MITTEILUNGSBLATT

DER
KARL-FRANZENS-UNIVERSITÄT GRAZ

80. SONDERNUMMER

Studienjahr 2021/22 | Ausgegeben am 06. 07. 2022 | 38.a Stück

Betriebsvereinbarung

über das elektronische Zutrittssystem

abgeschlossen zwischen

der Universität Graz

sowie

dem Betriebsrat für das wissenschaftliche Universitätspersonal

und

dem Betriebsrat für das allgemeine Universitätspersonal

Impressum: Medieninhaberin, Herausgeberin und Herstellerin: Universität Graz, Universitätsplatz 3, 8010 Graz. Verlags- und Herstellungsort: Graz.
Anschrift der Redaktion: Rechts- und Organisationsabteilung, Universitätsplatz 3, 8010 Graz.
E-Mail: mitteilungsblatt@uni-graz.at
Internet: https://mitteilungsblatt.uni-graz.at/

Offenlegung gem. § 25 MedienG
Medieninhaberin: Universität Graz, Universitätsplatz 3, 8010 Graz. Unternehmensgegenstand: Erfüllung der Ziele, leitenden Grundsätze und Aufgaben gem. §§ 1, 2 und 3 des Bundesgesetzes über die Organisation der Universitäten und ihre Studien (Universitätsgesetz 2002 - UG), BGBl. I Nr. 120/2002, in der jeweils geltenden Fassung.
Art und Höhe der Beteiligung: Eigentum 100%.
Grundlegende Richtung: Kundmachung von Informationen gem. § 20 Abs. 6 UG in der jeweils geltenden Fassung.

BETRIEBSVEREINBARUNG
ÜBER DAS ELEKTRONISCHE ZUTRITTSSYSTEM

abgeschlossen zwischen der Universität Graz einerseits

sowie

dem Betriebsrat für das wissenschaftliche Universitätspersonal

und

dem Betriebsrat für das allgemeine Universitätspersonal

andererseits

Inhaltsverzeichnis

I. PRÄAMBEL

§ 1. Zweck des elektronischen Zutrittssystems

(1) Die Universität Graz setzt ein elektronisches Zutrittssystem ein, um das Eigentum der Universität Graz und ihrer MitarbeiterInnen bzw. die Infrastruktur der Universität Graz vor Beschädigung, Einbruch und Diebstahl sowie sonstigem schädigenden Verhalten zu schützen und die Sicherheit für die MitarbeiterInnen und Studierenden der Universität Graz zu gewährleisten. Weiters soll verhindert werden, dass nicht berechtigte Personen Bereiche der Universität Graz, die durch ein derartiges System geschützt sind, betreten.

(2) Die Installierung und der Betrieb des elektronischen Zutrittssystems sollen gewährleisten, dass ständig bzw. zu bestimmten Zeiten nur autorisierte Personen Zugang zu den Räumlichkeiten der Universität Graz haben. Das elektronische Zutrittssystem dient als „Schlüsselersatz“ zum Betreten der Räumlichkeiten der Universität Graz.

(3) Das elektronische Zutrittssystem soll Flexibilität und Sicherheit an den Standorten der Universität Graz bieten. Die Flexibilität des elektronischen Zutrittssystems stellt einerseits den internationalen Standard und die Anforderungen für Objekte in der Größe der Universität Graz dar und gewährleistet andererseits die relativ leicht anpassbare Möglichkeit von Schließkreisen und Schließhierarchien an die (sich ändernden) Anforderungen der Universität Graz.

(4) Die Sicherheit eines elektronischen Zutrittssystems liegt primär in der Möglichkeit Zutrittsmedien jederzeit zu sperren, zeitlich einzugrenzen und daher die Gefahren eines klassischen „Schlüsselverlustes“ abzuwenden.

