BETRIEBSVEREINBARUNG

für
operative Systeme

abgeschlossen zwischen der

Wirtschaftsuniversität Wien

als Betriebsinhaber

vertreten durch den

Rektor o.Univ. - Prof. Dr. Christoph Badelt

in der Folge kurz „WU" genannt,

einerseits

sowie dem

Betriebsrat für das wissenschaftliche Universitätspersonal der Wirtschaftsuniversität Wien

und dem

Betriebsrat für das allgemeine Universitätspersonal der Wirtschaftsuniversität Wien

beide gemeinsam in der Folge auch „Betriebsräte" genannt,

andererseits.

I. Allgemeines

1. Die WU setzt verschiedene automationsunterstützte Systeme ein, die personenbezogene Daten von Mitarbeitern/Mitarbeiterinnen (Arbeitnehmer/Arbeitnehmerinnen im engeren Sinne einschließlich der von der WU übernommenen Vertragsbediensteten sowie Beamte/Beamtinnen des Bundes, die der WU zur Dienstleistung zugewiesen sind) verwenden. Zum einen sind das Systeme der Personalwirtschaft, zum anderen aber auch personalwirtschaftsfremde Systeme wie insbesondere Kommunikationssysteme. Die verwendeten Systeme werden von der WU zur effizienten Abwicklung der Aufgaben der WU, zur Gewährleistung der Sicherheit an der WU sowie zur internen und externen Datenkommunikation eingesetzt.

2. Die WU und die Betriebsräte stimmen darin überein, dass die von der WU eingesetzten Systeme für die jeweiligen Zwecke, insbesondere für eine effiziente Administration sowie für die Gewährleistung einer zeitgemäßen internen und externen Kommunikation notwendig sind. Einigkeit besteht auch dahingehend, dass elektronische Systeme aufgrund der rasant fortschreitenden technologischen Entwicklung ständig einem hohen Anpassungs- bzw Aktualisierungsbedarf unterliegen und dass die WU daher veranlasst ist, diesem dynamischen Wandel entsprechend Folge zu leisten.

3. Die WU erklärt, dass sie personenbezogene Mitarbeiter/innen/daten nur im gesetzlich erlaubten und betrieblich unbedingt notwendigen Ausmaß verarbeitet oder an Dritte übermittelt.

II. Geltungsbereich und Regelungsgegenstand

1. Sachlich

Diese Betriebsvereinbarung regelt die automationsunterstützte Verwendung (Verarbeitung sowie Übermittlung im Sinne des § 4 DSG 2000) personenbezogener Arbeitnehmer/innen/daten sowie die damit allenfalls im Zusammenhang stehenden Kontrollen. Unter Arbeitnehmer/innen/daten sind Daten über Mitarbeiter/innen sowie über sonstige Personen zu verstehen, die in den Betrieb der WU eingegliedert sind. Personenbezogene Daten liegen vor, wenn die Identität der betreffenden Person bestimmt oder bestimmbar ist (§ 4 Z 1 DSG 2000).

Regelungsgegenstand ist dabei die Verwendung personenbezogener Arbeitnehmer/innen/daten in den in Anlage 1 genannten Anwendungen bzw Systemen der WU. Die Grundsätze dieser Betriebsvereinbarung gelten sinngemäß für alle bestehenden und zukünftigen (Zusatz-)Betriebsvereinbarungen, die (auch) die Verwendung personenbezogener Arbeitnehmer/innen/daten zum Gegenstand haben, wenn dies nicht explizit ausgeschlossen wird.

2. Persönlich und örtlich

Diese Betriebsvereinbarung gilt für alle Mitarbeiter/innen (Arbeitnehmer/innen im engeren Sinne einschließlich der von der WU übernommenen Vertragsbediensteten des Bundes sowie Beamte/Beamtinnen des Bundes, die der WU zur Dienstleistung zugewiesen sind) der WU sowie für

sonstige Personen, die in den Betrieb der WU eingegliedert sind. Nicht vom Anwendungsbereich erfasst ist insbesondere die Verwendung von Studierendendaten oder von Daten sonstiger Personen, über die die WU verfügt, auch wenn die Daten mit denselben Systemen verarbeitet werden wie die Arbeitnehmer/innen/daten.

