UNIVERSITÄT
SALZBURG

Mitteilungsblatt – Sondernummer der Universität Salzburg

Studienjahr 2026/27
17. November 2026
10. Stück

20. Betriebsvereinbarung über die Einführung und den Einsatz von IT-Systemen zur automationsunterstützten Verarbeitung personenbezogener Daten der Mitarbeiter*innen

BETRIEBSVEREINBARUNG

über

*die Einführung und den Einsatz von IT-Systemen zur automationsunterstützten Verarbeitung personenbezogener Daten der Mitarbeiter*innen*

abgeschlossen zwischen der

Paris Lodron Universität Salzburg

Kapitelgasse 4/6, 5020 Salzburg

(im Folgenden „Universität" genannt)

und

Betriebsrat für das wissenschaftliche Universitätspersonal

und dem

Betriebsrat für das allgemeine Universitätspersonal

(im Folgenden gemeinsam „Betriebsräte" genannt)

A. Zielsetzung und Grundsätze

§ 1 Zielsetzung

Mit dieser Betriebsvereinbarung werden die gesetzlich vorgesehene Kontroll-, Interventions-, Informations- und Mitbestimmungsrechte der Betriebsräte im Zusammenhang mit der Einführung und dem Einsatz von IT-Systemen und der damit verbundenen automationsunterstützten Verarbeitung personenbezogener Daten von Mitarbeiter*innen konkretisiert und geeignete Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten und die Kontrolle am Arbeitsplatz gem. Art 88 Abs 2 DSGVO vereinbart.

§ 2 Grundsätze der Verarbeitung personenbezogener Daten

Mit dieser Betriebsvereinbarung wird sichergestellt, dass

1. die Verarbeitung von Daten der Mitarbeiter*innen rechtmäßig, transparent, zweckgebunden, nachvollziehbar und durch die Betriebsräte überprüfbar ist,
2. die Grundrechte auf Datenschutz und Privatleben, aber auch alle anderen Rechte der Mitarbeiter*innen geschützt werden,
3. die Mitarbeiter*innen insbesondere vor einer technisch möglichen Überwachung ihrer Leistung oder ihres Verhaltens geschützt werden,
4. die Betriebsräte die ihnen gemäß den gesetzlichen Grundlagen zustehenden Rechte und ihre Funktion ordnungsgemäß wahrnehmen können.

B. Geltungsbereich

§ 3 Sachlicher Geltungsbereich

(1) Die Betriebsvereinbarung wird auf der Grundlage der gesetzlichen Bestimmungen, insbesondere im Sinne der §§ 91 Abs. 2, 96 AbS. 1 Z 3, 96a Abs. 1 Z. 1 ArbVG, Art. 88 DSGVO sowie Art. 2 Abs. 11 KI-VO abgeschlossen.

(2) Diese Betriebsvereinbarung regelt die Einführung und den Einsatz von Systemen zur automationsunterstützten Verarbeitung personenbezogener Daten von Mitarbeiter*innen der Universität und gilt für alle Systeme und Anwendungen, die ab dem Inkrafttreten dieser Betriebsvereinbarung in das Systemregister zu dieser Betriebsvereinbarung gemäß § 13 aufzunehmen sind. Aufzunehmen sind jedenfalls Systeme, die mehr als ein Drittel der Belegschaft betreffen.

(3) Systemen zur automationsunterstützten Verarbeitung personenbezogener Daten der Mitarbeiter*innen, die an der Universität Salzburg zum Zeitpunkt des Inkrafttretens dieser Betriebsvereinbarung bereits im Einsatz und im Systemregister eingetragen sind, erteilen die Betriebsräte mit Abschluss dieser Betriebsvereinbarung ihre Zustimmung. Die in dieser Betriebsvereinbarung geregelten Kontroll-, Informations- und Mitwirkungsrechte der Betriebsräte kommen auch auf die bereits im Einsatz befindlichen Systeme uneingeschränkt zur Anwendung.

(4) Die durch diese Betriebsvereinbarung verbrieften Rechte der Betriebsräte beziehen sich auf die vom Geltungsbereich dieser Betriebsvereinbarung umfassten Systeme.