(5) Das Zutrittssystem darf keinesfalls als Mittel für arbeitsrechtliche Kontrollen, insbesondere Arbeitszeiterfassungen, verwendet werden. Auch die Erstellung von Bewegungsprofilen bzw. eine Verknüpfung mit anderen Systemen zur Erstellung von Bewegungsprofilen, zur Videoüberwachung und ähnlichem ist nicht zulässig. Die gespeicherten Daten gem § 7 Abs 1 und 2 dürfen daher ausschließlich in den in dieser Betriebsvereinbarung taxativ aufgezählten Fällen (§ 8 Abs 3 und § 11) sowie bei unmittelbarer Gefahr für Leib und Leben ausgelesen werden.

(6) Die Universität Graz erklärt, dass sie personenbezogene MitarbeiterInnendaten nur im gesetzlich erlaubten und betrieblich unbedingt notwendigen Ausmaß verarbeitet und an Dritte übermittelt. Den Betriebsräten sind auf Wunsch Kopien der entsprechenden Auftragsverarbeitungsverträge gem Art 28 DSGVO zur Verfügung zu stellen.

§ 2. Verweis auf die RBV IKT 2019

Die vorliegende Betriebsvereinbarung enthält sachbezogene, detaillierte Regelungen für eine konkrete IKT-Anwendung. Die in der Rahmenbetriebsvereinbarung über den Einsatz personenbezogener Informations- und Kommunikationstechnologien (Rahmen-BV IKT 2019), verlautbart im Mitteilungsblatt am 26.06.2019, 36.b Stück, 110. Sondernummer, normierten allgemeinen Grundsätze gelten auch für die vorliegende Betriebsvereinbarung über das elektronische Zutrittssystem.

II. GELTUNGSBEREICH

§ 3. Personeller Geltungsbereich

(1) Diese Betriebsvereinbarung gilt für alle ArbeitnehmerInnen der Universität Graz, die dem Universitäten-KV oder – nach den Übergangsbestimmungen des UG – dem VBG unterliegen, die von der Universität Graz mit einem elektronischen Schlüssel (z.B.: Karte, Smartphone oder äquivalentes Medium) ausgestattet werden, um bestimmte Gebäude und Räume der Universität Graz über ein elektronisches Zutrittssystem betreten zu können.

(2) Die vorliegende Betriebsvereinbarung bildet weiters die Rechtsgrundlage für die Konkretisierung der Rechte und Pflichten der BeamtInnen an der Universität Graz, insbesondere des BDG 1979 und der IKT-Nutzungsverordnung des Bundes, BGBl. II Nr. 281/2009.

(3) Sämtliche in den vorangegangenen Absätzen genannten Personengruppen werden im Folgenden als "MitarbeiterInnen" bezeichnet.

(4) Nicht vom Anwendungsbereich erfasst sind Studierende sowie externe Personen (z.B. WerkvertragsnehmerInnen, Reinigungspersonal, LieferantInnen), die ebenfalls über eine Berechtigung zur Benützung des elektronischen Zutrittssystems an der Universität Graz verfügen.

§ 4. Sachlicher Geltungsbereich

Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten, die bei der Nutzung des elektronischen Zutrittssystems anfallen. Erlaubt ist nur die in der BV ausdrücklich geregelte Verarbeitung personenbezogener Daten. Vom Geltungsbereich dieser Betriebsvereinbarung sind sämtliche Gebäude und Räume der Universität Graz erfasst, das heißt insbesondere MitarbeiterInnenräume, Instituts- und Verwaltungsräumlichkeiten, Bibliotheksräumlichkeiten sowie Hörsäle und Seminarräume, technische Räume, Lagerräume, Systemräume, Archivräume und Druckerräume. Nicht unter den Geltungsbereich der Betriebsvereinbarung fallen Räume, die ausschließlich von Dritten genutzt werden (z.B. Räume des Reinigungspersonals).

§ 5. Örtlicher Geltungsbereich

Die vorliegende Betriebsvereinbarung gilt für sämtliche Standorte/Arbeitsstätten der Universität Graz.

