

MITTEILUNGSBLATT DER KARL-FRANZENS-UNIVERSITÄT GRAZ



www.uni-graz.at/zvwww/miblatt.html

52. SONDERNUMMER

Studienjahr 2009/10

Ausgegeben am 21. 7. 2010

39.d Stück

BETRIEBSVEREINBARUNG ÜBER DIE EINFÜHRUNG UND VERWENDUNG ELEKTRONISCHER SCHLISSYSTEME UND ZUTRIITTSKONTROLLSYSTEME

Impressum: Medieninhaber, Herausgeber und Hersteller: Karl-Franzens-Universität Graz,
Universitätsplatz 3, 8010 Graz. Verlags- und Herstellungsort: Graz.
Anschrift der Redaktion: Administration und Dienstleistungen, Universitätsdirektion, Universitätsplatz 3,
8010 Graz. E-Mail: mitteilungsblatt@uni-graz.at

**BETRIEBSVEREINBARUNG
ÜBER DIE EINFÜHRUNG UND VERWENDUNG
ELEKTRONISCHER SCHLIESSYSTEME
UND ZUTRITTSKONTROLLSYSTEME**

abgeschlossen zwischen

der Karl-Franzens-Universität Graz

vertreten durch den Rektor, Herrn Univ.-Prof. Mag. Dr. Alfred Gutschelhofer

und

dem Betriebsausschuss an der Karl-Franzens-Universität Graz

vertreten durch dessen Vorsitzenden, Herrn Univ.-Prof. MMag. DDr. Günther Löschnigg

INHALT

Präambel	2
I. Geltungsbereich und Gegenstand	2
II. Beschreibung der Systeme	2
Systemdarstellung	2
Systemeinsatz	3
III. Datenverwendung	4
Datenfluss	4
Löschregelung	4
Zugriffsberechtigungen	5
Datentransfer	5
IV. Informations-, Mitwirkungs- und Kontrollrechte der Betriebsräte	5
V. Schlussbestimmungen	6
Anhang 1 – Systemdarstellung	7
Anhang 2 – Einhaltung der Bestimmungen der BV	8

PRÄAMBEL

Der Einsatz elektronischer Schließsysteme ist als Mittel zur Erleichterung des technischen Alltagsbetriebes, zur Minimierung der Kosten im Fall des Verlustes von Zugangsmitteln (Token) und zur Sicherung des Gebäudes und besonders schützenswerter Zonen darin gegen unbefugtes Betreten und rechtswidrige Vorgänge (insbesondere Diebstahl und Vandalismus) konzipiert. Auf diese Zwecke ist der laufende Betrieb und jede den Betrieb administrierende oder ändernde Tätigkeit auszurichten. Die Anlage ist kein Instrument der Überwachung von Mitarbeiterinnen und Mitarbeitern im täglichen Betrieb. Ein Missbrauch des Systems für diesen Zweck ist durch technische Mittel wie unten beschrieben auszuschließen.

I. Abschnitt: GELTUNGSBEREICH UND GEGENSTAND

§ 1. Geltungsbereich und Gegenstand

(1) sachlich

Die Vereinbarung regelt die Verwendung und Speicherung von personenbezogenen Daten in allen elektronischen Schließsystemen und Zutrittskontrollsystemen der Universität Graz. Der Begriff elektronisches Schließsystem und der zeitgemäße Begriff computerunterstütztes Zutrittskontrollsystem wird im Folgenden synonym verwendet und mit dem Begriff elektronisches Schließsystem bezeichnet.

(2) persönlich

Die Vereinbarung gilt für alle Personen, die in einem Beschäftigungsverhältnis zur Universität Graz stehen.

(3) örtlich

Die Vereinbarung gilt für alle baulichen Einrichtungen und Areale der Universität Graz, in denen derartige Systeme zur Anwendung kommen.

(4) zeitlich

Die Betriebsvereinbarung tritt mit Ablauf des Tages ihrer Verlautbarung im Mitteilungsblatt in Kraft. Die Betriebsvereinbarung gilt auf unbestimmte Zeit. Sie kann jedoch gem. § 96 Abs. 2 ArbVG von beiden Vertragsparteien jederzeit schriftlich gekündigt werden.