§ 4 Persönlicher Geltungsbereich

(1) Diese Betriebsvereinbarung gilt für das wissenschaftliche und künstlerische sowie das allgemeine Universitätspersonal (§ 94 UG).

(2) Diese Betriebsvereinbarung gilt sinngemäß auch für die an der Universität Salzburg tätigen Beamt*innen und Personen, deren Arbeitsverhältnis gemäß §§ 126 Abs. 1 bis 4 oder 134 UG auf die Universität Salzburg übergeleitet wurde und die nach § 126 Abs. 5 bzw. 7 UG nicht ihren Übertritt in den Kollektivvertrag für die Arbeitnehmer*innen der Universitäten erklärt haben. Dies jedoch mit der Maßgabe, dass auf diese Mitarbeiter*innen (auch) die Bestimmungen des Beamtendienstrechtsgesetzes bzw. Vertragsbedienstetengesetzes anzuwenden sind.

C. Kontrollrechte der Betriebsräte

§ 5 Datenschutz-Folgenabschätzungen

Die Betriebsräte haben das Recht, in die von der Universität durchgeführten Datenschutz-Folgenabschätzungen Einsicht zu nehmen, sofern diese sich auf Verarbeitungsvorgänge von Personaldaten beziehen. Datenschutzfolgenabschätzungen werden von der Universität im Verarbeitungsverzeichnis den jeweils zugehörigen Verarbeitungsvorgängen zugeordnet. Die Mitwirkung der Betriebsräte an der Datenschutz-Folgeabschätzung richtet sich nach § 14.

§ 6 Datenschutz durch Technikgestaltung

Die Betriebsräte haben das Recht, in Bezug auf Personaldaten verarbeitende Systeme und Anwendungen die Einhaltung von Art. 25 DSGVO, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, zu kontrollieren, beispielsweise in Bezug auf die Umsetzung von Rollen- und Löschkonzepten, und entsprechende Vorschläge zu machen. Den Betriebsräten ist zu diesem Zweck auf ihr Verlangen Einsicht in das Systemregister zu geben.

§ 7 Verarbeitungsverträge

Die Betriebsräte haben das Recht, in von der Universität abgeschlossene (Sub-) Auftragsverarbeitungsverträge nach Art. 28 DSGVO bzw. Verträge über die gemeinsame Verantwortlichkeit (Art. 26 DSGVO) Einsicht zu nehmen, sofern diese die Verarbeitung von Personaldaten betreffen.

D. Informationsrechte der Betriebsräte

§ 8 Information über die Implementierung neuer Versionen bestehender IT-Systeme

Im Fall der Implementierung neuer Versionen von im Einsatz befindlicher IT-Systeme, die die Funktionalität und die Verarbeitung von Daten durch diese Systeme wesentlich verändern, sind die Betriebsräte vorab zu informieren. Auf Verlangen ist den Betriebsräten Einsicht in das Systemregister zu geben und mit ihnen darüber zu beraten.

§ 9 Information über Datenschutzverletzungen

Die Betriebsräte werden von der Universität zeitnah über Datenschutzverletzungen, welche die Verarbeitung von Personaldaten betreffen, informiert, sofern ein genereller Personenkreis von der Datenschutzverletzung betroffen ist. Die Betriebsräte werden im Weiteren darüber informiert, ob Meldungen gemäß Art. 34 und 35 DSGVO erfolgen oder nicht.

§ 10 Information über die Datenschutzerklärung

Die Universität hat den Betriebsräten und den Mitarbeiter*innen eine vollständige, aktuelle Datenschutzerklärung zur Verfügung zu stellen, in der über die Verarbeitung von Mitarbeiter*innendaten durch die von der Betriebsvereinbarung erfassten Systeme in einfacher, übersichtlicher und verständlicher Form informiert wird. Jede Änderung der Datenschutzerklärung betreffend die Verarbeitung von Mitarbeiter*innendaten ist den Betriebsräten und Mitarbeiter*innen zur Kenntnis zu bringen.

