MITTEILUNGSBLATT
DER
KARL-FRANZENS-UNIVERSITÄT GRAZ

105. SONDERNUMMER

Studienjahr 2016/17 | Ausgegeben am 28. 06. 2017 | 38.a Stück

Rahmenbetriebsvereinbarung

über den

Einsatz der Informations- und Kommunikationstechnologie im Arbeitsprozess

an der Universität Graz

(RBV IKT)

abgeschlossen zwischen der Universität Graz einerseits
sowie
dem Betriebsrat für das wissenschaftliche Universitätspersonal
und
dem Betriebsrat für das allgemeine Universitätspersonal
andererseits

Impressum: Medieninhaber, Herausgeber und Hersteller: Karl-Franzens-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://online.uni-graz.at/kfu_online/wbMitteilungsblaetter.list?pOrg=1

Offenlegung gem. § 25 MedienG
Medieninhaber: Karl-Franzens-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.

Inhaltsverzeichnis

PRÄAMBEL

(1) Zur Erfüllung der von der Universität Graz nach dem Universitätsgesetz 2002 wahrzunehmenden Aufgaben und zur Erreichung von sonstigen Zielen, die sich durch Gesetz, Verordnung, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben, soll ein sachadäquater Einsatz aller im Arbeitsprozess vorhandenen und künftig einzuführenden IKT-Systeme nach den im Datenschutzgesetz 2000 (DSG 2000) sowie in der vorliegenden Rahmenbetriebsvereinbarung enthaltenen Grundsätzen gewährleistet sein. Die Rahmenbetriebsvereinbarung bezweckt einen Ausgleich der Interessen der Universität – sowohl in Hinblick auf Qualitäts- und Effizienzstandards nach innen als auch in Hinblick auf Leistungs- und Qualitätsnachweise nach außen – mit den Interessen der Mitarbeiter und Mitarbeiterinnen der Universität betreffend ihrer Datenschutzanliegen.

(2) Die vorliegende Betriebsvereinbarung bildet einen Rahmen für zukünftig abzuschließende Einzel-Betriebsvereinbarungen, die sachbezogene, detaillierte Regelungen für einzelne konkrete IKT-Anwendungen im Arbeitsprozess treffen.

I. GELTUNGSBEREICH

§ 1. Personeller Geltungsbereich

(1) Die vorliegende Betriebsvereinbarung gilt gem. § 4 Z. 22 i.V.m. § 63 Abs. 2 Universitäten-KV für alle ArbeitnehmerInnen des wissenschaftlichen und des allgemeinen Universitätspersonals der Universität Graz, die dem Universitäten-KV unterliegen oder die nach den Übergangsbestimmungen des UG dem VBG unterliegen. Die rechtliche Grundlage für die vorliegende Betriebsvereinbarung bildet § 96a Arbeitsverfassungsgesetz (ArbVG).

(2) Die vorliegende Betriebsvereinbarung bildet weiters die Rechtsgrundlage für die Konkretisierung der Rechte und Pflichten der BeamtInnen an der Universität Graz. Für diese MitarbeiterInnen gelten jedenfalls die Bestimmungen des BDG 1979 sowie die Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bedienstete des Bundes (IKT-Nutzungsverordnung - IKT-NV), BGBl. II Nr. 281/2009.

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

§ 2. Sachlicher Geltungsbereich

(1) Die vorliegende Betriebsvereinbarung regelt einen Rahmen für die Planung, Einführung, Verwendung und Veränderung der bestehenden und zukünftigen IKT-Infrastruktur, die personenbezogene Daten der MitarbeiterInnen verwendet, im Arbeitsprozess der Universität Graz. Sie gilt für alle Anwendungen und IKT-Systeme mit personenbezogenen und vertraulichen Daten und für alle Systeme, auf denen BenutzerInnendaten (insbesondere BenutzerInnenkennung und Passwort) verwendet werden, mit denen auf solche Daten zugegriffen werden kann.

(2) Die Grundsätze der vorliegenden Betriebsvereinbarung gelten für alle (auch zukünftige) Einzel-Betriebsvereinbarungen über den konkreten Einsatz von IKT-Infrastruktur im Arbeitsprozess.

§ 3. Örtlicher Geltungsbereich

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

§ 4. Zeitlicher Geltungsbereich

Diese Betriebsvereinbarung tritt am 21.06.2017 in Kraft und wird vorerst für ein Jahr, somit bis zum 20.06.2018 abgeschlossen. Die Geltungsdauer der Betriebsvereinbarung verlängert sich jeweils um ein weiteres Jahr, sofern nicht eine Vertragspartei unter Einhaltung einer Frist von drei Monaten vor Ablauf der Jahresfrist erklärt, diese Betriebsvereinbarung nicht fortsetzen zu wollen.

II. BEGRIFFSDEFINITIONEN

§ 5. Begriffsdefinitionen

Es gelten die Definitionen aus dem Datenschutzgesetz (§ 4 DSG 2000) sowie folgende weitere Definitionen bzw. Abkürzungen:

a) "IKT" (Informations- und Kommunikationstechnologie): alle Instrumente und Anwendungen für die elektronische Kommunikation und die elektronische Informationsverarbeitung, die von der Arbeitgeberin für die Durchführung der universitären Aufgaben als Betriebsmittel zur Verfügung gestellt werden.

b) "IKT-Infrastruktur": alle Geräte und Systeme, die von der Arbeitgeberin als Betriebsmittel zur Verfügung gestellt werden oder im Einvernehmen mit der Arbeitgeberin für universitäre Zwecke benutzt werden und der Informationsverarbeitung für Zwecke der Arbeitgeberin dienen, beispielsweise Serversysteme, Arbeitsplatzrechner, Notebooks, interne Kommunikationsnetzwerke wie zum Beispiel das Intranet sowie externe Kommunikationsnetzwerke wie zum Beispiel das Internet, Telefon, Mobiltelefon und sonstige mobile Geräte, sowie die darauf befindlichen Applikationen und Daten;

c) "UNI-IT": Verwaltungseinheit Informationsmanagement, die in der Rolle eines internen Dienstleisters die IKT-Agenden im Auftrag der Universität Graz ausführt.

d) PDV-System: Personendaten verarbeitendes System.