3. Zeitlich

Diese Betriebsvereinbarung tritt am 01.08.2009 in Kraft und kann von beiden Vertragsparteien unter Einhaltung einer 6-wöchigen Kündigungsfrist aufgekündigt werden.

4. Die Betriebsvereinbarung 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.

III. Zielsetzung und rechtliche Grundlagen

1. Mit dieser Betriebsvereinbarung soll sichergestellt werden, dass die Mitarbeiter/innen vor einer missbräuchlichen Verwendung personenbezogener Daten, insbesondere einer missbräuchlichen Überwachung ihres Verhaltens und einem missbräuchlichen Zugriff auf ihre Daten geschützt werden.

2. Die WU und die Betriebsräte sind sich darüber einig, dass die Betriebsvereinbarung dazu dient, die Umsetzung von rechtlichen Bestimmungen zur Verhinderung des Datenmissbrauchs zu unterstützen.

3. Ein weiteres Ziel dieser Vereinbarung ist es, die gesetzlichen Erfordernisse nach dem DSG 2000 zu erfüllen und dabei an der WU eine effiziente und fehlerfreie Datenbewirtschaftung sicherzustellen. Die WU erklärt, bei der Verarbeitung personenbezogener Arbeitnehmer/innen/daten die diesbezüglichen gesetzlichen Bestimmungen zu beachten und verpflichtet sich, personenbezogene Arbeitnehmer/innen/daten wirksam gegen Verlust, Verfälschung und den Zugriff Unbefugter zu sichern.

IV. Beschreibung der Datenverwendung

1. Die vorliegende Betriebsvereinbarung bezieht sich auf die Verwendung personenbezogener Arbeitnehmer/innen/daten der WU. In Anlage 1 werden Systeme der WU aufgezählt, die mit personenbezogenen Arbeitnehmer/innen/daten operieren. Weiters wird in dieser Anlage abgebildet, welche Einheiten der WU zur personenbezogenen Auswertung der Daten berechtigt sind. Eine Änderung und/oder Ergänzung der berechtigten Einheiten erfolgt durch das zuständige Mitglied des Rektorats. Anlage 1 ist diesfalls entsprechend anzupassen und die Betriebsräte sind zu

informieren. Die Erteilung der Berechtigung an die der jeweiligen Einheit zugeordneten Mitarbeiter/innen erfolgt durch die in Anlage 1 jeweils angeführte autorisierte Person.

2. Die WU hat das Recht, die verwendeten Systeme stets auf dem aktuellen Stand der Technik zu halten. 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.

3. Bei wesentlichen Erweiterungen und/oder Änderungen dieser Systeme ist vorab die Zustimmung der Betriebsräte einzuholen. Anlage 1 ist danach entsprechend zu aktualisieren

4. Eine wesentliche Änderung eines Systems ist gegeben, wenn durch sie

- zusätzliche personenbezogene Daten erhoben, gespeichert und verarbeitet werden;
- der Kreis der Zugriffsberechtigten erweitert wird oder
- neue personenbezogene Auswertungen ermöglicht werden.

Anlage 2 enthält einen Beispielkatalog solcher wesentlichen Änderungen.

V. Umfang der Datenverwendung

1. Personenbezogene Arbeitnehmer/innen/daten dürfen von der WU nur im Rahmen der einschlägigen Gesetze und dieser Betriebsvereinbarung verwendet werden.

2. Eine Übermittlung von personenbezogenen Arbeitnehmer/innen/daten an Dritte darf – mit Ausnahme des Pkt V.5. dieser Betriebsvereinbarung – ohne Zustimmung des/der betroffenen Mitarbeiters/Mitarbeiterin nur im Rahmen gesetzlicher und/oder kollektivvertraglicher Verpflichtungen erfolgen. In Anlage 3 wird jeweils angeführt, welche Daten an welchen Empfängerkreis weitergeleitet werden. Eine Erweiterung der übermittelten Daten und/oder des Empfängerkreises ist den Betriebsräten anzuzeigen und in Anlage 3 entsprechend anzuführen.

