1. ÄNDERUNG DER BETRIEBSVEREINBARUNG ÜBER ELEKTRONISCHE ZUTRITTSSYSTEME

Die **WU (Wirtschaftsuniversität Wien),** Welthandelsplatz 1, 1020 Wien, (im Folgenden auch „Arbeitgeberin" genannt), vertreten durch die Rektorin Univ.-Prof. Dr. Edeltraud Hanappi-Egger, diese wiederum vertreten durch den Vizerektor für Personal Univ.-Prof. Dr. DDr.h.c. Michael Lang,

und

der **Betriebsrat für das wissenschaftliche Universitätspersonal** der WU und der **Betriebsrat für das allgemeine Universitätspersonal** der WU, Welthandelsplatz 1, 1020 Wien, (im Folgenden zusammen „ die Betriebsräte" genannt)

schließen gem. §§ 96 Abs 1 Z 3 und 96a Abs 1 Z 1 ArbVG in der geltenden Fassung folgende Betriebsvereinbarung hinsichtlich der elektronischen Zutrittssysteme an der WU ab.

Aufgrund des Inkrattretens der DSGVO mit 25.05.2018 werden Anpassungen an den Text der Betriebsvereinbarung vorgenommen. Der Name einer maßgeblich beteiligten Abteilung hat sich seit dem Inkrafttreten der Betriebsvereinbarung geändert, was ebenfalls angepasst wird.

Präambel

1. Auf Basis der gesetzlichen Normen soll diese Betriebsvereinbarung die Nutzung und den Umgang mit den durch die Verwendung des elektronischen Zutrittssystems ermittelten Daten regeln.

2. Die Mitarbeiter/innen sollen vor missbräuchlicher Verwendung personenbezogener Daten, insbesondere einer missbräuchlichen Überwachung ihres Verhaltens und eines missbräuchlichen Zugriffs auf ihre Daten geschützt werden. Die Betriebsvereinbarung dient dazu die Umsetzung von rechtlichen Bestimmungen zur Verhinderung des Datenmissbrauchs zu unterstützen.

3. Mit dem Betrieb des Zutrittsystems dürfen keine arbeitsrechtlichen Kontrollen, insbesondere keine Arbeitszeiterfassungen, der Mitarbeiter/innen durchgeführt werden. Die gespeicherten Daten dürfen daher ausschließlich zur Sicherung von Beweisen im Rahmen von Ermittlungen aufgrund begründeter Verdachtsfälle auf strafbare Handlungen sowie bei Gefahr für Leib und Leben verwendet werden. Die Erstellung von Bewegungsprofilen bzw. eine Verknüpfung mit anderen Systemen zur Erstellung von Bewegungsprofilen ist nicht zulässig.

4. Die WU erklärt, dass sie personenbezogene MitarbeiterInnendaten nur im gesetzlich erlaubten und betrieblich unbedingt notwendigen Ausmaß verarbeitet und an Dritte übermittelt.

5. Die WU erklärt, dass in keinem Fall eine Verknüpfung mit anderen Systemen (wie z.B. Videoüberwachung) stattfindet.

I. Geltungsbereich

1. Persönlich und örtlich

Diese Betriebsvereinbarung gilt für alle Mitarbeiter/innen der WU (Arbeitnehmer/innen einschließlich der auf die WU übergeleiteten Vertragsbediensteten des Bundes sowie der Beamt/inn/en des Bundes, die der WU zur Dienstleistung zugewiesen sind) und für alle im Wege der Arbeitskräfteüberlassung der WU für länger als 6 Monate zur Arbeitsleistung überlassenen Arbeitskräfte, die von der WU mit einem elektronischen Schlüssel ausgestattet wurden, um bestimmte Räumlichkeiten der WU über ein elektronisches Zutrittssystem betreten zu können (in der Folge: Mitarbeiter/innen). Nicht vom Anwendungsbereich erfasst sind Studierende sowie externe Personen (z.B. Werkvertragsnehmer/innen, Reinigungspersonal, Lieferant/inn/en), die ebenfalls über eine Berechtigung zur Benützung des elektronischen Zutrittssystems an der WU verfügen.