III. GRUNDSÄTZE DER DATENERMITTLUNG- UND VERWENDUNG

§ 6. Allgemeine Grundsätze

(1) Jegliche Ermittlung, Verarbeitung und Übermittlung personenbezogener Daten der MitarbeiterInnen ist nur zulässig, sofern

a) sich die Berechtigung unmittelbar aus Gesetz, Verordnung oder Norm der kollektiven Rechtsgestaltung ergibt

oder

b) die verwendete IKT-Infrastruktur, die Verwendungszwecke, der betroffene Personenkreis, die Zugriffsberechtigten, die DatenadressatInnen und die Speicherdauer in einer Betriebsvereinbarung bestimmt bzw. enthalten sind.

(2) Abs. 1 gilt sinngemäß auch für die Einsichtnahme in Personendaten der Universität Graz durch Dritte. Für Entwicklungs- und Wartungsarbeiten sind hiervon ausgenommen:

a) berechtigte Personen des SAP-Supportteams des Bundesrechenzentrums (BRZ),

b) berechtigte Personen des Entwicklungsteams von CAMPUSonline,

c) externe DienstleisterInnen, die eine ausreichende Gewähr für die rechtmäßige und sichere Datenverwendung im Sinne des § 11 DSG 2000 bieten. Die Arbeitgeberin hat die Betriebsräte vor Beginn der Arbeiten davon zu informieren, welche externen DienstleisterInnen welche Aufträge für Entwicklungs- und Wartungsarbeiten erhalten. Die Arbeitgeberin als Auftraggeberin hat dazu mit derartigen externen DienstleisterInnen eine Geheimhaltungserklärung ("NDA" = non-disclosure agreement) zu treffen und sie nachweislich auf die Regelungen der vorliegenden Betriebsvereinbarung und der betreffenden einzelnen Betriebsvereinbarungen im Zusammenhang mit personenbezogenen Daten hinzuweisen. Dem Betriebsrat ist auf Wunsch eine Kopie derartiger Geheimhaltungserklärungen zur Verfügung zu stellen.

(3) In allen Fällen sind hierbei folgende Grundsätze, die für die gesamte vorliegende Betriebsvereinbarung als Interpretationsmaximen gelten, zu beachten:

a) Die Ermittlung und Verwendung von Daten soll vorrangig in anonymisierter Form oder zumindest unter Beachtung eines hohen Anonymisierungsgrades erfolgen.

b) Die IKT-Infrastruktur an der Universität Graz versteht sich als Mittel zur produktiveren Durchführung der Arbeit unter Wahrung der aktiven Rolle der MitarbeiterInnen, deren Eigenverantwortlichkeit und deren persönlicher Kommunikationsmöglichkeiten.

c) Automatisierte Einzelentscheidungen i.S.d. § 49 DSG 2000 sind ohne explizite Ermächtigung durch eine Betriebsvereinbarung unzulässig.

d) Die verwendeten Systeme werden von der Arbeitgeberin ausschließlich zur effizienten Abwicklung der Universitätsverwaltung, zur Gewährleistung der Sicherheit an der Universität sowie zur internen und externen Datenkommunikation eingesetzt. Für sämtliche Phasen der Datenverarbeitung gilt der Grundsatz der Zweckbindung in materieller und formeller Weise: der Datenverarbeitung muss nicht nur ein berechtigter Zweck zugrunde liegen, der Verwendungszweck muss vielmehr auch im Vorhinein in der vorliegenden Betriebsvereinbarung festgelegt worden sein **(Grundsatz der Zweckbindung)**.

e) Der Umfang der ermittelten und verwendeten Daten der MitarbeiterInnen sowie die Dauer deren Verwendung sollen auf das unbedingt erforderliche Mindestausmaß begrenzt bleiben **(Grundsatz der Verhältnismäßigkeit)**.

f) Regeln und Kriterien der Datenermittlung und Datenverwendung sollen für alle Beteiligten einsehbar und nachvollziehbar sein **(Grundsatz der Transparenz)**.

g) Die mit personenbezogenen MitarbeiterInnendaten arbeitenden MitarbeiterInnen tragen eine besondere Verantwortung (**Grundsatz der Vertraulichkeit** und **Grundsatz der Rechtmäßigkeit**). Sind solche MitarbeiterInnen über die Zulässigkeit einer Verarbeitung oder Übermittlung im Zweifel, sind sie berechtigt, von ihren Vorgesetzten einen schriftlichen Arbeitsauftrag einzufordern.

(4) Personenbezogene Daten sind grundsätzlich auf zentralen, von der UNI-IT betreuten, Systemen zu verarbeiten. Dafür dürfen - mit Ausnahme der in Abs. 8 genannten Tätigkeiten berechtigter Personen der UNI-IT - ausschließlich die in konkreten Betriebsvereinbarungen angeführten Systeme verwendet werden.

(5) Zentral gehaltene personenbezogene Daten dürfen nur über eine in einer konkreten Betriebsvereinbarung genannte Schnittstelle von einem zentralen PDV-System auf ein anderes zentrales oder auf ein dezentrales PDV-System übernommen werden. Alle anderen Datentransfers und -verknüpfungen sind unzulässig.

(6) Dezentrale PDV-Systeme dürfen nur nach Maßgabe konkreter Betriebsvereinbarungen und nur dann verwendet werden, wenn sie zumindest gleichwertige Qualität der Datensicherheit und -verfügbarkeit wie die zentralen PDV-Systeme sicherstellen. Dies gilt insbesondere für Systeme in Akademischen und Verwaltungseinheiten, bei Universitätsorganen sowie für Systeme, die von Einzelpersonen in welcher Funktion auch immer verwendet werden.

(7) Personenbezogene Daten dürfen - mit Ausnahme der in Abs. 8 genannten Tätigkeiten berechtigter Personen der UNI-IT - nur auf den dafür vorgesehenen Systemen verarbeitet werden. Jede Übertragung von Daten der Kategorien A, C und D gemäß § 7 Abs. 2 auf andere Systeme und Datenträger ist grundsätzlich untersagt.

(8) Für Tätigkeiten berechtigter Personen der UNI-IT gilt: Zur Steigerung der Betriebssicherheit und der technischen Qualitätssicherung der gesamten universitären IKT-Infrastruktur (Problemanalyse, Incident Handling, Qualitätsmanagement) darf die UNI-IT im Anlassfall personenbezogene Daten in manueller oder teilautomatisierter Form, welche von den Anforderungen gem. Abs. 4 und 7 nicht umfasst ist, verarbeiten. Die für den Anlassfall benötigten Kopien der personenbezogenen Daten sind nach Beendigung des Vorganges zu löschen.