§ 11 Informationen über Hinweise

Die interne Stelle gemäß § 5 Z 6 Hinweisgeber*innenschutzgesetz (HSchG) informiert die Betriebsräte über Hinweise nach dem HSchG in der jeweils gültigen Fassung, sofern bei einem Hinweis eine Verletzung der DSGVO oder KI-VO behauptet wird und sofern sich die behauptete Verletzung auf die Rechte und Freiheiten von Mitarbeiter*innen auswirken kann. Die Betriebsräte

werden dabei über den Inhalt des Hinweises und den Ausgang des Verfahrens informiert. Eine Information hat zu unterbleiben, sollte durch die Information die Vertraulichkeit der Identität der*des Hinweisgeber*in und Dritter, die in der Meldung erwähnt werden, gemäß § 7 HSchG nicht gewahrt werden können oder sonstige Bestimmungen des HSchG verletzt werden.

E. Mitwirkungsrechte der Betriebsräte

§ 12 Einführung von Systemen zur automationsunterstützten Verarbeitung personenbezogener Daten

(1) Der Einsatz neuer Systeme zur automationsunterstützten Verarbeitung personenbezogener Mitarbeiter*innendaten setzt deren Aufnahme in das Systemregister dieser Betriebsvereinbarung voraus, soweit durch die tatsächliche oder vorgesehene Verwendung der Daten nicht eine sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergebende Verpflichtung erfüllt wird. Die Aufnahme eines neuen Systems in das Systemregister bedarf der Zustimmung der Betriebsräte.

(2) Die Betriebsräte sind von der geplanten Aufnahme eines neuen Systems in das Systemregister dieser Betriebsvereinbarung frühzeitig zu informieren. Die Betriebsräte haben das Recht, binnen zweier Wochen nach erfolgter Informationserteilung Auskünfte über die mit der Systemeinführung verbundenen Verarbeitungsvorgänge zu verlangen, die der Wahrnehmung der den Betriebsräten nach dem Gesetz und dieser Betriebsvereinbarung zustehenden Rechte dienen. Diese Informationen sind auf Verlangen in laienverständlicher Form für die Betriebsräte als auch in fachlich präziser Form zum Zwecke einer professionellen Beratung bereitzustellen.

(3) Nach erfolgter Auskunftserteilung gem. Abs 2 haben die Betriebsräte binnen zweier Wochen das Recht, die Einberufung der Arbeitsgruppe Mitarbeiter*innen-Datenschutz gem. Abschnitt F und deren Befassung mit der geplanten Systemeinführung zu verlangen. Die Arbeitsgruppe Mitarbeiter*innen-Datenschutz hat eine Empfehlung bezüglich des Systemeinsatzes und der Aufnahme in das Systemregister auszusprechen, die den Betriebsräten unverzüglich zur Kenntnis zu bringen ist.

(4) Das Recht zur Einberufung der Arbeitsgruppe kommt auch der Universität zu, sollten die Betriebsräte von ihren Rechten gem. Abs 2 oder Abs 3 keinen Gebrauch machen und der Aufnahme in das Systemregister nicht zustimmen.

(5) Die Informationen über die erfassten Systeme werden den Betriebsräten in einem technischen Systemregister zur Verfügung gestellt. Der Zugang zu diesem Systemregister ist mindestens je zwei Mitgliedern beider Betriebsräte zu erteilen. Welche Betriebsratsmitglieder diese Zugänge erhalten sollen, entscheidet der jeweilige Vorsitz. Das Systemregister muss folgende Anforderungen erfüllen: transparent, revisionssicher, personalisiert. Alle zwei Jahre ist das Systemregister zwischen den Betriebsvereinbarungsparteien auf Richtigkeit und Vollständigkeit zu prüfen.

§ 13 Datenschutz-Folgenabschätzungen

Die Betriebsräte haben das Recht, an der Durchführung von Datenschutz-Folgenabschätzungen mitzuwirken, sofern diese die Verarbeitung von Personaldaten betreffen, und eine Beratung über mögliche Risiken für die Rechte und Freiheiten für die Mitarbeiter*innen zu fordern.

