



**ZUSATZBETRIEBSVEREINBARUNG  
ZUR**

**Rahmenbetriebsvereinbarung betreffend automationsunterstützte Verwendung  
personenbezogener ArbeitnehmerInnendaten**

über die

**Einführung und Verwendung elektronischer MitarbeiterInnenausweise**

abgeschlossen zwischen der

Medizinischen Universität Wien  
als Betriebsinhaber  
vertreten durch den Rektor Univ.-Prof. Dr. Markus Müller

und dem

Betriebsrat für das allgemeine Universitätspersonal der  
Medizinischen Universität Wien  
vertreten durch die Vorsitzende Gabriele Waidringer

sowie dem

Betriebsrat für das wissenschaftliche Universitätspersonal der  
Medizinischen Universität Wien  
vertreten durch den Vorsitzenden Ass. Prof. Dr. Ingwald Strasser

(beide zusammen im Folgenden kurz: „die Betriebsräte“)



### Präambel

1. Sowohl das Allgemeine Krankenhaus der Stadt Wien (AKH) als auch die Medizinische Universität Wien (MedUni Wien) streben die Einführung von MitarbeiterInnenausweisen mit Chipkartenfunktion an, auf Seiten der MedUni Wien wird auch der vorklinische Bereich und der Verwaltungsbereich außerhalb des AKH einbezogen, weshalb die Ausgabe der Ausweise grundsätzlich vom jeweiligen Arbeitgeber erfolgen soll.
2. Ziel ist eine einheitliche technologische Lösung für die MitarbeiterInnenausweise unter Berücksichtigung der Notwendigkeiten von MedUni Wien und AKH und Wahrung der datenschutzrechtlichen und arbeitsrechtlichen Rahmenbedingungen; dabei ist zu unterscheiden zwischen dem Bereich der gemeinsamen Betriebsführung von AKH und MedUni Wien und den anderen Bereichen der MedUni Wien. Im Rahmen der gemeinsamen Betriebsführung von AKH und MedUni Wien werden für eine Übergangsphase die MitarbeiterInnenausweise bis auf weiteres vom AKH im Namen der MedUni Wien erstellt und ausgegeben.

Die jeweils aktuellen Applikationen der in die MitarbeiterInnenausweise integrierten Chips werden in den Anhängen festgelegt.

Der elektronische MitarbeiterInnenausweis und seine Applikationen dürfen nicht dazu verwendet werden eine mittelbare oder unmittelbare Leistungskontrolle oder Zeiterfassung der MitarbeiterInnen vorzunehmen

3. Zwischen AKH und MedUni Wien wird eine Vereinbarung abgeschlossen, in der die zweckgebundene Übermittlung und Verarbeitung der Daten, insbesondere die Datensicherheit geregelt werden. Eine Erweiterung des Personenkreises oder der seitens der MedUni Wien zur Verfügung gestellten personenbezogenen Daten sowie eine Zweckänderung oder Änderung der Funktionalität der Ausweise bedarf einer neuerlichen schriftlichen Vereinbarung der Parteien unter vorheriger Befassung der inneruniversitären Datenschutzkommission und der Betriebsratsgremien der MedUni Wien.
4. Grundlage für diese Zusatzbetriebsvereinbarung sind die Bestimmungen der Rahmenbetriebsvereinbarung betreffend automationsunterstützte Verwendung personenbezogener ArbeitnehmerInnendaten.
5. Diese Zusatzbetriebsvereinbarung regelt die Einführung und Verwendung elektronischer MitarbeiterInnenausweise. Für jede Applikation werden jeweils in einem Anhang detaillierte Regelungen getroffen.

## 1. Geltungsbereich und Rechtsgrundlage

### 1.1 Persönlicher Geltungsbereich:

Diese Zusatzbetriebsvereinbarung gilt für alle MitarbeiterInnen der MedUni Wien (ArbeitnehmerInnen im engeren Sinne einschließlich der von der MedUni Wien übernommenen Vertragsbediensteten des Bundes sowie BeamtInnen des Bundes, die der MedUni Wien zur Dienstleistung zugewiesen sind), die am AKH tätig sind oder dem



Verwaltungsbereich des Rektorats oder einer sonstigen im AKH verorteten Einrichtung der MedUni Wien zugeordnet sind.

