WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

BV Mobile Device Management System

Betriebsvereinbarung über den Einsatz des Mobile Device Management Systems

Inhalt

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 gemäß § 96 Abs 1 Z 3 ArbVG/§ 96a Abs 1 Z 1 ArbVG in der geltenden Fassung folgende Betriebsvereinbarung über den Einsatz des Mobile Device Management Systems (MDM) ab.

1. Einleitung

(1) Vorliegende Betriebsvereinbarung regelt die Verwendung des Mobile Device Management Systems (MDM-System) bei der Arbeitgeberin. Durch die Verwendung des MDM-Systems soll sichergestellt werden, dass mit Mobile-Devices in einem abgesicherten Rahmen auf WU-Systeme zugegriffen werden kann (**Systemzweck**). In diesem Zusammenhang wird wie folgt vorgegangen:

- Alle von der WU zur Verfügung gestellten Mobile-Devices werden in das MDM-System eingebunden, außer der Arbeitnehmer oder die Arbeitnehmerin teilt vorab schriftlich mit, dass er oder sie keine Einbindung haben will („opt-out-Mitteilung")
- Der Arbeitnehmer oder die Arbeitnehmerin kann auch sein oder ihr privates Mobile-Device in das MDM-System einbinden lassen, indem er oder sie eine entsprechende Einwilligungserklärung abgibt („opt-in-Mitteilung").

(2) Mit Mobile Devices, die nicht in das MDM-System eingebunden sind, kann kein automatisierter Abgleich (Synchronisation) mit Daten, die sich auf WU-Systemen befinden, erfolgen. In diesem Fall ist ein Zugriff auf WU-Systeme nur mit vorheriger Authentifizierung möglich (zB Open Web Access für Emails).

(3) Die Arbeitgeberin wird sich im Rahmen der technischen und wirtschaftlichen Möglichkeiten bemühen, einen Zugriff auf WU-Systeme außerhalb des MDM-Systems für die Arbeitnehmer und Arbeitnehmerinnen anzubieten.

2. Geltungsbereich

(1) **Persönlich**: Für alle Arbeitnehmer/innen der Arbeitgeberin iSd § 36 ArbVG.

(2) **Zeitlich**: Diese Betriebsvereinbarung tritt am 1. August 2019 in Kraft und wird auf unbestimmte Zeit abgeschlossen. Die Betriebsvereinbarung kann von den Vertragsparteien unter Einhaltung einer sechswöchigen Kündigungsfrist zum Ende eines jeden Kalenderjahres schriftlich aufgekündigt werden, wobei der früheste Kündigungstermin der 31.12.2020 ist. Vor der Aufkündigung sind jedoch Verhandlungen mit der jeweils anderen Abschlusspartei aufzunehmen mit dem Bemühen, eine Einigung zu finden.

(3) **Sachlich**: Diese Betriebsvereinbarung regelt die Verwendung des MDM-Systems

3. Begriffsbestimmungen

(1) Personenbezogene ArbeitnehmerInnendaten: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (die Arbeitnehmerin/den Arbeitnehmer) beziehen; als identifizierbar wird die Arbeitnehmerin/der Arbeitnehmer angesehen, wenn sie/er direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der Arbeitnehmerin/des Arbeitnehmers sind, identifiziert werden kann.

Es werden folgende Kategorien an ArbeitnehmerInnendaten unterschieden:

„Stammdaten" (Kategorie A) sind allgemeine Daten zur Person der Arbeitnehmerin/des Arbeitnehmers und sind vor allem zur Organisation/Abwicklung betrieblicher Arbeits- und Kommunikationsprozesse erforderlich (Beispiele: Name, Organisationseinheit, Dienstadresse, Büroraum, Telefonnummer, E-Mail-Adresse, User-ID).

- „Abwicklungsdaten" (Kategorie B) sind notwendig, um gesetzlichen und/oder vertraglichen Verpflichtungen (eindeutiger und legitimer Zweck) nachzukommen (Beispiele: Name, Privatadresse, Arbeitszeit, Urlaub, Qualifikationen).

- „Ortungsdaten" (Kategorie C) sind alle Daten, die den aktuellen Standort einer Person bestimmen.

- „Sensible Daten" (Kategorie D) sind alle Daten im Sinne des Art 9 Abs 1 DSGVO. Zudem werden der „Kategorie D" Daten über strafrechtliche Verurteilungen und Straftaten zugeordnet.