Diese Betriebsvereinbarung gilt für alle Standorte der WU.

2. Zeitlich

Die geänderte Fassung der Betriebsvereinbarung tritt am 25.05.2018 in Kraft und kann von jeder Vertragspartei unter Einhaltung einer 6-wöchigen Kündigungsfrist aufgekündigt werden.

3. Sachlich

Diese Vereinbarung regelt die Erhebung und Auswertung personenbezogener Daten, die bei der Nutzung der elektronischen Zutrittssyteme anfallen. Erlaubt ist nur die in der BV ausdrücklich geregelte Erhebung personenbezogener Daten. Vom Geltungsbereich dieser Betriebsvereinbarung sind Mitarbeiter/innen/räume, Instituts- und Departmenträumlichkeiten, Bibliotheksräumlichkeiten sowie Hörsäle und Seminarräume, technische Räume, Lagerräume, Systemräume, Archivräume und Druckerräume erfasst. Nicht unter den Geltungsbereich der Betriebsvereinbarung fallen Räume, die ausschließlich von Dritten genutzt werden (z.B. Räume des Reinigungspersonals).

II. 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, die Kartennummer und die Operation (dh

Türöffnung) erfasst.

Auswertungslogfiles sind Protokolldaten, die durch spezielle Zugriffe auf die Zutrittslogfiles entstehen. Bei Auswertungslogfiles werden folgende Daten erfasst: Datum und Uhrzeit, Kartennummer, Name der einsichtnehmenden Person und Grund der Auswertung (Meldungstext).

Für diese beiden Arten von Logfiles sind unterschiedliche Speicherungs- und Löschungsvorschriften vorgesehen (siehe Punkt VII.3.)

2. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (die betroffene Person) beziehen (Art 4 Z 1 DSG-VO).

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. Evaluierungsleser sind spezielle Geräte, die Berechtigungsdaten für OFFLINE-Türen auf Zutrittsmedien übertragen.

4. Revisionssichere Speicherung nach dem jeweiligen Stand der Technik bedeutet, dass alle Daten unveränderbar, unüberschreibbar und jederzeit wieder abrufbar gespeichert werden.

III. Zweck des elektronischen Zutrittssystems

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

2. Die Installierung und der Betrieb des elektronischen Zutrittssystems soll gewährleisten, dass ständig bzw zu bestimmten Zeiten nur autorisierte Personen Zugang zu den Räumlichkeiten der WU haben. Das elektronische Zutrittssystem dient als „Schlüsselersatz" zum Betreten der Räumlichkeiten der WU (Näheres zum elektronischen Schlüssel unter Punkt IV).

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

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

IV. Funktions- und Systembeschreibung

1. Bei diesem Zutrittssystem handelt es sich um ein zweiteiliges System, das aus einem anonymisierten und einem führenden System besteht, in denen Daten verarbeitet werden. Im führenden System finden sich die Personaldaten, wie z.B. die Personalnummer, und im anonymisierten System werden die Zutrittsdaten erfasst. Die Zuordnung zu einer Person ist erst durch eine Verknüpfung dieser beiden Systeme zulässig, was aber nur unter den in Pkt VII beschriebenen Voraussetzungen zulässig ist.

2. Das konzipierte Zutrittssystem setzt sich aus zwei Produktpaletten (ATS - online, SALTO - offline) zusammen. Dieses bzw. die Türlesesysteme (Online-System, Online Evaluierungsleser, Offline-System Funk, Offline System) werden in der technischen Systembeschreibung in Anlage ./A näher beschrieben.
3. Die Systembetreuer/innen haben nur auf die anonymisierten Daten Zugriff. Auf die Daten des führenden Systems darf nur im Rahmen von Ermittlungen aufgrund begründeter Verdachtsfälle auf strafbare Handlungen nach Zustimmung des Betriebsrates zugegriffen werden (Näheres unter Punkt VII.5. und IX).

Einmal pro Jahr kann zur technischen Überprüfung des Zutrittssystems unter Beisein der Betriebsräte die Wartungsfirma die Daten des anonymisierten und des führenden Systems zusammenführen.