### 1.2 Zeitlicher Geltungsbereich

Diese Zusatzbetriebsvereinbarung tritt mit 1. Juli 2018 in Kraft und ist vorerst befristet bis 31.12.2019.

Während dieser Zeit besteht eine Phase der beiderseitigen Prüfung ihrer Anwendbarkeit, binnen derer – über Wunsch einer Vertragsseite – auch ergänzende Gespräche mit dem Ziel einer einvernehmlichen Abänderung geführt werden können.

Sollte bis drei Monate vor Ablauf der Befristung keine Vertragspartei gegenüber der anderen Partei ausdrücklich und schriftlich auf einem Auslaufen der Betriebsvereinbarung mit Fristende bestehen, so verlängert sich diese Betriebsvereinbarung jeweils um 12 Monate.

### 1.3 Sachlicher Geltungsbereich

Diese Zusatzbetriebsvereinbarung regelt die Einführung und Verwendung von elektronischen MitarbeiterInnenausweisen, und die damit in Zusammenhang stehende Verarbeitung personenbezogener Daten von MitarbeiterInnen sowie die damit allenfalls in Zusammenhang stehenden Kontrollen im Anlassfall.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

### 1.4 Rechtsgrundlage

Diese Zusatzbetriebsvereinbarung wird auf der Grundlage der gesetzlichen Bestimmungen, insbesondere im Sinne der §§ 91 Abs. 2, 96 Abs. 1 Z 3, 96a Abs. 1 Z 1 sowie § 97 Abs 1 Z 6 ArbVG, abgeschlossen.

Die Grundsätze und Bestimmungen der Rahmenbetriebsvereinbarung betreffend automationsunterstützte Verwendung personenbezogener ArbeitnehmerInnendaten gelten sinngemäß für diese Zusatzbetriebsvereinbarung, sofern in der Zusatzbetriebsvereinbarung nicht ausdrücklich Abweichendes festgelegt ist.

Die Rechtsgrundlagen dieser Betriebsvereinbarung sind insbesondere:

- das Arbeitsverfassungsgesetz (ArbVG)
- das ArbeitnehmerInnenschutzgesetz (ASchG)
- das Datenschutzgesetz 2000 (DSG 2000) bzw. ab 25.05.2018 das Datenschutzgesetz (DSG) und die Datenschutzgrundverordnung (DSGVO)
- das Telekommunikationsgesetz (TKG)

in der jeweiligen Fassung.

## 2. Technische Ausstattung

2.1 In den MitarbeiterInnenausweisen wird ein Chip des Typs Myfare Desfire EV2 8K verwendet.

2.2 Auf dem Chip selbst werden die jeweiligen Applikationen gemäß den in den Anhängen definierten Verwendung(en) gespeichert. Die einzelnen Applikationen haben jeweils eine eigene Datenbank, in der nur jene Daten gespeichert werden, die für den Prozess notwendig sind.



- 2.3 Die technische Konfiguration erfolgt so, dass sowohl AKH als auch MedUni Wien die jeweiligen Applikationen auf dem Chip einrichten bzw. wieder löschen können.
- 2.4 Es gibt Applikationen, die von Seiten des AKH auf den Chip gespielt werden und solche, die von Seiten der MedUni Wien auf diesen gespielt werden. Für den gemeinsamen Bereich im AKH erhalten die MitarbeiterInnen die jeweils relevanten Applikationen. Dabei gibt es Grundapplikationen für alle MitarbeiterInnen (z.B. Mensa, AKH-Zutrittssystem/Außentüren) und spezielle Applikationen/Berechtigungen (z.B. Zutritt zu besonders geschützten Bereichen). Die Grundapplikationen werden vor der Ausgabe auf den MitarbeiterInnenausweis gespielt. Spezielle Applikationen/Berechtigungen werden bei Bedarf dezentral auf dem MitarbeiterInnenausweis eingerichtet. Der MedUni Wien bzw. dem AKH ist jederzeit auf Verlangen vom AKH bzw. der MedUni Wien darüber Auskunft zu geben, welche Applikationen/Berechtigungen auf dem jeweiligen MitarbeiterInnenausweis von ihm bzw. ihr eingerichtet sind.