3. Aufzeichnungen und/oder Auswertungen der Benutzeraktivitäten (Login/Logout, aufgerufene Transaktionen, Verbrauch von Systemressourcen etc.) dürfen ohne Zustimmung des/der betreffenden Mitarbeiters/Mitarbeiterin grundsätzlich nur zu folgenden Zwecken durchgeführt bzw verwendet werden:

- Einhaltung der Bestimmungen des § 14 DSG 2000 zur Datensicherheit;
- Gewährleistung der Systemfunktionalität und Systemsicherheit;
- Analyse und Korrektur von technischen Fehlern im System;
- Optimierung der Rechner- bzw Systemleistung;
- Leistungsverrechnung für den Betrieb der Rechner bzw der Systeme;

- Reaktion auf Fehler- sowie Problemmeldungen der Benuter/innen.[1]

Eine Auswertung der Protokolle im Hinblick auf das Benutzerverhalten einzelner Personen ist untersagt, es sei denn, sie ist im Einzelfall zur Erfüllung der in diesem Punkt genannten Zwecke erforderlich.

4. In begründeten Fällen des Missbrauchs der genannten Systeme oder bei Verdacht der Verletzung gesetzlicher, vertraglicher oder dienstlicher Pflichten durch eine/n Mitarbeiter/in erhält diese/r zunächst die Möglichkeit, sich persönlich zu dem Verdacht zu äußern. Kann die Angelegenheit nicht aufgeklärt werden, so wird unter Beiziehung eines Mitglieds des zuständigen Betriebsrates in die entsprechenden Protokolle Einsicht genommen, es sei denn der betroffene Mitarbeiter/die betroffene Mitarbeiterin lehnt es ab. Die WU hat dabei möglichst schonend vorzugehen und die Einsichtnahme auf den konkreten Verdacht des Missbrauchsfalls zu beschränken.

5. In begründeten Fällen des Missbrauchs der genannten Systeme haben die Betriebsräte das Recht, die Einsichtnahme in die entsprechenden Protokolle zu verlangen. Die davon betroffenen Mitarbeiter/innen sind der Auswertung beizuziehen.

VI. Fernwartung durch Externe und Remote-Zugriffe

1. Für Wartungszwecke kann externen Personen ein kontrollierter Zugang zu den Systemen der WU gewährt werden. Der externe Zugang ist ausschließlich für Wartungszwecke eingerichtet, wobei die WU für diesen Zugriff eine eigene User-ID zur Verfügung zu stellen hat. Alle externen Personen, die mit einer Applikation, in der personenbezogene Daten gespeichert sind, sowohl inhaltlich als auch im Rahmen technischer bzw betriebsrelevanter Aufgaben arbeiten, müssen vor der Aktivierung der entsprechenden Berechtigungen eine schriftliche Datenschutz- und Verschwiegenheitserklärung abgeben. Den Betriebsräten ist auf Verlangen über den Stand der Fernwartungsvereinbarungen Bericht zu erstatten.

2. Remote-Zugriffe auf Endgeräte von Arbeitnehmer/innen sind ausschließlich für eine effiziente Unterstützung im Falle einer Problem- und/oder Fehlerbehebung, für die Erfassung der vorhandenen Hard- und Softwarekomponenten sowie für die Installation von Software zulässig. Zur Aktivierung des Remote-Zugriffes ist vor jedem Zugriff von der/dem jeweiligen Mitarbeiter/in seine/ihre Zustimmung zur Verwendung einzuholen. Die Aktionen im Rahmen des Remote-Zugriffes sind mitzuprotokollieren.

3. Die Weitergabe der im Rahmen von Fernwartungen und/oder Remote-Zugriffen erfassten personenbezogenen Daten darf ausschließlich in anonymisierter oder aggregierter Form erfolgen.

