht mitlesen oder mithören können.

4.8 Speicherung und Löschung von personenbezogenen Daten

Die Speicherung von personenbezogenen Daten darf nur erfolgen, sofern eine Rechtsgrundlage (etwa gesetzliche Grundlage nach Universitätsgesetz) besteht.

Die Einrichtungen an der Montanuniversität Leoben haben in weiterer Folge Löschkonzepte und Löschroutinen zu erarbeiten. Der Datenschutzbeauftragte steht den Einrichtungen bei der Erarbeitung der Löschkonzepte und Löschroutinen zur Verfügung.

4.9 Nutzung von Cloud-Services und anderen IT-Anwendungen mit Personenbezug

Die Nutzung von Cloud-Services und anderen IT-Anwendungen mit Personenbezug[1] (in der Folge „CloudService") ist an der Montanuniversität Leoben grundsätzlich zulässig. Die Einführung eines neuen, aber auch die Verwendung eines bestehenden Cloud-Services sind jedoch stets abhängig von der geplanten Datenverarbeitung und somit individuell zu überprüfen. So kann ein Cloud-Service für die eine Datenverarbeitung zulässig sein und für eine andere aufgrund der Datensensibilität jedoch nicht. Vor der Verwendung/Einführung eines Cloud-Service zur Verarbeitung personenbezogener Daten muss folgender Prozess eingehalten werden:

Bei Auswahl des Cloud-Service ist mit der Abteilung ICT und Digitalisierung oder dem Datenschutzbeauftragten Kontakt aufzunehmen. Die Abteilung ICT und Digitalisierung und/oder der Datenschutzbeauftragte prüfen in weiterer Folge die Datenschutzkonformität der Datenanwendung und erteilen allfällige Auflagen, um die datenschutzrechtlichen Anforderungen zu erfüllen. Im nächsten Schritt oder parallel dazu wird seitens der Abteilung ICT und Digitalisierung geprüft, ob das Cloud-Service bereits an der Montanuniversität Leoben eingesetzt wird bzw. ob vorhandene Lizenzen bestehen. Sofern Mitarbeiter*innen-Daten betroffen sind, ist auch der Betriebsrat über die geplante Datenverarbeitung und das geplante Cloud-Service in Kenntnis zu setzen. Der eben beschriebene Prozess ist auch dann zu starten, wenn bereits Cloud-Services verwendet werden und noch keine Überprüfung im Sinne des oben Beschriebenen durch die Abteilung ICT und Digitalisierung und/oder den Datenschutzbeauftragten erfolgt ist. Sofern nicht ausschließlich universitätsinterne Services, sondern andere File- oder Cloud-Services verwendet werden, ist darauf zu achten, dass der jeweilige Serviceanbieter die technischen und organisatorischen Maßnahmen gemäß DSGVO einhält. In Zweifelsfragen ist die Abteilung ICT und Digitalisierung oder der Datenschutzbeauftragte zu kontaktieren. Sofern personenbezogene Daten in Länder außerhalb von EU/EWR (das heißt in Drittländer) übertragen werden oder von dort aus in anderer Weise Zugriffsmöglichkeiten bestehen, sind besondere Regeln zu beachten. Im Zweifel ist die Abteilung ICT und Digitalisierung oder der Datenschutzbeauftragte beratend heranzuziehen.

5. Datengeheimnis

Alle Mitarbeiter*innen sind nachweislich zur Wahrung des Datengeheimnisses gemäß § 6 DSG zu verpflichten. Insbesondere sind Mitarbeiter*innen zur Verschwiegenheit über alle Umstände, die ihnen in Ausübung ihrer Tätigkeit oder mit Beziehung auf ihre Tätigkeit bekannt werden, verpflichtet. Das Datengeheimnis gilt auch über das Ende des Dienstverhältnisses hinaus.

[1] Hier sind natürlich KI Anwendungen mitumfasst.

Montanuniversität
Leoben

6. Übertragen von personenbezogenen Daten

Personenbezogene Daten (z. B. in Datenbanken, Backups, Daten von Studierenden, Mitarbeiter*innen, Personal- und Gehaltsdaten, Screenshots mit derartigen Daten usw.) dürfen grundsätzlich nicht extern weitergegeben werden.