§ 7. Kategorisierung der personenbezogenen MitarbeiterInnendaten

(1) Die Kategorisierung der personenbezogenen MitarbeiterInnendaten dient folgenden Zwecken:

a) Aufbereitung der personenbezogenen Daten für eine möglicherweise verpflichtende Meldung beim Datenverarbeitungsregister nach § 17 DSG 2000. Die in einer Standardanwendung laut Standard- und Muster-Verordnung 2004, BGBl. II Nr. 312/2004, in der jeweils geltenden Fassung, angeführten Datenarten müssen nicht gemeldet werden.

b) Grundlage für organisatorische und technische Regelungen bei der Datenverwendung.

c) Sensibilisierung der Führungskräfte und der MitarbeiterInnen für Datenschutz und Datensicherheit.

(2) Die personenbezogenen MitarbeiterInnendaten werden für jedes eingesetzte IKT-System nach den folgenden vier Kategorien unterteilt:

Kategorie A: Sensible Daten im Sinne des § 4 Z. 2 DSG 2000:

Darunter fallen Daten der MitarbeiterInnen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben, sowie biometrische (z.B. Irisscan, Fingerprint), genetische Daten und Profil-Bilder.

Kategorie B: Allgemeine Daten zur Person:

Diese Daten umfassen die geschäftlichen Kommunikationsdaten (z.B.: Name, Einheit, Anschrift, Raum, Telefonnummer, E-Mail-Adresse). Diese Daten können üblicher Weise in einem Unternehmensadressbuch gefunden werden. Sie stehen zwar mit den einzelnen MitarbeiterInnen in Verbindung, gehören aber zu den Arbeitsmitteln im Unternehmen.

Kategorie C: Personenbezogene Daten, die über allgemeine Angaben zur Person und zu fachlichen Voraussetzungen hinausgehen, sofern sich die deren Ermittlung, Verarbeitung oder Übermittlung verpflichtend aus Gesetz, Verordnung, Norm der kollektiven Rechtsgestaltung oder dem Arbeitsvertrag ergibt und die nur für diesen eindeutigen Zweck verwendet werden dürfen:

Diese Daten müssen von der Arbeitgeberin zwingend verwendet werden. In diesen Fällen werden die Daten benötigt, um rechtlichen Verpflichtungen nachkommen zu können, z.B. im Zusammenhang mit Pfändungen, Gehaltsvorschüssen oder Geldaushilfen. Darüber hinaus können in diese Kategorie durch Betriebsvereinbarung zwischen der Arbeitgeberin und den Betriebsräten weitere Datenarten aufgenommen werden (z.B.: Anschrift, Arbeitszeit, Urlaubsanspruch, Bankverbindung, Qualifikationen, betriebliche Funktion).

Kategorie D: Sonstige Daten, die nicht unter die Kategorien A, B oder C fallen:

Diese Daten gehören zum Teil zu den Stammdaten, sind aber primär dem Privatbereich der MitarbeiterInnen zuzuordnen und stehen nicht direkt mit dem Arbeitsverhältnis in Verbindung (z.B. Familienstand, Zweitwohnsitz). Hierunter fallen Daten, die Aussagen über das Verhalten einzelner MitarbeiterInnen enthalten können (z.B. Abwesenheiten und Mehrdienstleistungen, Leistungsstunden für diverse Aufträge/Projekte, die Vergleiche zulassen, leistungsabhängige Entgeltbestandteile, Beurteilungen, vereinbarte Ziele aus MitarbeiterInnengesprächen).

§ 8. Umfang der Datenverwendung

(1) Von den MitarbeiterInnen werden entsprechend den im Anhang B enthaltenen Personendaten verarbeitenden Systemen ausschließlich die dort aufgelisteten Daten zu den dort vorgegebenen Zwecken verarbeitet bzw. übermittelt, sofern

a) sich die Berechtigung unmittelbar aus Gesetz, Verordnung oder Norm der kollektiven Rechtsgestaltung ergibt oder

b) die verwendete IKT-Infrastruktur, die Verwendungszwecke, der betroffene Personenkreis, die Zugriffsberechtigten, die DatenadressatInnen und die Speicherdauer in der vorliegenden oder einer anderen Betriebsvereinbarung bestimmt bzw. enthalten sind.

(2) Die Daten von MitarbeiterInnen dürfen weder zu Zwecken der Leistungskontrolle, der betrieblichen oder außerbetrieblichen Kontrolle des Verhaltens der MitarbeiterInnen noch der MitarbeiterInnenbeurteilung bzw. Evaluierung der/des Einzelnen herangezogen werden, sofern dies nicht ausdrücklich durch Gesetz, Verordnung oder eine Norm der kollektiven Rechtsgestaltung vorgesehen ist.

(3) Fotos der MitarbeiterInnen werden ausschließlich für universitätseigene Ausweise und Publikationen (Veröffentlichungen) verwendet. Die Auswahl der Fotos bedarf der Zustimmung des einzelnen Mitarbeiters/der einzelnen Mitarbeiterin.

(4) Von den Systemverantwortlichen ist zu prüfen, ob das angestrebte Ziel der Datenverwendung auch ohne Personenbezug mit vertretbarem Aufwand erreicht werden kann. Ist dies nicht der Fall, ist die Notwendigkeit des Abschlusses einer Einzelbetriebsvereinbarung für das konkrete IKT-System unter Anwendung des im Anhang A geregelten Geschäftsprozesses zu prüfen und bejahendenfalls eine Einzelbetriebsvereinbarung abzuschließen.

(5) Eine Verwendung von personenbezogenen MitarbeiterInnendaten, die im Rahmen einer Verpflichtung aus Gesetz, Verordnung oder Norm der kollektiven Rechtsgestaltung erfolgt, kann ohne vorheriges Einverständnis der Betriebsräte durchgeführt werden. Die Betriebsräte sind jedoch im Vorhinein zu informieren und können die Notwendigkeit (d.h., ob eine Auswertung im Rahmen, der in einer der genannten Rechtsquellen festgeschrieben ist, liegt) überprüfen.