- „App-Inventardaten" (Kategorie E) sind alle Daten, die Informationen über die am Mobile Device installierten Apps enthalten (zB Name der App, Version der App, Datum des letzten Updates der App).

- „Log-In-Daten" (Kategorie F) sind alle Daten, die Informationen über die aktive Nutzungszeit von Mobile Devices durch den Arbeitnehmer und die Arbeitnehmerin enthalten.

(2) Mobile-Devices: Smartphones oder Tablets (ungeachtet dessen, ob sie der WU oder dem Arbeitnehmer oder der Arbeitnehmerin gehören), die mit einem vom MDM-System unterstützten Betriebssystem (derzeit Apple iOS oder Google Android) betrieben werden.

(3) Updates: Aktualisierungen des MDM-Systems, die keine Funktionserweiterung darstellen. Beispiel: Einspielen eines Sicherheits-Updates oder einer neuen Programmversion.

(4) Systemerweiterung: Anpassungen des MDM-Systems, die zu einer Erweiterung der in 4.1 aufgezählten Funktionen führen. Beispiel: Erweiterung um eine Ortungsfunktion.

4. Funktion des MDM-Systems

(1) Folgende Funktionen des MDM-Systems sind an der WU aktiviert:
- Erzwingung eines Pin- oder Passcodes
- Sperren des Zugriffs auf WU-Systeme und des automatisierten Abgleichs mit darauf befindlichen Daten, wenn ein Sicherheitsrisiko identifiziert wird

- Erstellen von Statistiken
- Löschen der für die Nutzung des MDM-Systems erforderlichen Funktionen und der vom MDM-System gespeicherten Daten vom Mobile-Device sowie Sperren der Synchronisation mit dem WU E-Mail Konto auf Wunsch des Arbeitnehmers oder der Arbeitnehmerin
- Zurücksetzen des Mobile-Devices auf Wunsch des Arbeitnehmers oder der Arbeitnehmerin auf den Werkszustand

(2) Soweit möglich, wird der Arbeitnehmer oder die Arbeitnehmerin vom Sperren/Blockieren des Zugriffs auf WU-Systeme im Vorhinein informiert.

(3) Das derzeit verwendete MDM-System wird in **Anhang 1** kurz beschrieben. Die WU ist berechtigt, das jeweils verwendete MDM-System stets auf dem aktuellen Stand der Technik zu halten und sonstige notwendige Anpassungen (Updates) vorzunehmen, solange sie zu keiner Systemerweiterung führen.

(4) Systemerweiterungen können nur mit vorheriger Zustimmung des Betriebsrats vorgenommen werden.

5. Umfang der Nutzung des MDM-Systems

(1) Im Rahmen des MDM-Systems werden ausschließlich Daten der Kategorie (A), (E) und (F) verarbeitet. Zur Identifikation von Apps, von denen Sicherheitsgefahren ausgehen, kann es weiters zur Verarbeitung von Daten der Kategorie (D) kommen.

(2) Auswertungen personenbezogener Daten dürfen im Rahmen des MDM-Systems nur zu den in Punkt 1 Abs 1 dieser Betriebsvereinbarung genannten Zwecks sowie zur Wahrung berechtigter Interessen der WU gemäß Art 6 Abs 1 lit f DSGVO, insbesondere zur Aufrechterhaltung der System- oder Datensicherheit, erfolgen.

Auswertungen, die unter Missachtung dieses Absatzes vorgenommen werden, dürfen nicht als gerichtliche oder außergerichtliche Beweismittel zum Nachteil der Arbeitnehmer/innen verwendet werden. Es besteht ein diesbezügliches außergerichtliches, gerichtliches und behördliches Beweismittel- und Beweisverwertungsverbot. Unzulässige Auswertungen dürfen auch in keiner Weise zu arbeitsrechtlichen Konsequenzen führen.

(3) Jede Auswertung und jeder Verarbeitungsvorgang ist von der WU zu protokollieren. Auf Verlangen des Betriebsrates ist dem Betriebsrat Einsicht in die Protokolldaten zu geben.

(4) Für alle im Rahmen des MDM-Systems verarbeiteten personenbezogenen Arbeitnehmer- und Arbeitnehmerinnendaten gilt, dass diese nach Zweckerfüllung und dem Ablauf gesetzlicher oder anderer rechtlicher Aufbewahrungsfristen zu löschen oder zu anonymisieren sind. Daten der Kategorie F werden innerhalb von einem Monat gelöscht.