§ 6. Geltungsdauer

Diese Betriebsvereinbarung tritt am 01.07.2022 in Kraft und wird vorerst für ein Jahr, somit bis zum 30.06.2023 abgeschlossen. Die Geltungsdauer der Betriebsvereinbarung verlängert sich jeweils um ein weiteres Jahr, sofern nicht eine Vertragspartei unter Einhaltung einer Frist von spätestens drei Monaten vor Ablauf der Jahresfrist erklärt, diese Betriebsvereinbarung nicht fortsetzen zu wollen.

II. FUNKTIONS- UND SYSTEMBESCHREIBUNG

§ 7. Definitionen

(1) Unter Logfiles (Ereignisprotokolldaten) werden in dieser Betriebsvereinbarung alle gesammelten Meta-Daten zur Protokollierung von Aktionen im System verstanden.
Zutrittslogfiles sind Protokolldaten, die erstellt werden, wenn der Zutritt erfasst wird. Im Rahmen dieser Zutrittslogfiles wird jeweils das Datum, die Uhrzeit, der elektronische Schlüssel und die Operation (das heißt Türöffnung) erfasst. Auswertungslogfiles sind Protokolldaten, die durch spezielle Zugriffe auf die Zutrittslogfiles entstehen. Bei Auswertungslogfiles werden folgende Daten erfasst: Datum und Uhrzeit, elektronischer Schlüssel, Personenname und Meldungstext (Grund der Auswertung).

(2) Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art 4 Z 1 DS-GVO). Unter historischen (personenbezogenen) Daten werden in dieser Betriebsvereinbarung jene Zutritts- oder Raumbuchungsdaten (nicht Zutrittsberechtigungen) verstanden, die einen Bezug zu einer Person herstellen bzw. herstellbar machen, die innerhalb der zulässigen Aufzeichnungs- bzw. Speicherdauer unter bestimmten Bedingungen abrufbar sind bzw. ausgelesen werden können.

(3) Revisionssichere Speicherung nach dem jeweiligen Stand der Technik bedeutet, dass die betreffenden Daten unveränderbar, unüberschreibbar und jederzeit wieder abrufbar gespeichert werden.

(4) SystemadministratorInnen sind Personen, die autorisierte Änderungen in zentralen und dezentralen Systemen vornehmen können, z.B. betreffend Zugang zu Netzwerken, Diensten, Systemen und Datenbeständen im oder in Verbindung mit dem Universitätsnetz. Die Identität dieser Personen und eine zuverlässige Möglichkeit der schnellen Kontaktaufnahme mit ihnen sind jenen Personen bekannt zu machen, die für die Berechtigungsvergaben im System UNIGRAZonline (§ 8 Abs 1) zuständig sind, um im Fall von Störung, Missbrauch oder Angriffes von außen rasche Abhilfe veranlassen zu können.

§ 8. Schlösser, Karten und ihre Funktionen

(1) Bei dem in dieser Betriebsvereinbarung geregelten Zutrittssystem handelt es sich um ein System, welches vom datenführenden System (UNIGRAZonline) befüllt wird. Im Zutrittssystem werden nur die einzelnen Türen, Bereiche und Öffnungszeiten eingerichtet. Die Berechtigungen werden von jenen Personen, die im System UNIGRAZonline die Berechtigung (Rolle) für das Ressourcenmanagement innehaben, im datenführenden System vergeben und in das Schließsystem übertragen. Die eindeutige Verknüpfung der Person vom datenführenden System zum Zutrittssystem erfolgt über die ID (= Kennung) des Mifare (= Transponder)-Chip, den Vor- und Nachnamen sowie die akademische Einheit oder Verwaltungseinheit.

(2) Die SystemadministratorInnen haben im Regelbetrieb keinen Zugriff auf die Logfiles gem § 7 Abs 1. Auf diese Daten des Zutrittssystems darf nur im Rahmen von Ermittlungen aufgrund begründeter Verdachtsfälle auf strafbare Handlungen nach Zustimmung des Betriebsrates zugegriffen werden.