[1] Siehe Erläuterungen zu Punkt V.3.

Ist eine personenbezogene Weitergabe der Daten unbedingt erforderlich, sind die Betriebsräte vor deren Verwendung zu informieren und die Zustimmung des/der jeweiligen Arbeitnehmers/Arbeitnehmerin einzuholen.

VII. Aufbewahrung und Löschung von Daten

Die Aufbewahrungsdauer der Daten richtet sich nach der in Anlage 4 jeweils festgelegten Frist. Die Frist von 4 Wochen für die Protokollspeicherung der Systeme Email, Email Exchange, Novell/Windows Server, WWW/CMS, Radius, Netzwerk und Helpdesk wird ein Jahr nach Inkrafttreten dieser Betriebsvereinbarung durch die Frist von 2 Wochen ersetzt.

VIII. Verhaltenspflichten der Arbeitnehmer/innen

1. Ausdrücklich festgehalten wird, dass jede/r Mitarbeiter/in verpflichtet ist, personenbezogene Daten von Dritten, die ihr/ihm im Zuge der Beschäftigung bei der WU anvertraut oder sonst bekannt oder zugänglich wurden, entsprechend den Bestimmungen des DSG 2000 geheim zu halten und diese nur im Rahmen ihrer/seiner dienstlichen oder gesetzlichen Pflichten zu verwenden. Insbesondere ist eine Übermittlung von Daten an Dritte nur aufgrund einer ausdrücklichen Anordnung eines/einer Vorgesetzten bzw zulässig. Das Datengeheimnis ist auch nach Beendigung des Beschäftigungsverhältnisses zu wahren (§ 15 DSG 2000).

2. Mitarbeiter/innen, die Zugang zu den aufgezeichneten Daten haben, sind hinsichtlich ihrer Geheimhaltungspflichten entsprechend zu belehren; sie haben eine entsprechende Geheimhaltungsverpflichtung zu unterzeichnen.

Wien, am 14.07.2009

Für den Rektor

……..
Vizerektor Univ.-Prof. Dr. Michael Holoubek

Für den Betriebsrat für das
allgemeine Universitätspersonal:

……..
HR Dr. Klemens Honek

Für den Betriebsrat für das
wissenschaftliche Universitätspersonal:

……..
ao. Univ.-Prof. Dr. Peter Berger

Anlage 1:
Systeme, die mit personenbezogenen ArbeitnehmerInnendaten operieren sowie diesbezügliche Zugriffsberechtigungen
Systemadministrator/inn(en) haben per se Zugriff und werden nicht explizit gelistet

System	Beschreibung	Zugriffsberechtigte Einheiten	Autorisierte Person(en)
Evaluierung	Unterstützung der standardisierten Lehrveranstaltungsevaluierung (über Learn@WU). Im System sind die Prozessdaten, Auszählungen und Bilddateien (Scans der offenen Antworten) sämtlicher Lehrveranstaltungsevaluierungen der WU gespeichert.	Vizerektorat für Lehre	Leiter/in Qualitätsmanagement & Program Delivery
BACH - Applikationen	Unterstützung der gesamten Lehr- und Prüfungsverwaltung der WU. Zusätzlich werden auch andere Bereiche der WU Verwaltung abdeckt. ZB Urlaubsverwaltung, Mitarbeiterausweisausstellung, Forschungsdatenbank FIDES etc	STAB, PAB, Studienmanagement, Studienrecht, ZAS, Personal, Forschungsservice, Controlling, Abgeltung der Lehre, Executive Academy, Interne Revision	Bereichs- bzw. Abteilungsleiter/in
SAP-HR/PM-SAP	Personaladministration, Organisationsmanagement, Bewerber/innenverwaltung, Gehaltsverrechnung	Personalabteilung, Abteilung für Personalentwicklung und Personalplanung, Abgeltung für Lehre, Controlling, Personalverrechnung, Interne Revision	Abteilungsleiterin
LV-Access	Abrechnung von Lehr- und Prüfungstätigkeit	Abgeltung der Lehre, Interne Revision	AbteilungsleiterSAP und Sonderprojekte
Email	E-Mails per se, (Inhalt, angefügte Dokumente und Adressdaten), Zugriffsprotokolle und Zugriffsberechtigungen	Benutzer/innen selbst	Abteilungsleiterin IT-Services/ZIS
Email Exchange	E-Mails per se, (Inhalt, angefügte Dokumente und Adressdaten), Zugriffsprotokolle und Zugriffsberechtigungen	Benutzer/innen selbst	Abteilungsleiterin IT-Services/ZIS
Novell/Windows Server	Zentrale Speicherung von Dokumenten, die Benutzer/innen bei Ihrer täglichen Arbeit erzeugen sowie zentrale Druckservices	Benutzer/innen selbst	Abteilungsleiter/in Netzwerk-Telekommunikation (TK/IT-Services) sowie Abteilungsleiter/in Dezentrale Systeme (DZI/IT-Services)
Learn@WU	Personenbezogene Daten	Vizerektorat für	Leiter/in