§ 14 Auslesen von Protokolldaten und sonstigen personenbezogenen Daten

(1) Ein Auslesen von Protokolldaten, die Benutzer*innenaktivitäten dokumentieren, ist ohne Zustimmung der betroffenen Mitarbeiter*innen zu folgenden Zwecken zulässig:

Z 1 Umsetzung von Maßnahmen zur Informationssicherheit und Einhaltung der relevanten Sicherheitsrichtlinien;

Z 2 Gewährleistung der Systemfunktionalität und Systemsicherheit;

Z 3 Analyse und Korrektur von technischen Fehlern;

Z 4 Optimierung der Rechner- bzw. Systemleistung;

Z 5 Leistungsverrechnung für den Betrieb der Rechner bzw. der Systeme

Z 6 Überprüfung der Einhaltung von Betriebsvereinbarungen.

(2) Das Auslesen von Protokolldaten unter Herstellung eines direkten Personenbezugs hat in den Fällen des Abs 1 unter Einbindung des Datenschutzbeauftragten zu erfolgen und setzt im Sinne einer stufenweisen Kontrollverdichtung voraus, dass eine rein technische oder organisatorische Lösung ohne direkten Personenbezug nicht möglich ist und eine Aufforderung zur Verhaltensänderung erfolglos geblieben ist. Die Betriebsräte sind diesfalls umgehend zu informieren.

(3) Ein Auslesen ohne stufenweise Kontrollverdichtung ist nur zulässig

Z 1 bei einer nachweislichen konkreten unmittelbaren Gefährdung für die IT-Infrastruktur oder ihre korrekte Funktionsfähigkeit;

Z 2 in Fällen, in denen die unmittelbare Gefahr eines monetären Schadens droht, eine Aufforderung von Ermittlungsbehörden vorliegt oder die unbedingte Notwendigkeit zur sofortigen Abwehr der Folgen eines Data Breach gem. Art. 33 DSGVO gegeben ist;

Z 3 zur unbedingt erforderlichen Aufrechterhaltung der Kernprozesse Lehre und Forschung.

Die Betriebsräte, der Datenschutzbeauftragte und der*die CISO sowie die Betroffenen sind diesfalls umgehend zu informieren.

(4) Über die in Abs 1 genannten Zwecke hinaus ist eine Auswertung von Protokolldaten mit direktem Personenbezug oder sonstiger personenbezogener Daten unter den folgenden Voraussetzungen zulässig, wenn der begründete Verdacht des Missbrauchs von Systemen oder der Verletzung gesetzlicher, vertraglicher oder dienstlicher Pflichten besteht:

Z 1 Der begründete Verdacht ist in einem Protokoll zu dokumentieren und die Betriebsräte sind vor Durchführung der Auswertung zu informieren.

Z 2 Die Auswertung personenbezogener Daten hat unter Beiziehung des zuständigen Betriebsrates nach vorheriger Analyse der Fakten, insbesondere unter Einsichtnahme in das vorab erstellte Protokoll, zu erfolgen. Die Auswertung hat möglichst schonend zu erfolgen und ist auf den konkreten Verdacht des Missbrauchsfalls bzw. der Dienstpflichtverletzung zu beschränken.

Z 3 Die betreffenden Mitarbeiter*innen sind von der Durchführung der Auswertung zu informieren, sofern diese Information nicht die Aufklärung gefährdet. Die betroffenen Mitarbeiter*innen

erhalten die Möglichkeit, sich persönlich zu dem Verdacht zu äußern. Der jeweils zuständige Betriebsrat ist der Aussprache beizuziehen.

Z 4 Nach Bereinigung der Gefährdungslage bzw. Aufklärung des Vorfalles sind die zugrundeliegenden personenbezogenen Daten zu löschen bzw. zu anonymisieren. Ausgenommen davon ist die allfällige Einleitung dienstrechtlicher Maßnahmen.

§ 15 Automatisierte Entscheidungsfindung einschließlich Profiling und Predictive Analytics

Die Bestimmungen des Art. 22 DSGVO kommen mit der Maßgabe zur Anwendung, dass gegenüber Mitarbeiter*innen automatisierte Entscheidungsfindung im Einzelfall einschließlich Profiling und Predictive Analytics, soweit datenschutzrechtlich zulässig, nur mit ausdrücklicher Zustimmung der Betriebsräte erfolgen darf. Die Zustimmung bezieht sich auf den jeweiligen Arbeitsprozess im Gesamten und nicht auf Entscheidungen im Einzelfall.