II. Abschnitt: BESCHREIBUNG DER SYSTEME

§ 2. Systemdarstellung

Im Anhang 1 sind die folgenden Daten des jeweiligen elektronischen Schließsystems zu beschreiben:

a) Software

aa) Welches Programmpaket in welcher Version und von welchem Hersteller kommt zum Einsatz

ab) Rollen- und Rechtebeschreibung der beteiligten Personen

ac) Der Umfang und die Art der aus dem führenden System (z. B. SAP, CampusOnline) bezogenen Daten

ad) Ein vollständiges Verzeichnis aller verwendeten Dateien der eingesetzten Software inklusive ihrer Größe und des Erstellungs- bzw. Änderungsdatums zum Zeitpunkt der Übergabe.

b) Hardware

Die verwendete Serverhardware (Steuerrechner), inklusive eines eventuell angeschlossenen Datenspeichers (NAS, SAN, etc.) und das Backupsystem wird im Detail beschrieben. Ebenso der Typ, der Hersteller und die Anbindung der Zutrittserfassungsterminals an den Steuerrechner.

c) Standorte

Die Standorte des Servers, des Backupsystems, der Zutrittserfassungsterminals sind umfassend und vollständig zu beschreiben.

d) Zugangsmittel (Token)

In den wesentlichen Merkmalen zu beschreiben sind

- da) der Typ (Karte, Schlüssel, usw.) des Tokens
- db) die Funktionsweise des Tokens (z.B kontaktlos, Lesegerät, usw.)
- dc) die Daten, die auf dem Token gespeichert sind

§ 3. Systemeinsatz

(1) **Zuständigkeit und Verantwortung:** Im Auftrag der Dienstgeberin betreibt der ZID (Zentraler Informatikdienst) alle zentralen elektronischen Schließsysteme der Universität Graz.

(2) Auch bestehende dezentrale elektronische Schließsysteme werden unter der Anleitung des ZID betrieben. Der operative Betrieb dieser Anlagen sowie die Verwaltung von Zugangsberechtigungen erfolgt durch Personen der dezentralen Einheiten.

(3) Der Auftrag zum operativen Betrieb eines elektronischen Schließsystems erfolgt durch den Leiter/die Leiterin der betroffenen Organisationseinheit in schriftlicher Form. Die beauftragten Personen der dezentralen Einheiten haben in der Regel keinen Zugriff auf personenbezogene Daten. Ist dieser aus technischen Gründen unvermeidlich, so ist den beauftragten Personen gegenüber durch die vorgesetzte Dienststelle schriftlich absolute Verschwiegenheit bezüglich dieser Daten anzuordnen.

(4) Alle neuen oder geplanten elektronischen Schließsysteme sind ausschließlich unter der Anleitung des ZIDs einzuführen.

(5) **Administration:** Die Administration des elektronischen Schließsystems ist personell von der Ausgabe der Token zu trennen.

(6) Zur Administration einer elektronischen Schließanlage müssen mindestens drei Personen eingeschult werden. Die Reihenfolge der Vertretungen ist im Anhang 2 festzuhalten. Die Angaben zu den Administrator/inn/en im Anhang 2 müssen bei Änderungen aktuell gehalten werden.

(7) Vom Rektor ist eine Person mit der Supervision der Systemsicherheit der elektronischen Schließsysteme zu beauftragen. Die Aufgabe dieser Person ist es, die Betriebssicherheit der elektronischen Schließsysteme im Hinblick auf Schutz vor Fremdeingriffen, Virenbefall oder ähnlichem zu gewährleisten. Diese Person erhält jederzeit Zugang zu allen elektronischen Schließanlagen der Universität Graz und ist in deren Administration einzuschulen. Die beauftragte Person hat in der Regel keinen Zugriff auf personenbezogene Daten. Ist dieser aus technischen Gründen unvermeidlich, so ist der beauftragten Person gegenüber durch den Rektor schriftlich absolute Verschwiegenheit bezüglich dieser Daten anzuordnen.

(8) **Betrieb:** Der Token ist vom/von der Arbeitnehmer/in persönlich aufzubewahren. Ein Verlust des Token ist unverzüglich mitzuteilen. Der/die Arbeitnehmer/in erhält dann Ersatz. Um bei Verlust eine missbräuchliche Verwendung auszuschließen, wird der Token im elektronischen Schließsystem für ungültig erklärt und gesperrt. Bei Ausscheiden aus dem Arbeitsverhältnis ist der Token zurückzugeben.

III. Abschnitt: DATENVERWENDUNG

§ 4.

(1) Beim Öffnen der Türen durch Arbeitnehmer/inn/en, werden Türnummer, Datum, Uhrzeit und Personalnummer erfasst und an den Steuerrechner übermittelt.