### 3. Datenübermittlung an das AKH

- 3.1 Die MedUni Wien überlässt dem AKH auf Basis einer Vereinbarung mit dem AKH personenbezogene Daten der vom Geltungsbereich dieser Zusatzbetriebsvereinbarung erfassten MitarbeiterInnen ausschließlich für den Zweck der Herstellung und Aktualisierung von Ausweisen für die jeweiligen MitarbeiterInnen und der Verwaltung der Berechtigungen für die in den Anhängen festgelegten Applikationen des MitarbeiterInnenausweises sowie für den Zweck des Abgleichs der in Punkt 3.2 lit a bis d genannten Daten (Vorname, Zuname, Akademischer Grad/Titel, Organisationseinheit) mit dem Telefonbuch im AKH-Intranet.
- 3.2 Seitens der MedUni Wien werden folgende abschließend aufgezählte personenbezogene Daten an das AKH übermittelt:
- Vorname
  - Zuname
  - Akademischer Grad, Titel
  - Organisationseinheit
  - Personalnummer
  - Personal-Key
  - E-Mail-Adresse
  - Arzt/Ärztin bzw. Nichtarzt/Nichtärztin
  - gegebenenfalls Fotos
  - Geschlecht
- 3.3 Seitens des AKH werden folgende abschließend aufgezählte personenbezogene Daten an die MedUni Wien übermittelt:
- Personal-Key
  - Kartenummer
  - Chip-Nummer (U-ID)
  - Karten-Status
  - Kartenerstellungsdatum
  - Foto
  - Applikationen



3.4 Im Rahmen der gemeinsamen Betriebsführung von AKH und MedUni Wien werden für eine Übergangsphase die MitarbeiterInnenausweise bis auf weiteres vom AKH im Namen der MedUni Wien erstellt und ausgegeben.

3.5 Die MedUni Wien ist berechtigt, jederzeit die Erstellung und/oder Ausgabe der MitarbeiterInnenausweise selbst zu übernehmen.

#### **4. Applikationen**

4.1 Die jeweils aktuellen Applikationen der in die MitarbeiterInnenausweise integrierten Chips werden in den Anhängen festgelegt.

#### **5. Auswertungen**

5.1 Auswertungen sind grundsätzlich unzulässig und dürfen nur in den in den Anhängen definierten Fällen unter Einbindung der zuständigen Gremien der MedUni Wien bzw. entsprechend der Rahmenbetriebsvereinbarung erfolgen. Die Auswertung von Bewegungsprofilen muss technisch unterbunden werden. Es darf keine Verknüpfung von personenbezogenen Daten mit anderen Systemen geben.

5.2 Zur Kontrolle kann quartalsweise unter Einbindung der Betriebsratsgremien unter Einhaltung des 4-Augen-Prinzips eine Auswertung darüber angefordert werden, wann welche Auswertung gemacht hat.

#### **6. Schlussbestimmungen**

6.1 Die Anhänge bilden einen integrierenden Bestandteil dieser Zusatzbetriebsvereinbarung.



Der Rektor

Univ. Prof. Dr. Markus Müller

Der Vorsitzende des Betriebsrats für das  
wissenschaftliche Universitätspersonal

Ass.-Prof. Dr. Ingwald Strasser

Die Vorsitzende des Betriebsrats für das  
allgemeine Universitätspersonal

Gabriele Waldfinger

Wien, am ..... 12.7.2018 .....