4. Das von der WU 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 Organisationseinheiten und den einzelnen Räumen ermöglichen kann. Dieses Zonenkonzept gewährleistet, dass ausschließlich dafür Berechtigte Zugang zum Gebäude, zu den Organisationseinheiten und zu einzelnen Räumen haben (Näheres unter Punkt VI).

5. Das an der WU verwendete elektronische Zutrittssystem wird in der Systembeschreibung in Anlage ./A hinsichtlich folgender Punkte näher beschrieben:

1. Produktdarstellung, Türgruppen und Türlesesysteme
2. Systembeschreibung
3. Verwaltung des Zutrittssystems
4. Aktivierungsmerkmale

6. Die Mitarbeiter/innen erhalten von der Personalabteilung gegen Unterschrift 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 Mitarbeiter/in den Zutritt zu allen Räumen, zu denen ihm/ihr eine Zutrittsberechtigung eingeräumt wurde.

7. Die maximale Empfindlichkeitsdistanz des elektronischen Schlüssels ist 20cm.

8. Bei Änderung des Arbeitsplatzes und/oder der Zuständigkeit eines Mitarbeiters/einer Mitarbeiterin erhält der/die Mitarbeiter/in entweder einen neuen elektronischen Schlüssel (gegen Retournierung des alten elektronischen Schlüssels) oder wird die Codierung seines/ihres elektronischen Schlüssels vom Sicherheitsmanagement geändert.

Scheidet ein/e Mitarbeiter/in aus dem Geltungsbereich dieser Betriebsvereinbarung aus, ist der elektronische Schlüssel unverzüglich der Personalabteilung zu übergeben. Die Rückgabe des elektronischen Schlüssels ist schriftlich zu dokumentieren.

Bei Beschädigung oder Bruch des elektronischen Schlüssels ist die Personalabteilung unverzüglich in Kenntnis zu setzen.

Ein Verlust des elektronischen Schlüssels ist sofort bei der Abteilung Sicherheitsmanagement und/oder bei der WU-Sicherheitszentrale zu melden, damit der elektronische Schlüssel gesperrt werden kann. Die WU hat zu diesem Zweck eine Telefonnummer und eine Mailadresse der WU-Sicherheitszentrale (24-Stunden Sicherheitsdienst) bekannt zu geben. sicherheitsdienst@wu.ac.at, DW: 4000. 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.

Die Neuausstellung des elektronischen Schlüssels (bei Verlust oder Beschädigung/Bruch) erfolgt durch das Sicherheitsmanagement.

9. Die WU hat das Recht, das verwendete System stets auf dem aktuellen Stand der Technik zu halten, soweit sich aus dem Folgenden nichts Anderes ergibt. Änderungen, insbesondere Software-Versionswechsel des Zutrittssystems sind umgehend an die Betriebsräte zu melden. Kommt es dabei zu einer wesentlichen Funktionsänderung des Systems, ist die Zustimmung der Betriebsräte vor Ein- bzw Durchführung der Systemänderung einzuholen und ist die Anlage ./A und die BV entsprechend abzuändern.
Eine wesentliche Änderung eines Systems ist gegeben, wenn durch sie z.B.

- zusätzliche personenbezogene Daten erhoben, gespeichert und verarbeitet werden
- jede weitere Aktivierung von Funktionsmerkmalen (siehe dazu Anlage ./A 4) mit denen personenbezogene Daten verarbeitet werden
- der Kreis der Zugriffsberechtigten erweitert wird oder
- neue personenbezogene Auswertungen ermöglicht werden.

Beispiele für wesentliche Änderungen sind die Ausstattung der Türgruppen mit anderen Türlesesystemen, die Änderung oder Neueinführung von wesentlichen Funktionen des Zutrittssystems wie die Änderung der Empfindlichkeitsdistanz der Lesegeräte.

Den Betriebsräten wird monatlich ein Bericht übermittelt, der alle durchgeführten Änderungen bzw. Neueinführungen von Systemen, die personenbezogene Daten verarbeiten, in verständlicher und knapper Form wiedergibt.