(3) Einmal pro Jahr darf das Wartungsunternehmen zur technischen Überprüfung des Zutrittssystems im Beisein je eines Vertreters/einer Vertreterin der Betriebsräte die Daten des anonymisierten und des führenden Systems zusammenführen. Die dabei entstehenden Daten sind unmittelbar nach der Wartungsarbeit wieder zu löschen.

(4) Das von der Universität Graz eingesetzte elektronische Zutrittssystem setzt ein abgestuftes System mit unterschiedlichen Berechtigungskreisen (Zonenkonzept) um, das mittels eines elektronischen Schlüssels sowohl den Zutritt zum Gebäude selbst als auch den Zutritt zu den Einheiten und den einzelnen Räumen ermöglichen kann. Dieses Zonenkonzept gewährleistet, dass ausschließlich dafür Berechtigte Zugang zum jeweiligen Gebäude, zur jeweiligen Einheit oder zu einzelnen Räumen haben.

(5) Die MitarbeiterInnen erhalten einen elektronischen Schlüssel (z.B. Karte oder äquivalentes Medium), der mit einer Nummer versehen ist. Diese Nummer unterscheidet sich von der Personalnummer. Der elektronische Schlüssel ermöglicht dem/der MitarbeiterIn den Zutritt zu allen Räumen, zu denen ihm/ihr eine Zutrittsberechtigung eingeräumt wurde.

(6) Die maximale Empfindlichkeitsdistanz des elektronischen Schlüssels ist 10 cm.

(7) Bei Änderung des Arbeitsplatzes und/oder der Zuständigkeit eines Mitarbeiters/einer Mitarbeiterin erhält der/die MitarbeiterIn entweder einen neuen elektronischen Schlüssel (gegen Retournierung des alten elektronischen Schlüssels) oder es wird die Codierung seines/ihres elektronischen Schlüssels geändert. Scheidet einE MitarbeiterIn aus dem Anwendungsbereich dieser Betriebsvereinbarung aus, ist der elektronische Schlüssel (Bedienstetenkarte) unverzüglich der Zentralen Registratur und Postadministration zu übergeben und zu deaktivieren. Die Rückgabe des elektronischen Schlüssels ist schriftlich zu dokumentieren.

(8) Ein Verlust des elektronischen Schlüssels ist von dem/der LeiterIn der betroffenen Einheit bei der Zentralen Registratur und Postadministration zu melden. Die Universität Graz hat zu diesem Zweck eine Telefonnummer und eine Mailadresse zur Verfügung zu stellen und im Intranet bekanntzumachen. Die Deaktivierung wird dann automatisch auf das Zutrittssystem übertragen. Ab dem Zeitpunkt der Sperre des elektronischen Schlüssels kann der elektronische Schlüssel nicht mehr benutzt werden. Die Sperrung des elektronischen Schlüssels ist notwendig, um Missbrauch durch Dritte zu verhindern.

(9) Die Neuausstellung des elektronischen Schlüssels bei Verlust oder Beschädigung/Bruch kann über die Visitenkarte im UNIGRAZonline beantragt werden. Die Ausgabe erfolgt durch die Zentrale Registratur und Postadministration.

§ 9. Zutrittsrechte und deren Vergabe

(1) Für die Erteilung von Zutrittsberechtigungen mittels elektronischer Schlüssel für die MitarbeiterInnen der jeweiligen Einheit sind die LeiterInnen der akademischen Einheiten und Verwaltungseinheiten zuständig. Die Rechtevergabe wird im System UNIGRAZonline protokolliert. Die genannten LeiterInnen haben die aktuell für den Zutritt ausgegebenen elektronischen Schlüssel bei jeder Änderung auf einem Ausdruck aus dem System UNIGRAZonline durch Unterschrift zu bestätigen.