Anhänge



## Anhang

zur Zusatzbetriebsvereinbarung über die Einführung und Verwendung elektronischer  
MitarbeiterInnenausweise

Datenaustausch MUW	Beschreibung	Zweck	Datenkategorien	Speicherort	Speicherdauer	Zugriffsberechtigung
Ausweiserstellung	Applikation zur Erstellung von Ausweisen für AKH-MitarbeiterInnen	Verwaltung von Ausweisdaten und Vergabe von Berechtigungen für Essensbezahlung, Sperr- und Zutrittssystemen und Wäscheausgabe Personenspezifische Daten	VorUndNachname  NachnameTitel EternalNumber PersNr Nachname PersTyp Titel Vorname Abteilung Kommentar Kommentar2 Besucherbegleitung Foto Staatsangehoerigkeit Ausweisnummer Anrede Firma Strasse PLZ Stadt Staat GebDat GebOrt TelNr Email LetzteAenderung DatensatzNeu Kontaktperson Kontaktabteilung KontaktTelNr Unterschrift Dokument Arbeitsstation Funktion Bereich Mkz SAP_ID KeyNumber_tmp Ausgetreten Ausgetreten_am Zusatz LetzteAenderungAmpel KarteUebergeben DatensatzKNeu	SQL-Server (db-ausweise.routine.akhwi.n.at), File-Server (v01fil04.routine.akhwi.n.at), AVASYS-Server (v01ava01.ht.akhwi.n.at)	für die gesamte Dauer der Beschäftigung	Username und Passwort; MitarbeiterInnen des AKH-Personalbüros für die Anwendung; MitarbeiterInnen der AKH-EDV-Abteilung zur Betriebsführung
		Kartenspezifische Daten	LetzteKAenderung Kartenstatus Strichcode Layout ChipSN Kodierdatum Druckdatum Zutrittsgruppen GueltigBis GueltigVon KartenNr KartenKommentar EternalNumber CardID ZutrittsgruppenSMS ZutrittsgruppenGueltigVon ZutrittsgruppenGueltigBis Kartenkodierdefinition AOC KartenVerifikation			
Essensbezahlung	Kassensystem im AKH-Betriebsrestaurant inkl. bargeldloser Bezahlmöglichkeit.	Verwaltung von bargeldloser Bezahlung im AKH-Betriebsrestaurant mittels MitarbeiterInnenausweis	PKE-Kartenummer Kundengruppe (Rabattierung) Betrag (Guthaben) Gültigkeitsdatum	v01sqi09.routine.akhwi.n.at	keine Regelung, Guthaben hat kein Ablaufdatum. Zugriffsberechtigung über Gültigkeitsdatum geregelt.	UserID und Passwort; MitarbeiterInnen der AKH-Küche für die Anwendung; MitarbeiterInnen der AKH-EDV-Abteilung zur Betriebsführung; Firma Ventopay



<b>Sperr-/Zutrittssystem</b>	Applikation zur Verwaltung von Berechtigungen für die AKH-Sperr- und Zutrittssystemen	Verwaltung von Sperr- und Zutrittsberechtigungen im AKH	Name:  Vor- und Nachname  Akadem. Grad  Ort: Bauteil, Ebene, Tür  Gültigkeit: von: bis:  Kartennr: xy  Kartenstatus: verloren/ungültig, etc;  Zugehörigkeit: AKH, MUW, VKMB, Gast etc.  Organisation: Klinik, Institut, etc.	VM Ware V01AVA01.ht.akhwienn.at / AKH Computerraum Ebene 3C	keine Regelung, da lediglich die Berechtigung mit J/N gespeichert wird (Videomaterial flexibel 0-xx H)	Username und Passwort; MitarbeiterInnen des AKH-Personalbüros für die Anwendung; MitarbeiterInnen der AKH-EDV-Abteilung zur Betriebsführung
<b>Wäscheautomat</b>	Verwaltung von Wäscheausgabe für AKH-MitarbeiterInnen	Automatische Ausgabe von Wäsche mittels MitarbeiterInnenausweis	Kartennummer Nachname Vorname	WäscheDB (KAV-IT), AdvantTex	keine Regelung, da lediglich die Berechtigung mit J/N gespeichert wird	Username und Passwort; Berechtigte MitarbeiterInnen des AKH (Freischaltung durch AKH Wäscherei); MitarbeiterInnen der AKH-EDV-Abteilung zur Betriebsführung
<b>CMS Intranet Telefonbuch</b>	CMS-Intranet-Telefonbuch	Telefonbuch des AKH für alle Mitarbeiter des AKH	Nachname Vorname Titel Akad.Grad Organisationseinheit Geschlecht Mailadresse Personenkey	SQL Server/Produktiver Cluster (v01sql10)	Die Daten werden nur solange verwendet wie sie in der Quelle vorhanden sind	AKH interner Zugriff auf die Telefonbuchdaten. Zugriff auf Personenkey nur durch Admins.