10. Die Betriebsräte haben jederzeit das Recht zu überprüfen, ob das aktuelle System noch mit dem in dieser Betriebsvereinbarung beschriebenen übereinstimmt und sich Systemänderungen auf Wunsch von Mitarbeiter/inne/n der Einrichtung Sicherheitsmanagement erklären zu lassen.

V. Standorte der elektronischen Zutrittssysteme

Alle Räumlichkeiten und Server-Schränke an den Standorten der WU (abgesehen von Schächten, einigen technischen Räumen und den WC-Türen sowie Duschen der Mitarbeiter/innen in nicht jederzeit öffentlich zugänglichen Bereichen) sind mit einem elektronischen Zutrittssystem ausgestattet.

VI. Zutrittsberechtigungen und Zonenkonzept

Die WU erstellt bis 01.10.2013 ein Zonenkonzept, in dem geregelt ist, welche Personen zu welchen Räumen der WU Zugang haben. Dieses Gesamtkonzept wird im Intranet der WU unter https://swa.wu.ac.at/richtl/Lists/Richtlinien/DispForm.aspx?ID=342&ContentTypeId=0x0100FB50C36DBBE35B48B128BA24D5DED6B0 veröffentlicht. Änderungen dieses Konzepts werden ebenfalls auf dieser WU-Intranetseite veröffentlicht und die Änderungen werden den Betriebsräten und den Arbeitnehmer/inne/n umgehend mitgeteilt. Änderungen des Zonenkonzepts, die nur einzelne Organisationseinheiten betreffen und nicht für die gesamte WU gelten, sind darüberhinaus jeweils im Sekretariat der jeweiligen Organisationseinheit zur Einsichtnahme aufzulegen.

Interessensvertretungen (wie z.B. Betriebsrat und Arbeitskreis für Gleichbehandlungsfragen) haben das Recht, für die ihnen zugewiesenen Räumlichkeiten die Zutrittsberechtigungen selbst festzulegen, die dann vom/von der Systemadministrator/in umzusetzen sind.

VII. Speicherung und Löschung der Daten

1. Die Zutritte und Zutrittsversuche zu Räumlichkeiten und Server-Schränken an den Standorten der WU werden entsprechend der Produktdarstellung und Systembeschreibung (Anhang ./A) gespeichert.

2. Die Zutrittslogfiles (siehe Punkt II.) werden so gespeichert, dass nur das mit der Wartung des Zutrittssystems betraute Unternehmen, das zuständige Mitglied des Rektorats, der/die mit der (Teil-)Administration des Zutrittssystems betraute Leiter/in des Sicherheitsmanagements bzw. der Network Infrastructure und deren Stellvertreter/innen nach Zustimmung der Betriebsräte darauf Zugriff haben. Diese Personen sind funktionsbezogen in Anlage ./B aufgezählt. Die Berechtigungen dieser Personen und deren Änderungen werden den Betriebsräten bekanntgegeben.
Zu den Auswertungslogfiles siehe XI.

3. Alle im Zusammenhang mit den Zutrittssystemen ermittelten Daten (Zutrittlogfiles) werden für einen Zeitraum von höchstens 12 Tagen zu Zwecken der Nachvollziehbarkeit im Rahmen von Fällen nach Punkt IX. dieser Betriebsvereinbarung gespeichert. Spätestens mit Ablauf dieser Frist werden die Daten gelöscht. Alle Auswertungslogfiles werden für einen Zeitraum von drei Jahren zu Zwecken der Nachvollziehbarkeit im Sinn der Revisionssicherheit gespeichert.

4. Alle durch das Zutrittssystem ermittelten Daten müssen nachvollziehbar und nach dem jeweiligen Stand der Technik revisionssicher gespeichert werden.

5. Die Verknüpfung des anonymisierenden und des leitenden Systems darf nur in folgenden Fällen erstellt werden:

a. im Rahmen von Ermittlungen aufgrund begründeter Verdachtsfälle auf strafbare Handlungen,
b. bei Gefahr für Leib und Leben

Im Rahmen von Ermittlungen aufgrund begründeter Verdachtsfälle auf strafbare Handlungen (lit a) dürfen die Daten des anonymisierten und des führenden Systems, nur unter den in den Punkten VII und IX genannten Kriterien, zusammengeführt werden.