Ist eine Übertragung von personenbezogenen Daten zwingend notwendig (z.B. zur Fehleranalyse) UND ist eine Anonymisierung der Daten nicht zweckmäßig bzw. nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, muss VOR der Übermittlung eine schriftliche Genehmigung des Datenschutzkoordinators in Abstimmung mit dem Datenschutzbeauftragten eingeholt werden.

Folgende Datenübertragungen sind genehmigungsfrei und können ohne gesonderte Genehmigung des Datenschutzkoordinators /Datenschutzbeauftragten durchgeführt werden:

- Datenübertragungen aufgrund gesetzlicher Verpflichtungen (z.B. Sozialversicherung, Finanzamt), sofern ein sicherer Übertragungsweg verwendet wird
- Vom Dienstgeber explizit freigegebene Datenübertragungen (z.B. Aufträge, Bestellungen, Rechnungen,)
- Übertragung von anonymisierten[i] oder fiktiven Daten
    - Daten sind anonymisiert, wenn keinerlei Rückschlüsse auf den/die Betroffenen und sonstige beteiligte Personen möglich sind.
- Interne Kommunikation (innerhalb der Infrastruktur der Montanuniversität)

Übertragungen von personenbezogenen Daten müssen in jedem Fall über einen sicheren Übertragungsweg gemäß dem Stand der Technik erfolgen (z.B. als verschlüsseltes ZIP-File, über HTTPS oder VPN).

7. Nutzung von Privaten Endgeräten

Die Verwendung privater Endgeräte für universitäre Zwecke ist im Regelfall zulässig. Auf die Einhaltung datenschutzrechtlicher Vorgaben (insbesondere die Verschlüsselung personenbezogener Daten der Montanuniversität Leoben) ist zu achten. Im Zweifel sollen der Datenschutzkoordinator und/oder der Datenschutzbeauftragte beratend herangezogen werden.

Der*Die Mitarbeiter*in hat die Montanuniversität Leoben (Dienstvorgesetzte und Datenschutzbeauftragter) unverzüglich zu informieren, wenn zu befürchten ist, dass dienstliche personenbezogene Daten unbefugt in die Hände Dritter gelangt sein könnten, beispielsweise weil ein Endgerät gestohlen oder verloren wurde oder in sonstiger Weise abhandengekommen ist.

7.1 USB-Sticks, CDs, DVDs, externe Festplatten, Speicherkarten und andere mobile elektronische Datenträger

Das Speichern von personenbezogenen Daten auch auf privaten USB-Sticks, CDs, DVDs, Speicherkarten, externen Festplatten und anderen mobilen Speichermedien ist nach Maßgabe datenschutzrechtlicher Vorgaben zulässig. Im Zweifel sind der Datenschutzkoordinator und/oder der Datenschutzbeauftragte beratend heranzuziehen. Externe mobile Speichermedien, mit denen personenbezogene Daten verarbeitet werden, sind nach aktuellem Stand der Technik zu verschlüsseln.

Montanuniversität
Leoben

8. Verarbeitungsverzeichnis

Gemäß Art. 30 DSGVO ist der Datenschutzverantwortliche verpflichtet ein Verzeichnis aller Verarbeitungstätigkeiten (Verarbeitungsverzeichnis) zu führen. Die regelmäßige Aktualisierung wird durch den Datenschutzkoordinator in Zusammenarbeit mit den Fachabteilungen und unter Anleitung des Datenschutzbeauftragten sichergestellt. Art. 30 DSGVO definiert, welche Inhalte in das Verzeichnis aufzunehmen sind.

Das Verarbeitungsverzeichnis ist schriftlich zu führen und der Datenschutzbehörde auf Anfrage zur Verfügung zu stellen.

9. Datenschutz-Folgenabschätzung

Werden bei Verarbeitungstätigkeiten neue Technologien verwendet bzw. 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 diesbezügliche Verantwortliche verpflichtet, vorab eine Datenschutz-Folgenabschätzung durchzuführen.

Darüber hinaus werden in Art. 35 DSGVO Fälle gelistet, bei denen eine Datenschutz-Folgenabschätzung zwingend notwendig ist z.B:

- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Zudem hat die Aufsichtsbehörde Listen von Verarbeitungsvorgängen erstellt, für die eine Datenschutz-Folgenabschätzung durchzuführen ist link: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010375 bzw. für die keine Datenschutz-Folgenabschätzung durchzuführen ist link: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010206).