	sind auf Learn@WU an sich nur auf Studierendenebene gespeichert; ansonsten Lernmaterialien, Inhaltskataloge, Textbücher etc.	Lehre	Qualitätsmanagement & Program Delivery
Telefon + Topcall	Telefonanlagen und Telefon-Server sowie Gebührenabrechnung; Topcall unterstützt Fax- und Voice-Mail-Services		Abteilungsleiter/in Netzwerk-Telekommunikation (TK/IT-Services)
WWW/CMS	Editieren und Publizieren von Web-Seiten auf WU Servern sowie Zugriffsprotokollierung. Betroffen: statische Web-Seiten, im WU-CMS (Typ-A), persönliche und Instituts-Webseiten außerhalb des CMS (Typ-B) sowie dynamische Instituts- und Projekt-Web-Seiten (Typ-C)	Benutzer/innen selbst	Abteilungsleiter IT-Services/IC (für Typ-A) sowie Abteilungsleiterin IT-Services/ZIS (für Typ-B und Typ-C)
Radius	Authentisierung, Autorisierung und Accountverwaltung für Netzwerkzugänge insbesonder ADSL-Zugang, VPN und WLAN		Abteilungsleiter/in Netzwerk-Telekommunikation (TK/IT-Services)
Netzwerk	Zentrale Switches, Router, Paketfilter, Name-Server, DHCP-Server, Wireless-Komponenten und Netzwerk-SysLog-Server		Abteilungsleiter/in Netzwerk-Telekommunikation (IT-Services)
Zentrale Protokollierung	Protokoll-Daten unterschiedlicher Systeme (zB E-Mail-Verkehrsdaten, Logins, System-Logs diverser Server etc.), die auf den zentralen Log-Server geschrieben werden		Abteilungsleiterin IT-Services/ZIS
Helpdesk	Verarbeitung von Supportanfragen von Kund/inn/en und Steuerung der Abwicklung innerhalb der Abteilungen des IT-Services (gegebenenfalls auch unter Einbeziehung externer Dienstleister, zB MCE)	Mitarbeiter/innen IT-Services (InfoCenter, TK, ZIS)	Abteilungsleiter/in Infocenter (IT-Services)
Reservierung von Präsentationsmedien	Verarbeitung von Daten, die im Rahmen des vom IT-Services betriebenen Verleihs von Präsentationsmedien, anfallen	Mitarbeiter/innen IT-Services (InfoCenter)	Abteilungsleiter/in Infocenter (IT-Services)
Dezentrale Rechner/Notebooks	Alle auf lokalen PCs und Notebooks gespeicherten Dokumente	Benutzer/innen selbst	Abteilungsleiter/in Dezentrale Systeme (DZI/IT-Services)
Executive Academy (Website)	Zugangsdaten der berechtigten User/innen	Benutzer/innen selbst	Abteilungsleiter/in IT & eAcademy