Bei technischen Überprüfungen des Systems dürfen die Daten des anonymisierten und des führenden Systems, nur wie unter Punkt IV.3. erläutert, verwendet werden.
Bei technischen, behördlichen bzw. arbeitnehmer/innen/schutzrelevanten Überprüfungen sowie Evaluierungen von Arbeitnehmer/innen/schutzmaßnahmen dürfen die Daten des anonymisierten und des führenden Systems nicht zusammengeführt werden. Die anonymisierten Daten dürfen aber soweit erforderlich zu folgenden Zwecken verwendet werden:

c. für die technische Überprüfung des Systems,
d. bei behördlichen Überprüfungen,
e. im Zusammenhang mit arbeitnehmer/innen/schutzrelevanten Überprüfungen,
f. zur Evaluierung von Arbeitnehmer/innen/schutzmaßnahmen,

VIII. Transparenz

1. Die betroffenen Mitarbeiter/innen der WU sind über die Tatsache der Aufzeichnung ihrer personenbezogenen Daten im Zusammenhang mit dem elektronischen Zutrittssystem sowie über den Inhalt dieser Betriebsvereinbarung durch deren Veröffentlichung im Intranet unter http://www.wu.ac.at/intranet/einrichtungen/personal/recht/betriebsvereinbarungen der WU zu informieren.
2. Den Betriebsräten ist auf ihr Verlangen in die entsprechende Programmdokumentation Einsicht zu gewähren. Zusätzlich haben die Betriebsräte jederzeit die Möglichkeit, sich das System vom/von der Leiter/in des Sicherheitssmanagements oder in seiner/ihrer Abwesenheit von seinem/ihrem Stellvertreter bzw. seiner/ihrer Stellvertreterin erläutern zu lassen.

IX. Einsichtnahme und Auswertung

1. Einsichtnahmen in die Zutrittslogfiles sowie personenbezogene Auswertungen der Daten aus dem elektronischen Zutrittssystem dürfen nach Zustimmung der Betriebsräte durch das zuständige Mitglied des Rektorats, den/die Leiter/in des Sicherheitsmanagements oder deren Stellvertreter/innen im Beisein je eines Vertreters/einer Vertreterin der Betriebsräte ausschließlich im Rahmen von Ermittlungen aufgrund begründeter Verdachtsfälle auf strafbare Handlungen vorgenommen werden.

2. Das zuständige Mitglied des Rektorats, der/die Leiter/in des Sicherheitsmanagements oder deren Stellvertreter/innen sind verpflichtet, den Betriebsräten eine beabsichtigte Einsichtnahme in die Protokolle ehestmöglich mitzuteilen und den begründeten Verdacht auf strafbare Handlungen darzulegen. Die Betriebsräte haben zwei Arbeitstage Zeit darüber zu entscheiden, ob sie ein Vetorecht einlegen, und der WU ihre Entscheidung schriftlich bzw. per Mail mitzuteilen. Wird Veto eingelegt, ist eine Einsichtnahme nicht zulässig.
Auf Verlangen der Betriebsräte haben die oben genannten, zuständigen Funktionsträger/innen 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 WU für die Dauer der Ermittlungen bzw. des Verfahrens länger als in den in Punkt VII.2. genannten Fristen aufbewahrt werden. In diesem Fall wird ein Datenexport im Beisein der Betriebsräte vorgenommen.
Die Aufbewahrung solcher Zutritts- und Auswertungsdaten bei Ermittlungen bzw. Verdachtsfällen auf strafbare Handlungen muss gesondert protokolliert werden.
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.

4. Abgesehen von den Fällen nach Punkt VII.5. bzw. IX ist die Einsichtnahme in die Protokolle grundsätzlich nur in das anonymisierte System (Ausnahme 1x im Jahr, siehe Punkt IV.3.) gestattet.