10. Technische und organisatorische Maßnahmen (TOMs)

Der Datenschutzverantwortliche hat geeignete technische und organisatorische Maßnahmen (TOMs) 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.

Ziel ist, ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Hinsichtlich der Definition des Stands der Technik erfolgt die Orientierung an (inter-)nationalen Normen und Best-Practice-Ansätzen.

Gemäß Art. 32 DSGVO schließen die Maßnahmen u. a. Folgendes ein:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten

- Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung
- Sicherstellung, dass die Verfügbarkeit personenbezogener Daten und der Zugang zu diesen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Alle Mitarbeiter*innen werden regelmäßig hinsichtlich der vorgegebenen datenschutzrechtlichen Regelungen im Umgang mit personenbezogenen Daten geschult.

11. Einwilligungsprozess

Die Rechtmäßigkeit der Verarbeitung kann durch eine der folgenden Bedingungen sichergestellt werden (Art. 6 DSGVO):

- Erfüllung eines Vertrags bzw. Durchführung vorvertraglicher Maßnahmen
- Erfüllung einer rechtlichen Verpflichtung
- Schützen von lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person
- Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt
- Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten

Trifft keine der oben genannten Bedingungen zu, kann die Rechtmäßigkeit der Verarbeitung auch durch die Einwilligung einer natürlichen Person zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke sichergestellt werden.

Der Datenschutzverantwortliche muß bei der Einholung der Einwilligung folgende Punkte sicherstellen:

- Das Ersuchen um Einwilligung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen, sodass es von den anderen Sachverhalten klar zu unterscheiden ist.
- Die Einwilligung muss durch eine freiwillige, eindeutige Handhabung erfolgen, mit der bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
- Die Einwilligung der betroffenen Person muss nachgewiesen werden können.
- Die betroffene Person muss vor der Abgabe der Einwilligung informiert werden, dass die Einwilligung jederzeit widerrufen werden kann.
- Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

12. Data Breach

Im Fall einer Verletzung des Schutzes personenbezogener Daten wird durch den Datenschutzbeauftragten in Abstimmung mit dem Datenschutzkoordinator unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde gemeldet (es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt). Erfolgt die Meldung an die zuständige Aufsichtsbehörde nicht binnen 72 Stunden, so wird eine Begründung für die Verzögerung beigefügt.

Der Datenschutzbeauftragte stellt in Abstimmung mit dem Datenschutzkoordinator sicher, dass die Meldung an die Aufsichtsbehörde die gemäß Art. 33 Abs. 3 DSGVO geforderten Informationen enthält. Zudem stellt der Datenschutzkoordinator in Abstimmung mit dem Datenschutzbeauftragten sicher, dass sämtliche Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit in Zusammenhang stehenden Fakten, Auswirkungen sowie ergriffenen Maßnahmen dokumentiert sind.

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Datenschutzkoordinator die Betroffenen unverzüglich über die Verletzung gemäß Art. 34 DSGVO.

Durch Vorgabe definierter Verhaltensweisen sowie durch Schulung und Sensibilisierung der Mitarbeiter*innen wird die angemessene Behandlung von Data-Breach-Vorfällen sichergestellt.

Folgende Punkte sind einzuhalten:

- Jeder Mitarbeiter*in meldet alle (vermeintlichen) Data-Breach-Vorfälle umgehend an den Datenschutzkoordinator. Dieser informiert umgehend den externen Datenschutzbeauftragten.
- Die Einschätzung, ob es sich bei der Meldung um einen Data-Breach-Vorfall handelt, erfolgt durch den externen Datenschutzbeauftragten.
- Die Behandlung von Data-Breach-Vorfällen hat mit **höchster Priorität** vor allen anderen Aktivitäten zu erfolgen.

13. Betroffenenrechte

Der Datenschutzverantwortliche ist dafür zuständig, die Rechte der Betroffenen zu wahren und sicherzustellen, dass diese bei Geltendmachung durch geeignete organisatorische, technische und rechtliche Maßnahmen fristgerecht erfüllt werden.

Da ab dem Zeitpunkt von eingehenden Anfragen Dritter, welche die Betroffenenrechte adressieren, gesetzliche Fristen zu laufen beginnen, sind diese umgehend an den Datenschutzkoordinator/ Datenschutzbeauftragten weiterzuleiten.