(2) Das führende System ist UniGraz-Online. Daraus werden nur folgende personenbezogenen Stammdaten bezogen und verarbeitet:

- a) Zugehörigkeit zur Organisationseinheit
- b) Vor- und Zuname
- c) Personalnummer
- d) Ausweisnummer, Ausweiskennziffer

(3) Im elektronischen Schließsystem werden nur folgende universitätsbezogene Stammdaten verarbeitet:

- a) Jahreskalender
- b) Raum-Zeitzone
- c) Tür-Beschreibungen

(4) Die an den Zutrittserfassungsterminals erfassten Daten werden laufend an den Steuerrechner übermittelt.

(5) Logdaten, die keine personenbezogenen Daten enthalten, dürfen ausschließlich lokal und zur Auffindung bzw. Korrektur von Fehlfunktionen der Anlage durch die Administrator/inn/en verwendet werden.

(6) Logdaten, die personenbezogene Daten enthalten, dürfen ausschließlich lokal und zur Auffindung bzw. Korrektur von Fehlfunktionen der Anlage, sowie bei begründetem Verdacht einer gerichtlich strafbaren oder Schadenersatz begründenden Handlung ausgewertet werden. Eine solche Auswertung ist von dem/r Rektor/in nach Zustimmung der Betriebsräte anzuordnen. Sie hat unter Beiziehung einer von den Betriebsräten entsandten Person sowie der/des Datenschutzbeauftragten gemäß Betriebsvereinbarung PDVS zu erfolgen. Die Teilnahme von den Betriebsräten entsandten Personen ist nicht erforderlich, wenn die Betriebsräte schriftlich oder per elektronischem Brief auf eine Entsendung verzichtet haben.

(7) Die im vorherigen Absatz genannten Logdaten dürfen auch ausgewertet werden, wenn die/der betroffene Arbeitnehmer/in dies selbst begehrt, um die Logdaten als Beweismittel zur Sicherung seiner/ihrer Rechte zu verwenden. Dabei sind die Betriebsräte beizuziehen.

(8) Weitere Auswertungen oder Verarbeitungen finden nicht statt, insbesondere sind jegliche Anzeigen von Personenbewegungsdaten unzulässig.

§ 5. Datenfluss

Die gespeicherten Daten aus dem elektronischen Schließsystem dürfen nicht mehr an das führende System (z. B. SAP, UNIGRAZonline) zurück geschrieben werden.

§ 6. Löschregelung

(1) Unbeschadet anderer rechtlicher Vorschriften sind alle im Zusammenhang mit dieser Vereinbarung ermittelten bzw. damit berechneten Daten zu löschen, sobald ihre Speicherung zu einem im Sinne dieser Vereinbarung festgelegten Zweck nicht mehr erforderlich ist. Die Löschung hat jedenfalls spätestens 8 Kalenderwochen nach Ermittlung der Daten zu erfolgen.

(2) Die Löschroutinen sind so zu programmieren, dass die Daten automatisch in regelmäßigen Abständen gelöscht werden.

(3) Die Administrator/inn/en stellen sicher, dass auch eventuelle Sicherungen (Backups) innerhalb des obengenannten Zeitraumes gelöscht sind.

(4) Am Ende der Lebensdauer des jeweiligen elektronischen Schließsystems ist von den Administrator/inn/en dafür Sorge zu tragen, dass alle personenbezogenen Daten nachweislich und unwiederbringlich zerstört werden.

§ 7. Zugriffsberechtigungen

Der Zugriff auf die entsprechenden Funktionen wird auf das Personal begrenzt, das für die Wartung der Hard- und Software zuständig ist. Diese Personen sind an die Bestimmungen des Datenschutzes gebunden und dürfen keine dieser Betriebsvereinbarung widersprechenden Weisungen entgegennehmen. Dies bestätigen sie durch ihre Unterschrift in Anhang 2 dieser Betriebsvereinbarung.

§ 8. Datentransfer

Ausgaben bzw. Auslagerungen von Daten auf externe Speichermedien bzw. eine Übertragung oder Überlassung (on-line oder in anderer Form) an andere EDV-Systeme ist nicht zulässig. Die Herstellung einer mittelbaren oder unmittelbaren Schnittstelle zum Datenexport in Richtung Betriebsdatenerfassungssystem, Personalverwaltungs- bzw. Personalinformationssystem, Zeiterfassungssystem ist nicht zulässig.