X. Gefahr für Leib und Leben

1. Das zuständige Mitglied des Rektorats und der/die Leiter/in des Sicherheitsmanagement bzw. die Stellvertreter/innen dürfen abgesehen von den in Punkt IX näher erläuterten Verfahren nur zur Abwehr einer konkreten Gefahr für Leib, Leben oder Gesundheit von Menschen in die Protokolle des elektronischen Zutrittssystems Einsicht nehmen und personenbezogene Auswertungen vornehmen.

2. Gefahr für Leib und Leben liegt vor, wenn eine konkrete Gefährdung für Leib, Leben oder Gesundheit eines Menschen gegeben ist und die drohende Gefahr durch die Einsichtnahme in die Protokolle bzw. die Auswertung der personenbezogenen Daten abgewendet werden kann (z.B. im Falle eines Brandes, eines Amoklaufs, bei Unwettern, Bombendrohungen, udgl.).

3. Bei Gefahr für Leib und Leben können das zuständige Mitglied des Rektorats und der/die Leiter/in des Sicherheitsmanagements bzw. ihre Stellvertreter/innen die geeigneten Maßnahmen (Einsichtnahme in die Protokolle, Auswertung der personenbezogenen Daten) zum Schutz von Leib, Leben und Gesundheit von Menschen unter gleichzeitiger Verständigung der Betriebsräte unverzüglich durchführen. Ist Gefahr für Leib und Leben gegeben und sind die Betriebsräte nicht sofort erreichbar, so genügt die nachträgliche, unverzügliche Verständigung über diese Maßnahmen.

4. Grundsätzlich sind die Betriebsräte auch in diesen Fällen unverzüglich zu verständigen und zur Einsichtnahme beizuziehen. Ist dies nicht möglich, erfolgt die nachträgliche Verständigung schriftlich bzw. per Mail und hat den Namen der einsichtnehmenden Person, Datum und Uhrzeit der Einsichtnahme, Aufzählung der Türen, in die Einsicht genommen wurde, die Benennung des Anlassesfalles und den Grund für die Einsichtnahme zu enthalten.

XI. Protokollierung

1. Jede Einsichtnahme in die Zutrittslogfiles oder Auswertung der Zutritte ist in einem Protokoll unter Angabe der Namen der einsichtnehmenden 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. Das Zutrittssystem protokolliert nur Zutrittsdaten, nicht aber Austrittsdaten.

3. Näheres zu den Zutritts- und Auswertungslogfiles bzw. den Protokolldaten findet sich unter Punkt II.

XII. Datenschutz

1. Personenbezogene Arbeitnehmer/innen/daten dürfen von der WU nur im Rahmen der einschlägigen Gesetze und dieser Betriebsvereinbarung (inkl. ihrer Anlagen) verwendet und an Dritte weitergegeben werden.

2. Die WU hat für die Vertraulichkeit der ermittelten personenbezogenen Daten im Sinne der datenschutzrechtlichen Bestimmungen zu sorgen. Mitarbeiter/innen, die Zugang zu den aufgezeichneten 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.

3. Ausdrücklich festgehalten wird, dass die WU verpflichtet ist, überall dort Datensicherheitsmaßnahmen zu ergreifen, wo Zugang zu personenbezogenen Daten besteht. Die WU hat dabei dafür Sorge zu tragen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt werden, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

XIII. Sonstiges

1. Abänderungen dieser Betriebsvereinbarung können im Einvernehmen zwischen allen Parteien ausschließlich in schriftlicher Form erfolgen.

2. Streitigkeiten aus und im Zusammenhang mit dieser Betriebsvereinbarung sind vor dem Arbeits- und Sozialgericht Wien auszutragen.

3. Die Betriebsvereinbarung für Operative Systeme kommt ab dem Inkrafttreten dieser Betriebsvereinbarung auf das Zutrittssystem der WU nicht mehr zur Anwendung. Die bisherige BV Zutritt wird durch die vorliegende BV gänzlich ersetzt.