	(Mailadresse und verschlüsseltes Passwort), Eventmanagement		
Aleph	Entlehndaten	Bibliothek	Abteilungsleiter/in Bibliothek
Adobe Connect	System zur videounterstützen Zusammenarbeit (Diskussionen, Präsentationen, Abstimmungen etc.)	Benutzer/innen selbst	Abteilungsleiter/in Infocenter (IT-Services)

Anlage 2:
Beispiele für wesentliche Änderungen

Beispiele, die zeigen sollen, ob bei der Einführung bzw Änderungen eines Systems das personenbezogene Daten verarbeitet, der Begriff „wesentlich" zutreffend ist.

- Zutrittskontrolle: Es werden neue Türen mit Zutrittskartenlesern versehen oder es werden Funktionen neu eingeführt oder geändert (zB Änderung der Empfindlichkeitsdistanz der Lesegeräte);
- Videoüberwachung: Es werden zusätzliche Kameras installiert oder neue Funktionen eingeführt oder geändert (zB Änderung des Blickwinkels der Kamera);
- Erweiterung von SAP HR: Es werden zusätzliche Bedienstete von der Datenverwendung betroffen;
- Erweiterung von SAP HR: Entwicklung einer e-Recruiting-Anwendung, über die Bewerber/innen ihre Bewerbungsdaten online eingeben und Attachments (Lebenslauf, Zeugnisse etc) hochladen können, wobei diese Daten in der Folge WU-intern allen in der Hierachie mit der potentiellen Stellenbesetzung Beteiligten zugängig gemacht werden;
- Erweiterung von SAP HR: Implementierung der Self-Service-Funktionalität von SAP HR (Employee Self Service und Management Self Service), die Mitarbeiter/innen und Vorgesetzten die Möglichkeit geben, Verwaltungsabläufe rund um Personalangelegenheiten (zB Antrag auf Dienstzeitänderung, Antrag auf Änderung des Beschäftigungsausmaßes, Anträge auf Karenzierung, Meldung der Geburt von Kindern, Eheschließung, Adressänderung etc) im Selbstbedienungsbetrieb zu erledigen;
- Zeiterfassungssystem: Installation eines elektronischen Systems zur automatisierten Zeiterfassung.

Anlage 3:
Aufstellung, welche personenbezogenen ArbeitnehmerInnendaten außerhalb der gesetzlichen Verpflichtungen an Dritte weitergeleitet werden

Personenbezogene Arbeitnehmer/innen/daten	**Empfängerkreis**
Name (Vorname, Nachname, Titel/akadem. Grad) der jeweiligen versicherten MitarbeiterInnen, Personalnummer, Höhe des einzuzahlenden Betrages, Periode (auf die sich der Betrag bezieht), Polizzennummer	Diverse Versicherungen bezüglich Zukunftssicherung (Uniqa, Generali, Merkur, Wüstenrot, Beamtenversicherung, Wiener Städtische, Sparkassen Versicherung, Niederösterreichische Versicherung, Bawag Versicherung)
Name (Vorname, Nachname, Titel/akadem. Grad) des/der jeweils vom Drittmittelgeber betroffenen Mitarbeiter/s/in, Höhe des Bruttobezuges, Lohnzettel/E 18 Lohnkonten, Eintritts- und Austrittsdatum	Drittmittelgeber sowie von diesen namhaft gemachte Prüfungsinstanzen (Wirtschaftsprüfer, Kontrollamt)
ausschließlich von Beamten/Beamtinnen: Titel, Vor-, Nachname, Geschlecht, Funktion, WU-Anschrift, WU - e-mail-Adresse	Zentralausschuss
Name (Vorname, Nachname, Titel/akadem. Grad) der Mitglieder, Personalnummer, Höhe des Mitgliedbeitrages, Wohnanschrift	GÖD
Name (Vorname, Nachname, Titel/akadem. Grad)	Sodexo (bezüglich Weihnachtsgutscheine)
Name (Vorname, Nachname, Titel/akadem. Grad) der von der Versicherung betroffenen MitarbeiterInnen, Wohnanschrift, Höhe des Beitrages, Personalnummer	BPK