(6) Aus Data Warehouses dürfen Ad-hoc-Berichte (das heißt einmalige Auswertungen bzw. nicht standardisiert verfügbare Auswertungen nach frei zusammengestellten Auswertungskriterien), die personenbezogene ArbeitnehmerInnendaten umfassen, und von einer internen oder externen anfordernden Stelle angefragt werden, ausschließlich zur Abdeckung eines im Einzelfall nicht vorhersehbaren bzw. nicht standardisiert verfügbaren, sachlich begründeten Auswertungsbedarfs durchgeführt werden. Die in einem IKT-System für Ad-hoc- Berichte befugten Zugriffsberechtigungen sind im Rollenkonzept der jeweiligen Systembeschreibung gem. § 14 Abs. 2 dieser Betriebsvereinbarung darzustellen. Ad-hoc-Berichte, die von einer internen oder externen anfordernden Stelle angefragt werden, bedürfen der Genehmigung der Rektorin bzw. des Rektors, wenn sie nicht öffentlich verfügbare Einzeldaten von ArbeitnehmerInnen umfassen oder wenn sie im Fall von Medienanfragen nicht bereits öffentlich verfügbare aggregierte Daten beinhalten. Die Genehmigung der Rektorin bzw. des Rektors darf nur nach vorheriger Einholung einer Stellungnahme der Datenschutzkontaktperson erfolgen.

§ 9. Zugriff auf IKT-Systeme

(1) Es ist sicherzustellen, dass nur befugte Personen Zugang zu personenbezogenen und vertraulichen Daten haben. Dafür sind geeignete Identifikations- und Authentisierungsmethoden einzusetzen (z.B. Benutzerkennung und Passwort).

(2) Berechtigungen für den Zugriff auf Daten sind nur in dem Umfang zu erteilen, wie dies für die Aufgabenerfüllung notwendig ist. Diese Rechte sind Inhalt der Systembeschreibungen laut Anhang B.

(3) Bei Systemen und Anwendungen, die für den Betrieb der Universität Graz oder eine ihrer Einheiten von geschäftswichtiger Bedeutung sind, muss im Vertretungsfall weiterhin ein administrativer Zugang möglich sein. Dies hat in einer von Personen unabhängigen Weise gelöst zu werden, daher keinesfalls in Form von Passwortlisten.

§ 10. Aufzeichnungen über Datenzugriffe bzw. über BenutzerInnenverhalten

A. Systemsoftware:

(1) Aufzeichnungen und Auswertungen der Systemsoftware über BenutzerInnenaktivitäten (z.B. Logins, durchgeführte Transaktionen) dürfen nur verwendet werden für die

a) Gewährleistung der Systemsicherheit,

b) Abrechnung der Systemnutzung,

c) Analyse und Korrektur von technischen Fehlern im System und

d) Optimierung der Rechnerleistung.

(2) Der Zugriff auf die entsprechenden Funktionen wird auf die MitarbeiterInnen, die für die Wartung der Hard- und Software zuständig sind, begrenzt.

(3) Die entsprechenden Dateien werden nach Ablauf von zwölf Monaten jeweils zu Quartalsende gelöscht.

B. BearbeiterInnenkennzeichen:

(4) Der in Dateien eines Systems gespeicherte BenutzerInnenname bzw. ein ihn identifizierbares Kennzeichen darf nur in Anzeigen oder Ausdrucken von auf die einzelnen Vorgänge bezogenen Daten (z.B. Sachbelege wie ein Rechnungswesensbeleg in SAP, der den BenutzerInnennamen des Belegerfassers/der Belegerfasserin enthält) verwendet werden.

(5) Es werden keine Programmfunktionen zur Verfügung gestellt, die Statistiken oder Listen erstellen, in denen der BenutzerInnenname bzw. eine entsprechende Kennung erscheinen oder die mit Zugriff auf solche Daten entstehen.

(6) Felder in Bewegungsdateien, die BenutzerInnennamen oder SachbearbeiterInnenkürzel enthalten, werden für die Abfrageinstrumente auf Endbenutzerebene gesperrt. Ausnahmen von den vorgenannten Regelungen bedürfen der vorherigen Zustimmung der Betriebsräte.

C. Remote-Zugriff auf Endgeräte auf Betriebssystemebene:

(7) Die Möglichkeit eines Remote-Zugriffs auf Endgeräte dient ausschließlich einer effizienten Unterstützung im Problem- oder Fehlerfall.

(8) Zur Aktivierung des Remote-Zugriffs ist von der/dem jeweiligen BenutzerIn in jedem Einzelfall die Zustimmung zur Verwendung einzuholen. Nach durchgeführtem Remote-Zugriff wird der Zugriff beendet.

(9) Der Remote-Zugriff darf nur vom 1st und 2nd-Level Support der UNI-IT und nur von bestimmten Subnetzen der UNI-IT aus erfolgen.

(10) Die/der BenutzerIn kann den Remote-Zugriff mitverfolgen.

(11) Die Aktionen im Rahmen des Remote-Zugriffs sind in einem eigenen Logfile auf dem jeweiligen Endgerät mit zu protokollieren.

(12) Die Leitung der UNI-IT ist berechtigt, bei Gefahr in Verzug (z.B. in sicherheitskritischen Situationen) über ein Push-Service die Verteilung von Patches auf Endgeräte zu veranlassen.

D. Remote-Zugriffe für die Verwaltung (Management) von IKT-Endgeräten

(13) Die Möglichkeit eines automatischen Zugriffes auf Endgeräte dient ausschließlich der Erfassung der vorhandenen Hard- und Softwarekomponenten und deren Änderungen.

(14) Der Zugriff darf nur von bestimmten Subnetzen der UNI-IT aus erfolgen.

(15) Die auf diese Weise erfassten Daten dürfen ausschließlich in anonymisierter oder aggregierter Form weitergegeben, gespeichert oder verwendet werden.

§ 11. Übertragung von Daten auf PC's, mobile Endgeräte etc.

Die Übertragung von personenbezogenen Daten auf PC, Laptop, mobile Endgeräte (z.B. Smartphone, Tablet-PC, PDA) oder dgl. sowie von solchen Geräten auf bewegliche Speichermedien (z.B. USB-Stick, externe Festplatten, Datenbänder) soll die Ausnahme darstellen. In diesen Fällen gilt eine besondere Sorgfaltspflicht und es kann eine persönliche Verantwortlichkeit mit entsprechenden Haftungen entstehen.

§ 12. Datenarchivierung

(1) Sämtliche in Zusammenhang mit der vorliegenden Betriebsvereinbarung ermittelten Daten sind zu archivieren, wenn entweder ein Auftrag aus Gesetz, Verordnung oder Norm der kollektiven Rechtsgestaltung dafür vorliegt oder die Archivwürdigkeit der Daten im Sinne einer zukünftigen wissenschaftlichen Verwendung, analog zur Aufbewahrungspflicht unikal überlieferten Schriftguts, gegeben ist.