Anlage ./A

Funktionsbeschreibung

1. Produktdarstellung, Türgruppen, Türlesesysteme

In der folgenden Tabelle wird dargestellt mit welchen Türlesersystemen und welcher Software das elektronische Zutrittssystem an der WU arbeitet. Des Weiteren wird aufgezählt, welche Türgruppen an der WU mit welchen Türlesersystemen ausgestattet sind. Zur Speicherung von Daten siehe Punkt VII.

Türlesesysteme	Software	Verwaltet über	Türen
Online-System	ATS	ATS	Hauptzugangstüren Baufeld/Objekt, Bereichszugangstüren/ Departmenttüren, Technikräume mit hoher Sicherheitsanforderung
ONLINE Evaluierungsleser	ATS	ATS	(situiert in den Zugangsbereichen oder als ONLINE-Zutrittsleser)
Funk -System	SALTO	ATS	Hörsäle, Seminarräume, Projekträume
Offline-System	SALTO	ATS	Bürotüren, Mitarbeiter/innen-WC in öffentlichen Bereichen, Technikräume, Archiv, Lehrmittelräume, Reinigungsräume, Lagerräume
Online-Sallis	ATS	ATS	Sitzungssäle AD-Gebäude

2. Systembeschreibung

Die voranstehende Tabelle zeigt die verschiedenen technischen Möglichkeiten zur Auswertung von Zutrittsdaten auf. Die Verknüpfung mit Personendaten (von Mitarbeiter/innen) kann nur nach Maßgabe der Berechtigung(en) erfolgen (siehe IX.). Die Auswertung historischer personenbezogener Zutrittsdaten ist nur nach den Bestimmungen gemäß Punkt IX möglich.

OFFLINE

Die Daten werden im Türbeschlag gespeichert und mit einem PPD (Portable Programming Device)

können Buchungsdaten von einem Beschlag ausgelesen werden. Das tragbare Programmiergerät ist ein Kommunikationsgerät zwischen dem PC und der Schließeinheit. Die ausgelesenen Daten sind verschlüsselt und können erst nach Übertragung vom Lesegerät ins anonymisierte System dargestellt werden.

FUNK

Ist eine Kombination von ONLINE und OFFLINE. Daten des anonymisierten Systems werden per Funk und verschlüsselt an den/die PCs (Clients) weitergeleitet und nach Vorgabe der Regelungen der Betriebsvereinbarung - wie bei ONLINE - behandelt. Weiters ist eine Datenübertragung wie bei OFFLINE möglich.

ONLINE

Die Zutrittsdaten werden online in das anonymisierte System übertragen. Die Bearbeitung, Aktivierung und Deaktivierung von Zutrittsrechten am PC von Online-Türen ist durch berechtigte Personen (siehe dazu Anlage ./B) jederzeit möglich.

3. Verwaltung des Zutrittssystems

Welche Abteilungen sind zur (Teil-)Administration mit dem Zutritt zum anonymisierten System berechtigt:

Systembereiche	Funktion	Zugriffsberechtigte
Gesamtsystem	Systemadministration	Sicherheitsmanagement (SM)
IT-Bereiche	Teiladministration IT	IT Services - Network Infrastructure

4. Aktivierungsmerkmale (Aktivierung mit „X" gekennzeichnet)

In der ersten Spalte dieser Tabelle werden die aktivierten (System-)funktionen des elektronischen Zutrittssystems aufgezählt. In der zweiten Spalte findet man eine Beschreibung der aktivierten Funktionen. Die Aufgabenverteilung zwischen Systemadministrator/inn/en und Teiladministrator/inn/en wird in der dritten und vierten Spalte der Tabelle dargestellt.