Anlage 4:

Aufbewahrungsdauer der Daten

System	**Aufbewahrungsdauer**
Evaluierung	Einstweilige Speicherdauer 7 Jahre. Da das System Evaluierung ein sehr junges ist und es daher noch wenig Erfahrungswerte zur Aufbewahrungsnotwendigkeit der einzelnen Daten gibt, findet vor Vernichtung der Daten eine erneute Gesprächsrunde zwischen Vertreter/innen der Betriebsräte und der Universitätsleitung statt. In dieser soll anhand der bis dahin gesammelten (Praxis-) Erfahrung nochmals geprüft werden welche Daten kürzer/länger als die 7 Jahre benötigt werden.
BACH - Applikationen	- Die Stammdaten von Mitarbeiter/innen bleiben bis 30 Jahre nach Ausscheiden des/der Mitarbeiter/in in Bach gespeichert (es bleibt dadurch für diesen Zeitraum nachvollziehbar, wer welche LV gehalten hat; wichtig für Zeugnisse etc); - Daten für die Abrechnung externer Lehre werden nach 5 Jahren gelöscht; - ZAS-Kooperationsbeauftragte werden nach 30 Jahren gelöscht; - Die Aufbewahrungsdauer des Mitarbeiterfotos kann von dem/der Mitarbeiter/in selbst bestimmt werden; - Urlaubsanträge werden entsprechend der Verjährungsfrist im Kollektivvertrag nach 3 Jahren gelöscht.
SAP-HR/PM-SAP	Die Daten bleiben während der Dauer des Dienstverhältnisses plus eines Puffers von 10 Jahren in SAP gespeichert. Danach werden sie aus SAP gelöscht und in einem – noch zu implementierenden – Archivierungssystem gespeichert.
LV-Access	Speicherung für 3 Jahre
Email	Datenspeicherung bis 2 Monate ab Deaktivierung der Emailkennung Protokollspeicherung: 4 Wochen, nach einem Jahr 2 Wochen
Email Exchange	Datenspeicherung bis 2 Monate ab Deaktivierung der Emailkennung Protokollspeicherung: 4 Wochen, nach einem Jahr 2 Wochen
Novell/Windows Server	Datenspeicherung bis 2 Monate ab Deaktivierung der Emailkennung Protokollspeicherung: 4 Wochen, nach einem Jahr 2 Wochen
Learn@WU	Wird an die Regelungen der BACH-Applikationen gekoppelt
Telefon + Topcall	Datenspeicherung von intern nach extern: 2

	Monate Datenspeicherung Voicemail/Faxe: 3 Monate
WWW/CMS	Datenspeicherung: Löschung der Daten erfolgt ausschließlich durch die Redakteur/innen Protokollspeicherung: 4 Wochen, nach einem Jahr 2 Wochen
Radius	Datenspeicherung: 2 Monate Protokollspeicherung: 4 Wochen, nach einem Jahr 2 Wochen
Netzwerk	Protokollspeicherung: 4 Wochen, nach einem Jahr 2 Wochen
Zentrale Protokollierung	Protokollspeicherung: 2 Monate (nach 1 Woche nur mehr IT-Services)
Helpdesk	Datenspeicherung unbefristet Auf Wunsch des/der Mitarbeiterin können einzelne Anfragen gelöscht werden Protokollspeicherung: 4 Wochen, nach einem Jahr 2 Wochen
Reservierung von Präsentationsmedien	Datenspeicherung: 1 Semester
Dezentrale Rechner/Notebooks	Nach Rückgabe wird die Festplatte gelöscht
Executive Academy	Website: Datenspeicherung solange Mitarbeiter/innen aktiv sind
Aleph	Datenspeicherung unbefristet Protokollspeicherung: 7 Tage
Adobe Connect	Datenspeicherung: Löschung durch Benutzer Protokollspeicherung: 5 Wochen