(2) Die Migration der Daten in eine strukturierte Textdarstellung muss so beschaffen sein, dass eine langfristige Archivierungs- und Wartungsstrategie möglich ist.

(3) Die technische Umsetzung im Sinne einer Langzeitarchivierung digitaler Daten sowie der Zugang zu diesen Daten sind in einer eigenen Archivordnung mit Zustimmung der Betriebsräte zu regeln.

(4) Sämtliche Archivierungsvorgänge sind zu protokollieren und in einem digitalen Meta-Datenset als Basisverzeichnung zu verwalten.

§ 13. Löschen von Daten

(1) Sämtliche im Zusammenhang mit der vorliegenden Betriebsvereinbarung ermittelten Daten sind im jeweiligen Produktionssystem zu löschen, sobald ihre Speicherung/Verwendung zu einem in der Betriebsvereinbarung festgelegten Zweck nicht mehr erforderlich ist.

(2) Wenn es sich bei zentralen Personendaten verarbeitenden Systemen um archivwürdige Daten im Sinne des § 12 handelt, sind sie zuvor entsprechend zu archivieren.

(3) Sämtliche Löschvorgänge sind zu protokollieren.

(4) Spam-Mails, die von den Sicherheitseinrichtungen unter der Eingriffsmöglichkeit des Benutzers/der Benutzerin als solche (automatisch) klassifiziert werden bzw. die von im Internet publizierten höchst verdächtigen Mail-Servern stammen, werden entweder vom Mailsystem nicht angenommen oder als Spam gekennzeichnet und in Abhängigkeit der verwendeten Software in einen Quarantäneordner abgelegt.

IV. SYSTEMBESCHREIBUNG UND -EINSATZ

§ 14. Zentrale Personendaten verarbeitende Systeme

(1) An der Universität Graz kommen zur Ermittlung, Verarbeitung und Übermittlung von personenbezogenen MitarbeiterInnendaten ausschließlich die im Anhang B angeführten zentralen Personendaten verarbeitenden Systeme zur Anwendung.

(2) Im Anhang B werden sämtliche Systeme der IKT-Infrastruktur der Universität Graz genannt, die mit personenbezogenen MitarbeiterInnendaten operieren. In diesem Anhang ist jedes IKT-System mit folgenden Angaben zu beschreiben:

a) Name des IKT Systems,

b) Name der betreibenden Organisationseinheit, Akademischen Einheit oder Verwaltungseinheit,

c) Verantwortliche Personen und Vertretung,

d) Systembeschreibung, Verwendungszweck und potentieller Einsatzzweck,

e) Betroffene Personengruppen (Von welcher Personengruppe werden die Daten erfasst bzw. verarbeitet?),

f) Datenarten (Welche Daten werden erfasst, verarbeitet, gespeichert, gelöscht? Quellsysteme der Daten),

g) DatenadressatInnen (taxative Auflistung der möglichen Zielsysteme sowie welche Daten tatsächlich überspielt werden) und

h) Zugriffsberechtigungen (Die Zugriffsberechtigungen sind als Rollenkonzept darzustellen. Warum muss eine Rolle vergeben werden?).

(3) Im Anhang B werden die Datenflüsse zwischen den IKT-Systemen der Universität Graz grafisch dargestellt.

(4) Die Anwendung neuer Versionen der in den zentralen Personendaten verarbeitenden Systemen eingesetzten Software bedarf keiner Zustimmung der Betriebsräte, sofern ausschließlich programmtechnische Änderungen vorgenommen werden, die die Datenarten, die Datenstrukturen und deren Verknüpfungen, sowie Art und Umfang der Zwecksetzung der Datenverwendungen und damit die Zielsetzung der Mitbestimmung unberührt lassen. Änderungen der eingesetzten Softwareprodukte sowie Änderungen in der Software-Funktionalität sind aber den Betriebsräten und dem Datenschutzbeirat gem. § 21 unverzüglich mitzuteilen.

(5) Alle Daten, die über eine Schnittstelle von einem zentralen Personendaten verarbeitenden System auf ein anderes übernommen werden, sind im Anhang B auszuweisen. Alle anderen nicht im Anhang B angeführten Datentransfers und -verknüpfungen sind unzulässig.

(6) Alle Personendaten verarbeitenden Systeme der Universität Graz sollen grundsätzlich auf Servern der Universität Graz installiert sein. Abweichungen davon (insbesondere Cloud-Lösungen) sind jedenfalls nach Durchführung eines Verfahrens nach § 20 dieser Betriebsvereinbarung im Anhang B zu regeln.

(7) Unter den im Anhang B genannten Personendaten verarbeitenden Systemen gilt SAP-HR als führendes System. Ein Subset von Personendaten wird täglich über eine definierte Schnittstelle nach UNIGRAZonline überspielt. Alle weiteren zentralen Personendaten verarbeitenden Systeme übernehmen ihre Daten aus UNIGRAZonline.

(8) Ein Zurückschreiben von Daten in übergeordnete Systeme wie SAP-HR ist unzulässig. Dies gilt insbesondere für folgende Daten:

a) übernommene und dann veränderte personenbezogene Daten selbst,

b) Daten, die aufgrund ihres Inhalts unmittelbar mit personenbezogenen Daten des übergeordneten Systems verknüpft werden können sowie

c) Daten, welche personenbezogene Daten des übergeordneten Systems unmittelbar anreichern.

Alle Ausnahmen von den Regelungen dieses Absatzes sind in eigenen Betriebsvereinbarungen zu regeln.

§ 15. Dezentrale Personendaten verarbeitende Systeme

(1) Unter einem dezentralen Personendaten verarbeitenden System wird der Einsatz von Software und die Verarbeitung von personenbezogenen Daten in Organisations- und Akademischen Einheiten, universitäts- und fakultätsübergreifenden Leistungsbereichen, im Drittmittelbereich, in universitären Gremien und Kommissionen, sonstigen Universitätsorganen und durch Einzelpersonen verstanden.

(2) An der Universität Graz kommen ausschließlich die im Anhang B angeführten dezentralen Personendaten verarbeitenden Systeme zur Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten zur Anwendung.

(3) Die Einführung und Weiterverwendung von Systemen zur Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der MitarbeiterInnen ist für den gesamten Betrieb der Universität Graz unzulässig, sofern diese Systeme nicht in der vorliegenden oder einer sonstigen Betriebsvereinbarung geregelt sind. Dies gilt insbesondere für Systeme in Organisations- und Akademischen Einheiten, universitäts- und fakultätsübergreifenden Leistungsbereichen, im Drittmittelbereich, in universitären Gremien und Kommissionen sowie für Systeme, die von Einzelpersonen in welcher Funktion auch immer verwendet werden.