6. Maßnahmen zur Datensicherheit

(1) Zur Sicherstellung des Grundsatzes der Datensicherheit sind auf Basis einer Risikobewertung von der WU geeignete technische und organisatorische Maßnahmen iSd Art 32 EU-DSGVO zu ergreifen und zu dokumentieren.

(2) Insbesondere ist von der WU sicherzustellen, dass

- ausschließlich berechtigte Personen Zugang zu den im Rahmen des MDM-Systems aufgezeichneten Daten haben (Grundsatz der Zugriffssicherheit).

- nur Zugang zu jenen Daten besteht, die zur Erfüllung der jeweiligen dienstlichen Aufgaben des oder der Zugangsberechtigten notwendig sind („Need-to-know-Prinzip").

- nachvollzogen werden kann, wer welches Datum in welcher Art verarbeitet hat (Grundsatz der Verarbeitungsnachvollziehbarkeit).

(3) Ein aktuelles Berechtigungsverzeichnis wird dieser Betriebsvereinbarung als **Anhang 2** angeschlossen. Die WU verpflichtet sich, den Anhang 2 stets aktuell zu halten.

(4) Alle Arbeitnehmer und Arbeitnehmerinnen, die gemäß **Anhang 2** Zugriff auf im Rahmen des MDM-Systems aufgezeichnete Daten haben, sind über die Verpflichtungen, die sich aus den datenschutzrechtlichen Bestimmungen ergeben, zu informieren.

(5) Auf dienstliche Anwendungen darf nur unter strikter Einhaltung der von der WU festgelegten Nutzungsbedingungen zugegriffen werden, insbesondere ist von dem Benutzer oder der Benutzerin ein dementsprechender Passwortschutz zu verwenden.

7. Digitalisierungs-Jour-Fixe

(1) Zumindest zweimal im Jahr finden Beratungen mit dem Betriebsrat über das MDM-System statt (= Digitalisierungs-Jour-Fixe). Das Digitalisierungs-Jour-Fixe setzt sich zumindest aus einem Vertreter oder einer Vertreterin des jeweiligen Betriebsrates sowie zwei Vertretern oder Vertreterinnen der WU zusammen.

(2) Fixpunkte bei diesem Informationsaustausch sind: (i) Rückblickende Darstellung der seit dem letzten Treffen erfolgten Updates und Systemerweiterungen seitens IT-Services. (ii) Vorausschauender Überblick über geplante Updates und Systemerweiterungen durch IT-Services. (iii) Gemeinsamer Austausch über die in (i) und (ii) vorgestellten Themen.

(3) Das Digitalisierungs-Jour-Fixe dient ausschließlich dem Informationsaustausch und der Beratung, wobei Übereinstimmung besteht, dass dadurch die im Zusammenhang mit der Verarbeitung personenbezogener Arbeitnehmer- und Arbeitnehmerinnendaten bestehenden gesetzlichen Informations- und Beratungsrechte gegenüber dem Betriebsrat erfüllt werden.

(4) Unbeschadet dem Informationsaustausch im Rahmen der Digitalisierungs-Jour-Fixe ist der Betriebsrat auch außerhalb der Digitalisierungs-Jour-Fixe über Anpassungen im Umfang der Nutzung des MDM-Systems, die noch nicht in einem Digitalisierungs-Jour-Fixe behandelt wurden, im Vorhinein zu informieren.

8. Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieser Betriebsvereinbarung unwirksam sein oder werden, so bleiben die anderen Teile davon unberührt.

(2) Anhang 1 und 2 bilden keinen normativen Bestandteil dieser Betriebsvereinbarung, sondern haben lediglich informativen Charakter. Die WU ist dennoch stets dazu verpflichtet, die Anhänge aktuell zu halten.

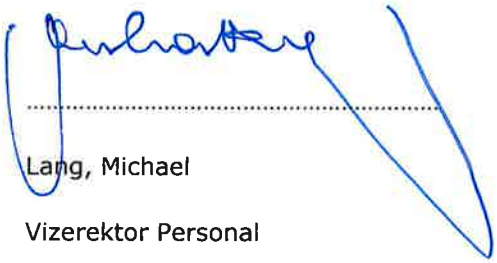
(3) Abänderungen dieser Betriebsvereinbarung können im Einvernehmen zwischen allen Parteien ausschließlich in schriftlicher Form erfolgen.