Systemfunktionen	**Beschreibung der Funktion**	**System-administration**	**Teiladministration** (nur für deren Bereiche)
Trennung von personenbezogenen Daten und Systemdaten sowie Trennung von internen und externen Personen Verknüpfung von historischen Mitarbeiter/innendaten (nach Maßgabe der Regelungen in VII.)		**X**	
Anlegen und Verwalten von Operatoren mit Verwaltung der Teilbereich-berechtigungen	Operatoren sind Personen, die Zutrittsberechtigungen bearbeiten können	**X**	
Vergabe von Prioritäten und Farben zu Alarm und Meldungstexten	Alarmen können unterschiedliche Prioritätslevel zugeteilt werden und mit farblichen Markierungen hinterlegt werden	**X**	
Anlegen von Onlinetüren	Neue ONLINE-Türen aktivieren	**X**	
Bearbeiten von Onlinetüren	z.B. Bezeichnung bzw. „Namensgebung" einer Türe	**X**	
Anlegen von Offlinetüren		**X**	
Bearbeiten von Offlinetüren		**X**	
Steuerung der Online-Türen über die Software	Türen öffnen, versperren, zeitsteuern	**X**	
Erstellen von Zutrittsbereichen für Onlinetüren		**X**	
Erstellen von Zutrittsbereichen für Offlinetüren		**X**	
Anlegen von Online-Personengruppen		**X**	

Verwalten von Online-Personengruppen	Personengruppen sind frei anlegbar und können beispielsweise Raumpfleger/innen, Sicherheitsdienst oder technischer Dienst sein.	X	X
Anlegen von Offline-Zutrittsebenen		X	
Verwalten von Offline-Zutrittsebenen		X	X
Zutrittsberechtigungs-vergabe individuell pro Online-Personengruppe (bspw. Reinigungspersonal, Studierende) und ohne Einschränkung der unterschiedlichen Berechtigungen für seinen Teilbereich		X	X
Zutrittsberechtigungs-vergabe individuell pro Offline-Zutrittsebene und ohne Einschränkung der unterschiedlichen Berechtigungen		X	X
Anlegen von Personen		X	
Löschen von Personen		X	
Eingabe des Eintritts - Austrittsdatum		X	
Anzeigen der letzten Bewegung bei einer Person (Einschränkung gilt nur für WU-Mitarbeiter/innen-daten)[1]			
Vergabe von temporären Berechtigungen zu einer Person	zeit- oder/und datumsabhängige Berechtigungen		
Ausgabe von Karten		X	X
Kartenmanagement (sperren von Karten sofern diese verloren wurden)		X	X (Sicherheitsdienst)
Freigeben von gesperrten Karten		X	

[1] Keine Berechtigung: Bewegungsprofile können nicht erstellt werden

Listenerstellung wahlweise sortiert nach Kartennummer, Personalnummer, Name oder Abteilung und Name		x	x
Einsicht auf externe Personen (Trennung von personenbezogenen Daten und Systemdaten/ Trennung von internen und externen Personen)		x	x
Einsicht auf Systemdaten (Trennung von personenbezogenen Daten und Systemdaten/ Trennung von WU-Mitarbeiter/innen und externen Personen)		x	x
Geteiltes Grafikbedienfenster mit Alarmtextfenster (der zuständige Teiladministrator/in kann sich seine/ihre gewünschten Alarme und Meldungen anzeigen lassen)	Alarme sind z.B.: Unberechtigt geöffnete Türe(n); Türen, die offen stehen	x	x
Gebäudepläne (Bitmapgrafiken mit dynamischen Symbolen zur Anzeige von Ereignissen, Alarmen und Bewegungen)[2]			

[2] Keine Berechtigung: Bewegungsprofile können nicht erstellt werden

Anlage ./B

Zugriffsberechtigte im Rahmen der Berechtigungen laut Betriebsvereinbarung:

(stv.) Leiter/in des Sicherheitsmanagements
(stv.) Leiter/in der Network Infrastructure
Vizerektor/in für Infrastruktur bzw. Vertreter/in gemäß der Geschäftordnung des Rektorats der WU
Mitarbeiter/innen des Wartungsunternehmens (derzeit Mitarbeiter/innen der Firma Essecca)

Wien, am 18.5.2018

Für die WU:

.....
Univ. – Prof. Dr. DDr.h.c. Michael Lang
Vizerektor für Personal

Für den Betriebsrat für das
allgemeine Universitätspersonal:

.....
FI Friedrich Hess

Für den Betriebsrat für das
wissenschaftliche Universitätspersonal:

.....
ao. Univ.-Prof. Dr. Angelika Schmidt