(4) Verletzungen dieser Bestimmung können nicht nur schadenersatzrechtliche Folgen, insbesondere gemäß § 33 DSG 2000, nach sich ziehen, sondern bilden auch eine Dienstpflichtverletzung.

(5) Nicht im Anhang B angeführte dezentrale Personendaten verarbeitende Systeme sind unverzüglich stillzulegen.

V. RECHTE UND PFLICHTEN

§ 16. Rechte und Pflichten der Arbeitgeberin

(1) Die Arbeitgeberin hat den Betrieb von ihr zur Kenntnis gebrachten IKT-Systemen, die aufgrund der vorliegenden oder einer anderen Betriebsvereinbarung unzulässig sind, unverzüglich zu unterbinden.

(2) Die Arbeitgeberin hat den MitarbeiterInnen den Inhalt der vorliegenden Betriebsvereinbarung und der auf ihrer Basis abgeschlossenen Einzel-Betriebsvereinbarungen im Intranet der Universität Graz zugänglich zu machen.

(3) Die Arbeitgeberin hat die MitarbeiterInnen, insbesondere auch neu Eintretende, über die Verarbeitung ihrer personenbezogenen Daten im Zusammenhang mit der IKT-Infrastruktur zu informieren.

(4) Die Arbeitgeberin hat für MitarbeiterInnen relevante betriebliche Änderungen und Unterbrechungen des Betriebs der IKT-Systeme in einem geeigneten innerbetrieblichen Medium (z.B. Intranet) anzukündigen. Es wird allen MitarbeiterInnen empfohlen, diese Meldungen regelmäßig zu verfolgen.

(5) Die Arbeitgeberin hat das Recht, die verwendete IKT-Infrastruktur stets auf dem aktuellen Stand der Technik zu halten, soweit sich aus der vorliegenden Betriebsvereinbarung nichts anderes ergibt. In den Fällen, die in Gesetz, Verordnung oder Norm der kollektiven Rechtsgestaltung vorgesehen sind, und bei wesentlichen Erweiterungen und/oder Änderungen eines IKT-Systems ist vorab die Zustimmung der Betriebsräte einzuholen. Eine wesentliche Änderung eines IKT-Systems liegt insbesondere vor, wenn

a) durch sie zusätzliche personenbezogene Daten erhoben, gespeichert und verarbeitet werden,

b) weitere Funktionsmerkmale, mit denen personenbezogene Daten verarbeitet werden, aktiviert werden,

c) der Kreis der Zugriffsberechtigten erweitert wird,

d) neue personenbezogene Auswertungen ermöglicht werden,

e) der physische Speicherort geändert wird

oder

f) die verantwortlichen Personen geändert werden.

(6) Die Anwendung neuer Versionen der in den Systemen eingesetzten Software bedarf keiner Zustimmung der Betriebsräte, sofern sie keine grundlegende Erweiterung darstellen.

§ 17. Allgemeine Rechte und Pflichten der MitarbeiterInnen

(1) Alle MitarbeiterInnen erhalten von der Arbeitgeberin auf Anforderung einmal jährlich eine kurze, allgemein verständliche Auflistung ihrer jeweiligen persönlichen Daten im Sinne des § 26 DSG 2000.

(2) Alle MitarbeiterInnen haben das Recht, Daten richtigstellen bzw. löschen zu lassen, wenn sie nicht berechtigt ermittelt wurden, wenn sie nicht richtig sind oder für den vorgesehenen Zweck nicht (mehr) erforderlich sind. Diesen Personen und dem für sie zuständigen Betriebsrat ist eine Überprüfungsmöglichkeit über die Korrektur bzw. Löschung einzuräumen. Entsteht Uneinigkeit über die Richtigkeit von Daten und kann die Arbeitgeberin die Richtigkeit nicht nachweisen, so sind diese Daten zu löschen.

(3) Alle persönlichen Zugangsdaten, Passwörter und sonstige Authentisierungs(hilfs)mittel sind vertraulich zu halten und nicht weiterzugeben. Auch eine Weitergabe an Vorgesetzte, System- und NetzwerkadministratorInnen oder anderes IKT-Personal ist nicht zulässig. Im Vertretungsfall muss gem. § 9 Abs. 3 dieser Betriebsvereinbarung in einer von Personen unabhängigen Weise (keinesfalls in Form von Passwortlisten) ein administrativer Zugang möglich sein.

§ 18. Rechte und Pflichten der Betriebsräte

(1) Bei der Änderung bestehender IKT-Systeme und bei der Beschaffung von neuen Systemen ist zur Wahrung der Mitwirkungsrechte der Betriebsräte das im § 20 beschriebene Verfahren für den Abschluss von Einzel-Betriebsvereinbarungen einzuhalten.

(2) Die Betriebsräte haben das Recht, sämtliche Personendaten verarbeitenden Systeme der Universität Graz, insbesondere die einzelnen Hard- und Softwarekomponenten, jederzeit daraufhin zu prüfen, ob diese der vorliegenden Betriebsvereinbarung entsprechen.

(3) 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 Arbeitgeberin zu tragen, sofern die Grundsätze der Angemessenheit sowie der Verhältnismäßigkeit gewahrt bleiben.

(4) Die Arbeitgeberin hat den Betriebsräten über allgemeine interne Aus-, Fortbildungs- und sonstige Schulungsmaßnahmen betreffend die eingesetzten Personendaten verarbeitenden Systeme zu informieren. Zwei Mitglieder jedes Betriebsrats sind jeweils berechtigt, an den internen Schulungen kostenlos teilzunehmen.

(5) Im Fall geplanter Änderungen und Ergänzungen der Personendaten verarbeitenden Systeme sind die Bestimmungen des § 109 ArbVG, insbesondere auch § 109 Abs. 1a ArbVG, sinngemäß anzuwenden.

§ 19. Datenschutzbericht

Das laut Geschäftsplan für das Informationsmanagement zuständige Rektoratsmitglied hat den Betriebsräten einmal in jedem Studienjahr einen Bericht zu Datenschutz und Datensicherheit an der Universität Graz vorzulegen.