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

(5) Die betroffenen Arbeitnehmer und Arbeitnehmerinnen der WU sind über den Inhalt dieser Betriebsvereinbarung durch deren Veröffentlichung im Intranet der WU unter https://swa.wu.ac.at/Serviceeinrichtungen/personalabt/SitePages/Betriebsvereinbarungen.aspx zu informieren.

Wien, am 17.7.2019

Für die WU:



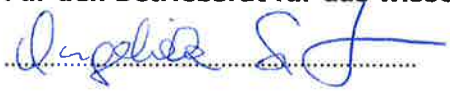
Lang, Michael

Vizerektor Personal

Für den Betriebsrat für das allgemeine Universitätspersonal:

Hess, Friedrich
Vorsitzender des Betriebsrates für das allgemeine Universitätspersonal

Für den Betriebsrat für das wissenschaftliche Universitätspersonal:



Schmidt, Angelika
Vorsitzende des Betriebsrates für das wissenschaftliche Universitätspersonal

Anhänge:

- Anhang 1: Beschreibung des derzeit verwendeten MDM-Systems
- Anhang 2: Berechtigungsverzeichnis

Anhang 1: Beschreibung des derzeit verwendeten MDM-Systems

Systembeschreibung:

Als MDM-System wird derzeit "Mobile Iron" eingesetzt. Folglich wird jedes in das MDM-System eingebundene Mobile-Device mit der MobileIron Clientsoftware „Mobile@Work" ausgestattet.

1. Derzeitige Funktionen von „Mobile Iron"

ID	Funktionen	Für MDM-Administratoren oder Administraorinnen STÄNDIG AKTIVIERT	Für MDM-Administratoren oder Administratorinnen nur nach Zustimmung durch die Arbeitnehmer/innen AKTIVIERBAR	Möglich, aber nicht aktiviert	Nicht möglich
1	Erzwingung eines Pin- oder Passcodes	•			
2	Sperren des Zugriffs auf WU-Systeme und des automatisierten Abgleichs mit darauf befindlichen Daten, wenn ein Sicherheitsrisiko identifiziert wird	•			
3	Erstellen von Statistiken	•			
4	Löschen der für die Nutzung des MDM-Systems erforderlichen Funktionen und der vom MDM-System gespeicherten Daten vom Mobile-Device sowie Sperren der Synchronisation mit dem WU E-Mail-Konto		•		
5	Zurücksetzen des Mobile-Devices auf Wunsch des Arbeitnehmers oder der Arbeitnehmerin auf den Werkszustand		•		

6	Orten von Geräten			•	
7	Aktivieren von Mikrofon oder Kamera mittels MDM				•
8	Sichern (Backup) von Geräten mittels MDM				•
9	Fernsteuern von Geräten mittels MDM				•

2. Derzeit mit „Mobile Iron" verarbeitete personenbezogene Daten:

ID	Parameter	Wert/Einstellung (BEISPIELNAME)
1	User ID	mustermann
2	Attribute Distinguished Name	CN=mustermann,OU=NW,OU=ZID,OU=Rektorat,OU=Personal,DC=ad,DC=wu-wien,DC=ac,DC=at
3	cn	mustermann
4	Current Phone Number	+4367600000000
5	Device Name	mm's iPhone 6
6	Display Name	Mustermann, Max
7	displayName	Mustermann, Max
8	distinguishedName	CN=mustermann,OU=NW,OU=ZID,OU=Rektorat,OU=Personal,DC=ad,DC=wu-wien,DC=ac,DC=at
9	Email Address	max.mustermann@wu.ac.at
10	First Name	Max
11	givenName	Max
12	Home Phone Number	67600000000
13	Last Name	Mustermann
14	LDAP User Distinguished Name	cn=mustermann,ou=nw,ou=zid,ou=rektorat,ou=personal,dc=ad,dc=wu-wien,dc=ac,dc=at
15	mail	max.mustermann@wu.ac.at
16	memberOf	OU=ShareGruppen,OU=Gruppen,DC=ad,DC=wu-wien,DC=ac,DC=at,CN=sp.CP_Datacenter.read,OU=SharepointGruppen
17	Principal	mustermann