(2) Eine Sperre von elektronischen Schlüsseln für alle Standorte der Universität Graz oder für einzelne Standorte/Arbeitsstätten ist durch den/die zuständige/n Dienstvorgesetzte/n nur im Fall von gesetzlichen Ermächtigungen oder Verpflichtungen, aufgrund disziplinarrechtlicher oder begründeter arbeitsrechtlicher Maßnahmen z.B. im Falle von Kündigung oder Entlassung, bzw. bei schwerwiegenden oder wiederholten Verstößen gegen die Hausordnung, verlautbart im Mitteilungsblatt am 23.05.2012, 33.a Stück, 36. Sondernummer in der geltenden Fassung, jeweils unter Hinzuziehung des zuständigen Betriebsrates, sowie weiters in folgenden Fällen zulässig:

a. beim Dienstende von zutrittsberechtigten MitarbeiterInnen,

b. zur Abwehr von Gefahren für Leib und Leben und

c. im Zuge von Sicherheitsmaßnahmen zur Abwehr einer Pandemie.

§ 10. Speicherung und Löschung der generierten Daten

(1) Die Zutritte und Zutrittsversuche zu den Räumlichkeiten und zur Infrastruktur (Serverschränke, Technikräume, etc.) an den Standorten der Universität Graz werden entsprechend der Software in den Logfiles lokal gespeichert.

(2) Alle im Zusammenhang mit dem Zutrittssystem verarbeiteten Daten (Zutrittslogfiles) werden für einen Zeitraum von höchstens 14 Tagen gespeichert. Spätestens mit Ablauf dieser Frist werden die Daten unwiderruflich gelöscht.

(3) Alle durch das Zutrittssystem verarbeiteten Daten werden revisionssicher und nach dem jeweiligen Stand der Technik gespeichert.

§ 11. Einsichtnahme und Auswertung

(1) Einsichtnahmen in die Zutrittslogfiles sowie personenbezogene Auswertungen der Daten aus dem elektronischen Zutrittssystem dürfen nach Zustimmung der Betriebsräte durch das für die IT-Angelegenheiten zuständige Mitglied des Rektorats, den/die LeiterIn der uniIT oder deren StellvertreterInnen im Beisein je eines Vertreters/einer Vertreterin der Betriebsräte, ausschließlich im Rahmen von Ermittlungen aufgrund begründeter Verdachtsfälle auf strafbare Handlungen, vorgenommen werden.

(2) Das für die IT-Angelegenheiten zuständige Mitglied des Rektorats, der/die Leiter/in der uniIT oder deren StellvertreterInnen sind verpflichtet, den Betriebsräten eine beabsichtigte Einsichtnahme in die Protokolle ehestmöglich mitzuteilen und den begründeten Verdacht auf strafbare Handlungen darzulegen. Die Betriebsräte haben einen allfälligen Widerspruch gegen die Einsichtnahme oder gegen die personenbezogene Auswertung der Daten der Universität Graz binnen zweier Arbeitstage schriftlich bzw. per Mail mitzuteilen. Im Fall eines Widerspruchs ist eine Einsichtnahme bzw. Auswertung nicht zulässig. Auf Verlangen der Betriebsräte haben die oben genannten, zuständigen FunktionsträgerInnen mit den Betriebsräten über die beabsichtigte Einsichtnahme oder die personenbezogene Auswertung der Daten zu beraten. Falls im Rahmen der Beratung eine Einsichtnahme bzw. Auswertung beschlossen wird, kann bereits im Rahmen des Beratungstermins ein Termin für die gemeinsame Einsichtnahme bzw. Auswertung vereinbart werden.