§ 16 Hochrisiko-KI-Systeme

Die Einführung von Hochrisiko-KI-Systemen gemäß dem III. Kapitel der KI-VO bedarf der Zustimmung der Betriebsräte, sofern dabei personenbezogene Daten der Mitarbeiter*innen verarbeitet werden oder sich das Hochrisiko-KI-System direkt auf die Mitarbeiter*innen auswirkt und das System nicht gemäß Artikel 6 der KI-VO von der Einstufung als Hochrisiko-KI-System ausgenommen ist.

Zu Hochrisiko-KI-Systemen zählen insbesondere:

Z 1 KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um Bewerbungen zu sichten oder zu filtern und Bewerber*innen zu bewerten;

Z 2 KI-Systeme, die bestimmungsgemäß für Entscheidungen, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Beendigung von Arbeitsverhältnissen beeinflussen, für die Zuweisung von Aufgaben aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften oder für die Beobachtung und Bewertung des Verhaltens von Personen verwendet werden sollen.

F. Arbeitsgruppe Mitarbeiter*innen-Datenschutz

§ 17 Aufgaben

Zur Evaluierung der Bestimmungen dieser Betriebsvereinbarung und zur Analyse der organisatorischen und technischen Veränderungen wird eine Arbeitsgruppe Mitarbeiter*innen-Datenschutz gebildet. Die Arbeitsgruppe hat – abgesehen von den Fällen des § 13 – zumindest einmal im Jahr eine Sitzung abzuhalten. Die Arbeitsgruppe unterstützt und berät die Universität in ihrer Rolle als datenschutzrechtliche Verantwortliche, insbesondere hinsichtlich der Ausarbeitung von transparenten Informationen für die von der Datenverarbeitung betroffenen Mitarbeiter*innen und der Aktualisierung des Verarbeitungsverzeichnisses und hat gegebenenfalls Vorschläge an das Rektorat zu richten. Die Entscheidungskompetenzen des Rektorats und der Betriebsräte gemäß ArbVG bleiben durch die Arbeitsgruppe unberührt.

§ 18 Zusammensetzung

Die Arbeitsgruppe besteht aus zwei von der Universität, jeweils einem von BR I und BR II zu nominierenden Mitgliedern, dem*der CISO sowie dem*der Datenschutzbeauftragten. Die Funktionsperiode der Arbeitsgruppe entspricht der des Rektorats. Für die innere Organisation der Arbeitsgruppe gilt die Geschäftsordnung der Schiedskommission in ihrer jeweils gültigen Fassung sinngemäß. Bei Bedarf kann die Arbeitsgruppe Auskunftspersonen sowie externe Fachpersonen auf Kosten der Universität in beratender Funktion ohne Stimmrecht beiziehen.

E. Datenschutzbeauftragte*r

§ 19 Bestellung

Die Universität hat den Betriebsräten gegenüber eine*n Datenschutzbeauftragte*n gemäß den Artikeln 37 bis 39 DSGVO namhaft zu machen. Bei der organisatorischen Eingliederung des*der Datenschutzbeauftragte*n hat die Universität nach Möglichkeit sicherzustellen, dass der oder die Datenschutzbeauftragte bei der Wahrnehmung seiner oder ihrer Aufgaben hinsichtlich anderer ihm oder ihr übertragenen Pflichten in keinen Interessenskonflikt geraten kann und dass diese*r seine oder ihre Aufgaben weisungsfrei wahrnehmen kann.

§ 20 Aufgaben

Der*die Datenschutzbeauftragte hat zusätzlich zu den rechtlichen Aufgaben eines*r Datenschutzbeauftragten die Einhaltung dieser Betriebsvereinbarung in datenschutzrechtlicher Sicht zu überprüfen. Dies dient der zusätzlichen Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen und schränkt die Rechte der Betriebsräte in keiner Weise ein. Diesbezüglich ist der*die Datenschutzbeauftrage den Betriebsräten einmal pro Jahr sowie jederzeit auf Anfrage berichtspflichtig.

Salzburg, am 10.11.2026

Für

die Universität Salzburg

den Betriebsrat

des wissenschaftlichen Universitätspersonals

des allgemeinen Universitätspersonals