18	sAMAccountName	mustermann
19	sn	Mustermann
20	upn	mustermann@ad.wu-wien.ac.at
21	userPrincipalName	mustermann@ad.wu-wien.ac.at

3. Auszug aus dem App Log:

Parameter	**Wert 1**	**Wert 2**
Action	Uninstall App	Install App
State	Success	Success
Performed By	amuhmtest	amuhmtest
Action Date	2019-04-23 20:46:45 +0000	2019-04-23 20:46:45 +0000
Performed On	amuhmtest (Android 6.0 - +4367682134106)	amuhmtest (Android 6.0 - +4367682134106)
Details	App Google Play services for Instant Apps 4.16-release-242931550 Uninstalled	App Google Play services for Instant Apps 4.17-release-243979070 Installed
Space Name		
Space Path		
Actor	{principal=amuhmtest, miUserId=9078, email=}	{principal=amuhmtest, miUserId=9078, email=}
Logged At	2019-04-23 20:46:45 +0000	2019-04-23 20:46:45 +0000
Version	1	1
User Role		
Object Id		
Object Name		
Subject ID	0b33ea97-d073-45fd-af27-7b5a6b0f1de3	0b33ea97-d073-45fd-af27-7b5a6b0f1de3
Subject Type	Smartphone	Smartphone
Subject Owner Name		
Completed At	2019-04-23 20:46:45 +0000	2019-04-23 20:46:45 +0000
Cookie		
Device	{phoneNumber=+4367682134106, uuid=0b33ea97-d073-45fd-af27-7b5a6b0f1de3, platform=Android 6.0}	{phoneNumber=+4367682134106, uuid=0b33ea97-d073-45fd-af27-7b5a6b0f1de3, platform=Android 6.0}
Requested At	2019-04-23 20:46:45 +0000	2019-04-23 20:46:45 +0000
Configuration		
Object Type		
Parent ID		
Update Request Id		
Log Type	userAction	userAction
Updated Blob		
Message		

Anhang 2: Berechtigungsverzeichnis

Zugriffsberechtigte im Rahmen der Berechtigungen laut Betriebsvereinbarung:

- Systemadministratoren oder Systemadministratorinnen der Abteilung Network Infrastructure
- (stv.) Abteilungsleiter oder (stv.) Abteilungsleiterin der Abteilung Network Infrastructure

9. Dokumentinformationen

Pflichtfelder sind mit einem „*" gekennzeichnet.

Abgeschlossen zwischen*	**Wirtschaftsuniversität Wien**, Welthandelsplatz 1, 1020 Wien – als Arbeitgeberin einerseits UND dem
	Betriebsrat für das wissenschaftliche Universitäts-personal
	sowie dem **Betriebsrat für das allgemeine Universitätspersonal** beide gemeinsam in der Folge auch „die Betriebsräte" genannt.
Kurztitel [1]*	BV Mobile Device Management System
Langtitel	Betriebsvereinbarung über den Einsatz des Mobile Device Management Systems
Dateiname[2]*	BV MDM_20190701_Endfassung.docx
Ersetzt	-
Titel englische Version	-
Version (Nummer, Datum)*	-
Inhaltsverantwortlich*	Vizerektor für Forschung / Pichler, Stefan
Autor/in*	IT-Services / Mika, Peter, Rechtsabteilung / Schneider Reingard
Ansprechperson für inhaltliche Fragen und praktische Umsetzung	IT-Services / Mika, Peter

Kommunikation* (Mehrfachauswahl möglich)	☒ E-Mail ☒ Mitteilungsblatt ☒ Regelungsdatenbank
Veröffentlicht im Mitteilungsblatt	Studienjahr 2018/19, 44. Stück, Nr. 236 vom 24.07.2019
Erstveröffentlichung (optional)	Studienjahr 2018/19, 44. Stück, Nr. 236 vom 24.07.2019

1 Beispiele für Kurztitel/Langtitel:
- Kurztitel = Kategorie und Schlagwort z.B. WUPOL Software
- Langtitel oder Subtitel = Bezeichnung aus der Abteilung, z.B. Regelung über die Verwendung von WU Software

2 Dateinamen max. 60 Zeichen; keine Umlaute, Sonderzeichen oder Leerzeichen verwenden

Gültig ab*	01.08.2018
Gültig bis*	31.12.2999
Genehmigt von	Vizerektor für Personal, Lang, Michael am 18.07.2019
Weitere Informationen*	