(3) Bei Ermittlungen bzw. Verdachtsfällen auf strafbare Handlungen können die Daten (Zutritts- und Auswertungslogfiles) der entsprechenden Türen von der Universität Graz für die Dauer der Ermittlungen bzw. des Verfahrens länger als in den in § 7 Abs 2 genannten Fristen aufbewahrt werden. In diesem Fall wird im Beisein je eines Vertreters/einer Vertreterin der Betriebsräte ein Datenexport vorgenommen. Die Aufbewahrung solcher Zutritts- und Auswertungsdaten bei Ermittlungen bzw. Verdachtsfällen auf strafbare Handlungen ist gesondert zu protokollieren. Bis zu einer allfälligen Einsichtnahme in die Protokolle bzw. Auswertung der Daten werden alle Daten anonymisiert und revisionssicher gespeichert. Nach Einstellung der Ermittlungen bzw. nach Beendigung des Verfahrens wegen strafbarer Handlungen sind die entsprechenden Zutritts- und Auswertungslogfiles unverzüglich zu vernichten.

§ 12. Protokollierung

(1) Jede Einsichtnahme in die Zutrittslogfiles oder Auswertung der Zutritte ist in einem Protokoll unter Angabe der Namen der Einsicht nehmenden Personen, des Datums, der Uhrzeit und des Grundes für die Auswertung festzuhalten und revisionssicher zu speichern. Den Betriebsräten ist jederzeit Einsicht in das Protokoll zu gewähren. Über Protokollierungen werden die Betriebsräte monatsweise informiert.

(2) Näheres zu den Zutritts- und Auswertungslogfiles bzw. den Protokolldaten wird in § 7 (Definitionen) geregelt.

IV. RECHTE UND PFLICHTEN

§ 13. Rechte und Pflichten der Arbeitgeberin

(1) Die Universität Graz hat für die Vertraulichkeit der verarbeiteten personenbezogenen Daten im Sinne der DS-GVO und des DSG zu sorgen. MitarbeiterInnen, die Zugang zu den verarbeiteten Daten haben, sind hinsichtlich ihrer Geheimhaltungspflichten, den damit einhergehenden Rechten und Pflichten und den damit verbundenen Rechtsfolgen bei Verletzungen nachweislich zu belehren bzw. zu schulen; sie haben eine entsprechende Geheimhaltungsverpflichtung zu unterzeichnen.

(2) Die Arbeitgeberin hat das Recht, das in dieser Betriebsvereinbarung geregelte elektronische Zutrittssystem auf dem aktuellen Stand der Technik zu halten, soweit sich aus der vorliegenden Betriebsvereinbarung nichts anderes ergibt. Hierfür ist die Zustimmung der Betriebsräte nicht erforderlich, sofern mit der jeweiligen Maßnahme keine Änderung oder Erweiterung der Funktion des Systems verbunden ist, vgl. § 16 Abs 4.

(3) Darüber hinaus gehende Erweiterungen und Änderungen des elektronischen Zutrittssystems bedürfen vorweg der Zustimmung der Betriebsräte. Eine solche Erweiterung oder Änderung liegt insbesondere vor, wenn

a. zusätzliche personenbezogene Daten erhoben, gespeichert und verarbeitet werden,

b. jede weitere Aktivierung von Funktionsmerkmalen mit denen personenbezogene Daten verarbeitet werden,

c. der Kreis der Zugriffsberechtigten erweitert wird oder

d. neue personenbezogene Auswertungen ermöglicht werden.

(4) Die Verantwortung für die Systempflege, die Datenhaltung und die Datensicherheit liegt grundsätzlich beim Rektorat. Dieses betraut mit den laufenden Aufgaben SystemadministratorInnen, wobei datenführendes System (UNIGRAZonline) und Zutrittskontrollsystem nicht von denselben Personen administriert werden dürfen. Mindestens drei Personen müssen auf den Umgang mit dem elektronischen Zutrittssystem eingeschult sein, um im Krankheits- oder Verhinderungsfall die Wartung und Betreuung vornehmen zu können.

(5) Die Arbeitgeberin hat den MitarbeiterInnen den Inhalt der vorliegenden Betriebsvereinbarung im Intranet der Universität Graz zugänglich zu machen.