Dies betrifft 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)

Montanuniversität
Leoben

Dokumentenverweis:	*siehe diesbezügliche Formulare auf der DS Homepage der MUL*

14. Informationspflichten

Der Datenschutzverantwortliche stellt mittels geeigneter Maßnahmen sicher, den Betroffenen alle Informationen, die sich auf eine Verarbeitung beziehen, zu übermitteln. Dies betrifft vor allem die Übermittlung von Informationen gemäß folgender Artikel:

- 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)
- Art. 15 bis 22 DSGVO (Betroffenenrechte)
- Art. 34 DSGVO (Benachrichtigung bei Data-Breach-Vorfällen)

Die Information über die durchgeführte Verarbeitungstätigkeit erfolgt dabei

- in präziser, transparenter, verständlicher und leicht zugänglicher Form,
- in einer klaren und einfachen Sprache sowie
- schriftlich, mündlich oder in anderer Form (ggfs. elektronisch).

15. Auftragsverarbeitung Rahmenbedingungen

Der Datenschutzverantwortliche stellt sicher, dass bei der Auswahl und Beauftragung eines Auftragsverarbeiters die Rahmenbedingungen gemäß Art. 28 und Art. 29 DSGVO eingehalten und schriftlich vereinbart werden. Dazu ist mit jedem Auftragsverarbeiter (d.h. Dienstleister), der personenbezogene Daten im Auftrag der Montanuniversität Leoben verarbeitet, ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) abzuschließen.

16. Überprüfung und Aufrechterhaltung des Datenschutzprozesses – Integration ins QM System der MUL

Datenschutzmanagement ist ein kontinuierlicher Prozess, der im laufenden Betrieb zu überprüfen, aufrecht zu erhalten und im Bedarfsfall anzupassen oder zu verbessern ist.
Das Rektorat ist für die Bereitstellung entsprechender organisatorischer, technischer und kaufmännischer Rahmenbedingungen verantwortlich.

Dazu sind folgende Maßnahmen vorzusehen:

- Durchführung regelmäßiger interner und externer Audits zur Überprüfung der Vollständigkeit, Korrektheit und Wirksamkeit der umgesetzten Prozesse und implementierten Maßnahmen

- Planung, Koordination und Durchführung von regelmäßigen Schulungen zu Datenschutzthemen
- Anpassung der Datenschutzprozessbeschreibungen aufgrund von Änderungen der Datenschutzanforderungen
- Regelmäßige Berichterstattung über den aktuellen IST-Stand hinsichtlich Datenschutz an das Rektorat

Montanuniversität
Leoben

17. Anhang – Datenschutzziele / Datenschutzgrundsätze

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

*a) auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden ("**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**");*

*b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken ("**Zweckbindung**");*

*c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein ("**Datenminimierung**");*

*d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden ("**Richtigkeit**");*

*e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden ("**Speicherbegrenzung**");*

*f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ("**Integrität und Vertraulichkeit**");*

*(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können ("**Rechenschaftspflicht**");*

Artikel 6

Rechtmäßigkeit der Verarbeitung

*(1) Die Verarbeitung ist nur rechtmäßig, wenn **mindestens eine der nachstehenden Bedingungen** erfüllt ist:*

*a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;*

*b) die Verarbeitung ist **für die Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur **Durchführung vorvertraglicher Maßnahmen** erforderlich, die auf Antrag der betroffenen Person erfolgen;*

*c) die Verarbeitung ist **zur Erfüllung einer rechtlichen Verpflichtung erforderlich**, der der für die Verarbeitung Verantwortliche unterliegt;*

*d) die Verarbeitung ist erforderlich, **um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen**;*

*e) die Verarbeitung ist **für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt** oder **in Ausübung öffentlicher Gewalt** erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;*

*f) die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich**, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.*

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

*(2) Die **Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen**, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine **rechtmäßig und nach Treu und Glauben** erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.*

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch
a) Unionsrecht oder
b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem
a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
c) die Art der personenbezogenen Daten, insbesondere ob besondere kategorienpersonenbezogene Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

[i] Anonymisierte Daten sind Daten, die derart verändert wurden, dass keine Zuordnung mehr zu natürlichen Personen möglich ist (auch nicht technisch). Der Anonymisierungsvorgang erfolgt beispielsweise durch Unkenntlichmachung wie Schwärzung von relevanten Abschnitten eines Screenshots oder Ersetzung von Buchstaben in Adressangaben.