### Konkretisierungen und Erläuterungen zur Exceltabelle:

In der Exceltabelle sind jene Applikationen aufgeführt, die im Einsatz sind, und die dazugehörigen Datenfelder.

Seitens MedUni Wien werden nur jene Daten übermittelt und dann vom AKH rückübermittelt, die gemeinsam definiert wurden. Die Gemeinde Wien speichert für ihre MitarbeiterInnen weitere Daten in den Systemen, diese sind in der Tabelle nur der Vollständigkeit halber aufgelistet. (Die Felder bleiben somit in der Datenbank mangels Inhalt frei).

Auf dem Ausweis selbst befinden sich keine Personendaten, nur Applikationen.

Spätestens 6 Monate nach dem Ausscheiden eines/einer Mitarbeiters/Mitarbeiterin werden sämtliche personenbezogenen Daten im Zusammenhang mit dem MitarbeiterInnenausweis gelöscht.

### Sperr- /Zutrittssystem:

- **Speicherdauer:** Die historischen Daten (Zutrittsdaten, Offline-Meldungen, usw.) werden im AVASYS 6 Monate lang gespeichert, danach gelöscht.

Im AVASYS besteht die Möglichkeit einzelne Meldungen, (z.B.: Türbuchungen) komplett aus der Aufzeichnung zu entfernen. Derzeit werden alle Meldungen protokolliert.





- Kameras: Derzeit sind insgesamt 4 Kameras eingebunden.  
3 Kameras sind eine Teststellung für die AKH-EDV (Axis Kameras, im Bauteil 61 - Ersatzrechenzentrum des AKH).  
Die vierte Kamera befindet sich im Bauteil 21 - Leitwarte - EB07 - Serverraum - Bosch Kamera.  
Bei allen vier Kameras findet eine Aufzeichnung statt. Bei Kamera 1 und 2 findet eine Daueraufzeichnung, bei Kamera 3 und 4 eine Motion Aufzeichnung statt. Alle Videodaten werden bis zu 72 Stunden gespeichert.
- Es erfolgt keine Speicherung von Name/Vorname, diese Daten werden bei Eintrag einer Zutrittsberechtigung über die ID der Karte geholt und angezeigt.
- Derzeit wird das optionale Angebot der Herstellerfirma - Aufzeichnung aller Türbuchungen - genutzt, dieses kann auch deaktiviert werden.

#### Wäscheautomat:

- Der Wäscheautomat hat die Daten zum Kontingent des/der Mitarbeiters/Mitarbeiterin an verfügbarer Wäsche und der tatsächlich aus dem Automaten entnommener Wäsche. Daraus ergibt sich, ob der/die MitarbeiterIn Wäsche aus dem Automaten entnehmen darf J/N (Beispiel: Kontingent: 3 Arztkittel Größe X / Entnommen: 3 Arztkittel Größe X -> Berechtigung = N).  
Bei Rückgabe von entnommener Wäsche wird das Kontingent wieder frei.
- Daten wie Nach-/Vorname, Kontingent und die ID des MitarbeiterInnenausweises sind in AdvanTex (Wäsche-DB) erfasst, Änderungen werden dem Automaten via Schnittstelle weitergeleitet.
- Der Server von AdvanTex steht in der KAV-IT - dem AKH werden lediglich Clients und User zur Verfügung gestellt.  
Der Server des Wäscheautomaten steht im AKH, wird jedoch inhaltlich nicht supported.
- In AdvanTex gibt es einen eigenen Bereich für das AKH. Zugriff haben dort zu Support-Zwecken die KAV-IT und die Serviceeinheit Wäsche und Reinigung (SWR), individuelle Berechtigungen können seitens DTI nicht eingesehen werden.  
Auf den Wäscheautomaten haben nur MitarbeiterInnen der SWR zu Support-Zwecken Remote Zugriff.
- Speicherdauer: Die Daten werden 6 Monate nach dem jeweiligen Vorgang gelöscht.