(6) Die Arbeitgeberin hat die MitarbeiterInnen, insbesondere auch neu Eintretende, über die Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem elektronischen Zutrittssystem zu informieren.

(7) Die Arbeitgeberin hat für MitarbeiterInnen relevante betriebliche Änderungen und Unterbrechungen des Betriebs des elektronischen Zutrittssystems in einem geeigneten innerbetrieblichen Medium (z.B. Intranet) anzukündigen.

§ 14. Rechte und Pflichten der MitarbeiterInnen

Die ausgehändigten elektronischen Schlüssel dürfen von den MitarbeiterInnen nicht weitergegeben werden. Sonstige Authentisierungs- bzw. Authentifizierungs(hilfs)mittel (APP, Chip) sind geheim zu halten. Auch eine Weitergabe an Vorgesetzte, MitarbeiterInnen, System- und NetzwerkadministratorInnen oder anderes IKT-Personal ist nicht zulässig. Allen MitarbeiterInnen steht das Recht zu, übernommene Ressourcen einzusehen und in Absprache mit der Dienst- und Fachaufsicht abzuändern.

§ 15. Rechte der Betriebsräte

(1) Die Betriebsräte haben das Recht, das elektronischen Zutrittssystem, insbesondere die einzelnen Hard- und Softwarekomponenten, jederzeit daraufhin zu prüfen, ob diese der vorliegenden Betriebsvereinbarung entsprechen.

(2) Zur Klärung (programm)technischer Fragen haben die Betriebsräte das Recht, hausinterne fachkompetente MitarbeiterInnen heranzuziehen. Wenn durch diese interne ExpertInnengruppe keine Klärung erzielt werden kann oder wenn keine geeigneten, unbefangenen hausinternen ExpertInnen vorhanden sind, sind externe ExpertInnen heranzuziehen. Die Kosten hierfür hat die Universität Graz zu tragen, sofern die Grundsätze der Angemessenheit sowie der Verhältnismäßigkeit gewahrt bleiben.

(3) Die Arbeitgeberin hat die Betriebsräte über allgemeine interne Aus-, Fortbildungs- und sonstige Schulungsmaßnahmen betreffend das eingesetzte elektronische Zutrittssystem zu informieren. Je zwei Mitglieder der Betriebsräte sind jeweils berechtigt, an den internen Schulungen kostenlos teilzunehmen.

(4) Für jede Veränderung elektronischen Zutrittssystems, ausgenommen den Austausch defekter Hard- und Software durch funktionsgleiche Komponenten, ist eine Änderung der gegenständlichen Betriebsvereinbarung erforderlich.

V. SCHLUSSBESTIMMUNGEN

§ 16. Publikation

Der Text dieser Betriebsvereinbarung ist im Mitteilungsblatt der Universität Graz zu veröffentlichen.

§ 17. Übergangsbestimmung

(1) Die Rechte der MitarbeiterInnen, die sich aus Gesetz, Verordnung oder einer Norm der kollektiven Rechtsgestaltung ergeben, werden durch die vorliegende Betriebsvereinbarung nicht berührt.

(2) Die Bestimmungen der Betriebsvereinbarung über die Einführung und Verwendung elektronischer Schließsysteme und Zutrittskontrollsysteme, verlautbart im Mitteilungsblatt am 21.7.2010, 39.d Stück, 52. Sondernummer, bleiben solange aufrecht, bis alle Schließsysteme auf das neue System geändert wurden.

Graz, am 30.06.2022

Für die Arbeitgeberin:

Der geschäftsführende Rektor:
Riedler

Für den Betriebsrat für das Wissenschaftliche Universitätspersonal:

Der Vorsitzende des Betriebsrats für das wissenschaftliche Universitätspersonal:
Wohlfahrt

Für den Betriebsrat für das Allgemeine Universitätspersonal:

Der Vorsitzende des Betriebsrats für das allgemeine Universitätspersonal:
i.V. Lindner