VI. VERFAHREN BEI DER ÄNDERUNG UND NEUEINFÜHRUNG VON IKT-SYSTEMEN

§ 20. Verfahren

(1) Im Anhang A wird das bei der Änderung bestehender IKT-Systeme und bei der Beschaffung von neuen Systemen zur Wahrung der Mitwirkungsrechte der Betriebsräte verbindlich einzuhaltende Verfahren grafisch dargestellt. Darin ist der Ablauf für den Abschluss von Einzel-Betriebsvereinbarungen mit den jeweils tätig werdenden Organen der Arbeitgeberin, den Betriebsräten, dem Datenschutzbeirat, der Datenschutzkontaktperson sowie den Verwaltungseinheiten so darzustellen, dass folgende Verfahrensschritte abgebildet werden:

a) Planung der Einführung (= Änderung bestehender IKT-Systeme, Beschaffung und/oder Implementierung von neuen IKT-Systemen) eines Systems (durch die einführende Abteilung),

b) Ausfüllen des Sheets, Beschreibung des Systems (durch die einführende Abteilung),

c) Sammeln der Inputs und Vorprüfung anhand der vorliegenden Betriebsvereinbarung (durch die Datenschutzkontaktperson),

d) Befassung des Datenschutzbeirats mit gleichzeitiger Information der Betriebsräte (durch die Rechts- und Organisationsabteilung),

e) Führen eines Dialogs mit Vorsitzenden bzw. VertreterInnen der Betriebsräte (durch die einführende Abteilung),

f) Beratung und Stellungnahme binnen sechs Wochen ab der Befassung, ob es sich um ein IKT-System der Kategorien B oder C handelt oder ob im Sinne der Kategorien A oder D ein Anhang zur vorliegenden Betriebsvereinbarung oder eine eigene Betriebsvereinbarung notwendig ist (durch den Datenschutzbeirat),

g) Beschluss über die Einordnung in eine Kategorie mit unverzüglicher Mitteilung an die Betriebsräte (durch das Rektorat)

h) Unverzügliche Aufnahme der Verhandlung und Erstellung eines Anhangs zur vorliegenden Betriebsvereinbarung oder einer eigenen Betriebsvereinbarung (Koordination durch die Rechts- und Organisationsabteilung),

i) Beschluss des Anhangs bzw. der eigenen Betriebsvereinbarung durch das Rektorat, Einholung der Zustimmung der Betriebsräte und formeller Abschluss durch Unterzeichnung (Koordination durch die Rechts- und Organisationsabteilung),

j) Einführung des Systems (durch die einführende Abteilung in Abstimmung mit der UNI-IT),

k) allfällige Änderung des Systems (durch die einführende Abteilung oder die UNI-IT) und

l) laufende Kontrolle (durch das jeweils aufgrund Gesetz, Verordnung oder Normen der kollektiven Rechtsgestaltung zuständige Organ).

(2) Sofern bei der Entwicklung und Erweiterung von IKT-Systemen Simulationsdaten (Testdaten), verwendet werden müssen, gilt: Falls eine Anonymisierung nicht möglich ist, dürfen personenbezogene Echtdaten von MitarbeiterInnen verwendet werden. In diesem Fall ist jedoch der Prozess zum Abschluss einer Einzel-Betriebsvereinbarung laut Anhang A der vorliegenden Betriebsvereinbarung einzuhalten.

VII. DATENSCHUTZBEIRAT UND DATENSCHUTZKONTAKTPERSON

§ 21. Datenschutzbeirat

(1) Zur Beratung aller Fragen, die sich im Zusammenhang mit der Einführung, dem Betrieb, der Auslegung und den Änderungen von IKT-Systemen ergeben, wird ein innerbetrieblicher Datenschutzbeirat gebildet. Die Beratungen, Ergebnisse und Erkenntnisse des Datenschutzbeirats dienen für die Arbeitgeberin und die Betriebsräte als Entscheidungshilfe.

(2) Aufgabe des Datenschutzbeirats ist es, einen Interessenausgleich zwischen Arbeitgeberin und Betriebsräten herbeizuführen. Er ist auch zu befassen, wenn bei Fragen im Zusammenhang mit der vorliegenden Betriebsvereinbarung keine Einigung erzielt wird. Weiters ist der Datenschutzbeirat vor geplanten Änderungen und/oder vor der geplanten Einführung von neuen IKT-Systemen, die die Verwendung personenbezogener Daten ermöglichen, entsprechend zu informieren.

(3) Arbeitgeberin und Betriebsräte verpflichten sich, im Konfliktfall erst dann den Rechtsweg zu beschreiten, wenn innerhalb zweier Monate ab der ersten Befassung des Datenschutzbeirats keine Einigung zustande gekommen ist. Dies wird dann als gegeben angenommen, wenn im Zuge der Beschlussfassung keine Einigung erzielt wird oder ein Beschluss innerhalb zwei Monaten ab der ersten Befassung des Datenschutzbeirats nicht zustande gekommen ist.

(4) Dem Datenschutzbeirat gehören an:

a) vier von der Arbeitgeberin nominierte VertreterInnen und

b) vier von den Betriebsräten nominierte VertreterInnen (je zwei vom Betriebsrat für das Wissenschaftliche Universitätspersonal und vom Betriebsrat für das Allgemeine Universitätspersonal).

(5) In jeweils gleicher Zahl sind von beiden Seiten Ersatzmitglieder namhaft zu machen.

(6) Den Vorsitz führt abwechselnd für jeweils zwei Studienjahre ein von den Betriebsräten namhaft gemachtes Mitglied und ein von der Arbeitgeberin namhaft gemachtes Mitglied. In den ersten beiden Studienjahren ab dem Inkrafttreten der vorliegenden Betriebsvereinbarung führt ein von den Betriebsräten nominiertes Mitglied den Vorsitz.

(7) Die Konstituierung des Datenschutzbeirats und die Wahl eines/einer Vorsitzenden sowie eines/einer Stellvertreter/in haben innerhalb von drei Monaten nach In-Kraft-Treten der vorliegenden Betriebsvereinbarung zu erfolgen.

(8) Die für die Ausübung der Mitgliedschaft im Datenschutzbeirat erforderliche Zeit stellt bezahlte Arbeitszeit der Mitglieder dar. Den Mitgliedern dürfen aus dieser Tätigkeit keine Nachteile entstehen.

(9) Für die Geschäftsführung und die organisatorischen Abläufe des Datenschutzbeirats ist sinngemäß die Geschäftsordnung des Senats und aller Senatskommissionen der Karl-Franzens-Universität Graz in der Fassung des Mitteilungsblatts vom 4.8.2004, 21.a Stück, 46. Sondernummer, anzuwenden.