IV. Abschnitt: INFORMATIONS-, MITWIRKUNGS- UND KONTROLLRECHTE DER BETRIEBSRÄTE

§ 9.

(1) Die Betriebsräte haben das Recht, sämtliche elektronischen Schließsysteme der Karl-Franzens-Universität, insbesondere die einzelnen Hard- und Softwarekomponenten, jederzeit daraufhin zu prüfen, ob diese der Betriebsvereinbarung entsprechen.

(2) Zur Klärung (programm)technischer Fragen haben die Betriebsräte das Recht, hausinterne fachkompetente Mitarbeiterinnen und Mitarbeiter 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 zu tragen, sofern die Grundsätze der Angemessenheit sowie der Verhältnismäßigkeit gewahrt bleiben.

(3) Die Arbeitgeberin hat den Betriebsausschuss über allgemeine interne Aus-, Fortbildungs- und sonstige Schulungsmaßnahmen betreffend die eingesetzten elektronischen Schließsysteme zu informieren. Zwei Mitglieder der Betriebsräte sind jeweils berechtigt, an den internen Schulungen kostenlos teilzunehmen.

(4) Im Fall geplanter Änderungen und Ergänzungen der elektronischen Schließsysteme sind die Bestimmungen des § 109 ArbVG, insbesondere auch § 109 Abs. 1a ArbVG, sinngemäß anzuwenden.

(5) Für jede Neuerrichtung eines elektronischen Schließsystems oder die Veränderung bestehender elektronischer Schließsysteme, ausgenommen Austausch defekter Hard- und Software durch funktionsgleiche Komponenten, ist eine Änderung der gegenständlichen Betriebsvereinbarung erforderlich.

V. Abschnitt: SCHLUSSBESTIMMUNGEN

§ 10.

(1) Die Betriebsvereinbarung über die Ermittlung, Verwendung und Übermittlung von ArbeitnehmerInnendaten, verlautbart im Mitteilungsblatt vom 16.4.2008, 28.a Stück, 14. Sondernummer, in der jeweils geltenden Fassung, sowie die datenschutzrechtlichen gesetzlichen Erfordernisse bleiben hiervon unberührt.

(2) Die im Anhang dieser Betriebsvereinbarung beigefügten Unterlagen sind untrennbarer Bestandteil der vorliegenden Betriebsvereinbarung.

(3) Diese Betriebsvereinbarung ist ohne ihre Anhänge im Mitteilungsblatt der Universität zu publizieren.

Graz, am

Rektor der Karl-Franzens-Universität Graz

Univ.-Prof.Mag.Dr.Alfred Gutschelhofer eh.

Für den Betriebsausschuss

Univ.-Prof.MMag.DDr.Günther Löschnigg

Für den Betriebsrat für das Allgemeine Universitätspersonal

Regina Lammer eh.

Für den Betriebsrat für das Wissenschaftliche Universitätspersonal

Ao. Univ.-Prof. Dr. Ingo H. Kropač eh.

ANHANG 1 – SYSTEMDARSTELLUNG

ANHANG 2 – EINHALTUNG DER BESTIMMUNGEN DER BV

[Bezeichnung des elektronischen Schließsystems]

Ich bestätige, dass mir der Inhalt der Betriebsvereinbarung über die Einführung und Verwendung elektronischer Schließsysteme an der Universität Graz bekannt ist und bekenne mich mit meiner Unterschrift zu deren Einhaltung.

Bezeichnung	Vollständiger Name	Unterschrift
1. Administrator/in		
2. Administrator/in		
3. Administrator/in		
Sicherheitsbeauftragte/r		

[Bezeichnung des elektronischen Schließsystems]

Ich bestätige, dass mir der Inhalt der Betriebsvereinbarung über die Einführung und Verwendung elektronischer Schließsysteme an der Universität Graz bekannt ist und bekenne mich mit meiner Unterschrift zu deren Einhaltung.

Bezeichnung	Vollständiger Name	Unterschrift
4. Administrator/in		
5. Administrator/in		
6. Administrator/in		
Sicherheitsbeauftragte/r		

[Bezeichnung des elektronischen Schließsystems]

Ich bestätige, dass mir der Inhalt der Betriebsvereinbarung über die Einführung und Verwendung elektronischer Schließsysteme an der Universität Graz bekannt ist und bekenne mich mit meiner Unterschrift zu deren Einhaltung.

Bezeichnung	Vollständiger Name	Unterschrift
7. Administrator/in		
8. Administrator/in		
9. Administrator/in		
Sicherheitsbeauftragte/r		