(10) Der Datenschutzbeirat ist beschlussfähig, wenn von Seiten der Arbeitgeberin zumindest zwei Mitglieder und von Seiten der beiden Betriebsräte zumindest je ein Mitglied anwesend sind. Gültige Beschlüsse können nur einstimmig gefasst werden und sind zu protokollieren.

(11) Der Datenschutzbeirat tagt zumindest einmal pro Semester. Der/Die Vorsitzende kann darüber hinaus jederzeit bei Bedarf eine Sitzung einberufen.

(12) Die Datenschutzkontaktperson gem. § 22 der vorliegenden Betriebsvereinbarung hat das Recht, an allen Sitzungen des Datenschutzbeirats als nicht stimmberechtigtes Mitglied teilzunehmen und ist nachweislich zu diesen einzuladen.

§ 22. Datenschutzkontaktperson

(1) Die Arbeitgeberin bestellt im Einvernehmen mit den Betriebsräten eine Datenschutzkontaktperson. Deren Aufgaben sind:

a) Überwachung der Einhaltung der Gesetze, insbesondere des DSG 2000, der Verordnungen sowie der Normen der kollektiven Rechtsgestaltung im Hinblick auf der an der Universität Graz verwendeten IKT-Systeme und

b) Funktion als Anlauf- und Auskunftsstelle für Fragen der Arbeitgeberin, der MitarbeiterInnen, der Betriebsräte, des Arbeitskreises für Gleichbehandlungsfragen, der Behindertenvertrauensperson sowie von sonstigen FunktionsträgerInnen der Universität Graz.

(2) Personenbezogene Daten von MitarbeiterInnen der Universität Graz dürfen von der Datenschutzkontaktperson nicht weitergegeben werden. Dies gilt auch für berechtigte Anfragen gemäß Abs. 1 lit. b sowie für Anträge von Betroffenen.

VIII. FORMALE BESTIMMUNGEN

§ 23. Anhänge als Teile der Betriebsvereinbarung

Die Anhänge bilden integrale Bestandteile der vorliegenden Betriebsvereinbarung und sind daher untrennbar mit deren Stammtext in seiner jeweils geltenden Fassung verbunden.

§ 24. Unberührt bleibende Rechte

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

§ 25. Unberührt bleibende Betriebsvereinbarungen

Folgende Betriebsvereinbarungen bleiben durch die vorliegende Betriebsvereinbarung unberührt:

a) Betriebsvereinbarung über die Lehrveranstaltungsevaluierung vom 2.9.2008 (nur mit dem Betriebsrat für das Wissenschaftliche Universitätspersonal) laut Mitteilungsblatt vom 3.9.2008, 48.a Stück, 86. Sondernummer,

b) Betriebsvereinbarung über die Einführung und Verwendung elektronischer Schließsysteme und Zutrittskontrollsysteme laut Mitteilungsblatt vom 21.7.2010, 39.d Stück, 52. Sondernummer,

c) Betriebsvereinbarung über die Benützung von digitalen Bild- und Tonübertragungsanlagen in Lehrveranstaltungsräumen (nur mit dem Betriebsrat für das Wissenschaftliche Universitätspersonal) laut Mitteilungsblatt vom 10.8.2011, 45.a Stück, 135. Sondernummer,

d) Betriebsvereinbarung über die Abrechnung von Kopier- und Telefonkosten vom 31.1.2013 laut Mitteilungsblatt vom 8.2.2013, 19.b Stück, 25. Sondernummer,

e) Betriebsvereinbarung zur Förderung der nachhaltigen Mobilität sowie zur Vergabe von Parkplätzen an der Karl-Franzens-Universität Graz vom 11.12.2013 laut Mitteilungsblatt vom 12.12.2013, 11.a Stück, 10. Sondernummer und

f) Betriebsvereinbarung über die Montage und den Betrieb von Videoüberwachungsanlagen an der Karl-Franzens-Universität Graz vom 25.2.2015 laut Mitteilungsblatt vom 4.3.2015, 22.a Stück, 26. Sondernummer.

§ 26. Publikation

Der Stammtext der vorliegenden Betriebsvereinbarung ist im Mitteilungsblatt der Universität zu publizieren. Die Anhänge sind nicht zu veröffentlichen, sondern in der Zentralen Registratur zur Einsichtnahme für die MitarbeiterInnen der Universität Graz aufzulegen sowie den Betriebsräten zur Verfügung zu stellen. Die Inhalte der Anhänge unterliegen der Verschwiegenheitspflicht.

§ 27. Auslegung

Für die Interpretation der vorliegenden Betriebsvereinbarung ist – soweit sich aus dem Gesamtzusammenhang nichts anderes ergibt – die Begriffsbildung des DSG 2000 und des ArbVG heranzuziehen.

§ 28. Übergangsbestimmung

(1) Die vorliegende Betriebsvereinbarung tritt am 21.06.2017 in Kraft. Sie ersetzt die Betriebsvereinbarung über die Ermittlung, Verwendung und Übermittlung von ArbeitnehmerInnendaten ("BV PDVS"), verlautbart im Mitteilungsblatt vom 16.04.2008, 28.a Stück, 14. Sondernummer.

(2) Anhang II (dezentrale Systeme) der Betriebsvereinbarung über die Ermittlung, Verwendung und Übermittlung von ArbeitnehmerInnendaten ("BV PDVS"), wird in den Anhang B der vorliegenden Betriebsvereinbarung übernommen. Dieser Anhang B ist bezüglich der dezentralen Systeme binnen 6 Monaten ab Inkrafttreten der vorliegenden Betriebsvereinbarung im Sinne der vorliegenden Rahmenbetriebsvereinbarung zu adaptieren. Erfolgt dies nicht innerhalb von weiteren 6 Monaten, tritt Anhang B hinsichtlich der betroffenen dezentralen Systeme außer Kraft.

Graz, am 20.06.2017

Für die Arbeitgeberin:
Univ.-Prof. Dr. Christa Neuper (Rektorin)

Für den Betriebsrat für das wissenschaftliche Universitätspersonal:
Ao. Univ.-Prof. Dr. Ingo Kropač (Vorsitzender)

Für den Betriebsrat für das allgemeine Universitätspersonal:
Regina Lammer, MSc (Vorsitzende)

Anhang A zur Rahmen-BV IKT

Prüfung eines Systems anhand den Kriterien der Rahmen-BV-IKT *(Stand 25. Mai 2016)*