

# **RAHMENBETRIEBSVEREINBARUNG**

betreffend  
automationsunterstützte Verwendung personenbezogener ArbeitnehmerInnen Daten

abgeschlossen zwischen der

**Medizinischen Universität Wien**  
als Betriebsinhaber  
vertreten durch den  
Rektor o.Univ.-Prof. Dr. Wolfgang Schütz

sowie dem

**Betriebsrat für das wissenschaftliche Universitätspersonal  
der Medizinischen Universität Wien**

und dem

**Betriebsrat für das allgemeine Universitätspersonal  
der Medizinischen Universität Wien (§ 135 Abs. 3 UG 2002)**

(beide gemeinsam in der Folge auch „Betriebsausschuss“ genannt)

## **I. Allgemeines**

1. Die Medizinische Universität Wien (MUW) setzt verschiedene automationsunterstützte Systeme ein, die personenbezogene Daten von MitarbeiterInnen (ArbeitnehmerInnen im engeren Sinne sowie Beamte des Bundes, die der MUW zur Dienstleistung zugewiesen sind) verwenden. Zum einen sind das Systeme der Personalwirtschaft, zum anderen aber auch personalwirtschaftsfremde Systeme. Die verwendeten Systeme werden von der MUW ausschließlich zur effizienten Abwicklung der Personalverwaltung sowie zur internen und externen Datenkommunikation eingesetzt.

2. Die MUW und der Betriebsausschuss stimmen darin überein, dass die von der MUW eingesetzten Systeme für eine effiziente Personaladministration sowie für die Gewährleistung einer zeitgemäßen internen und externen Kommunikation notwendig und zweckmäßig sind und den berechtigten Interessen der MUW dienen. Einigkeit besteht auch dahingehend, dass elektronische Systeme aufgrund der rasant fortschreitenden technologischen Entwicklung

ständig einem hohen Anpassungs- bzw Aktualisierungsbedarf unterliegen und dass die MUW daher veranlasst ist, diesem dynamischen Wandel entsprechend Folge zu leisten.

3. Die MUW erklärt, dass sie personenbezogene ArbeitnehmerInnendaten nur im gesetzlich vorgeschriebenen Ausmaß verarbeitet und/oder an Dritte übermittelt.
4. Zur einheitlichen Formulierung und Übersichtlichkeit wird auf die in Anlage 1 in Anlehnung an das DSG 2000 angeführte Terminologie verwiesen.

## **II. Geltungsbereich und Regelungsgegenstand**

### **1. Sachlich**

Diese Rahmenbetriebsvereinbarung regelt die automationsunterstützte Verwendung (Verarbeitung sowie Übermittlung im Sinne des § 4 DSG 2000) personenbezogener ArbeitnehmerInnendaten sowie die damit allenfalls im Zusammenhang stehenden Kontrollen. Unter ArbeitnehmerInnendaten sind Daten von MitarbeiterInnen sowie von sonstigen Personen zu verstehen, die in den Betrieb der MUW 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 ArbeitnehmerInnendaten in den entsprechenden Anwendungen bzw. Systemen der MUW.

Die Grundsätze dieser Rahmenbetriebsvereinbarung gelten sinngemäß für alle bestehenden und zukünftigen (Zusatz)Betriebsvereinbarungen, die gemäß den gesetzlich vorgesehenen Bestimmungen auf Basis dieser Rahmenbetriebsvereinbarung abgeschlossen werden und den konkreten Einsatz von Informations- bzw. Kommunikationssystemen beschreiben, bei denen personenbezogene Daten verwendet werden.

### **2. Persönlich und örtlich**

Diese Rahmenbetriebsvereinbarung gilt für alle MitarbeiterInnen (ArbeitnehmerInnen im engeren Sinne einschließlich der von der MUW übernommenen Vertragsbediensteten des Bundes sowie BeamteInnen des Bundes, die der MUW zur Dienstleistung zugewiesen sind) der MUW sowie für sonstige Personen, die in den Betrieb der MUW eingegliedert sind. Nicht

vom Anwendungsbereich erfasst ist insbesondere die Verwendung von PatientInnen- oder Studierendendaten, auch wenn die Daten mit denselben Systemen verarbeitet werden wie die ArbeitnehmerInnendaten.

### **3. Zeitlich**

Diese Rahmenbetriebsvereinbarung tritt mit Unterzeichnung in Kraft und gilt vorerst befristet bis 31.12.2009.

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

Sollte bis sechs Wochen vor Ablauf der Befristung keine Vertragsseite gegenüber der anderen Partei ausdrücklich und schriftlich auf ein Auslaufen der Betriebsvereinbarung mit Fristende bestehen, so verlängert sich diese Betriebsvereinbarung jeweils um weitere zwölf Monate.

## **III. Zielsetzung und rechtliche Grundlagen**

1. Mit dieser Rahmenbetriebsvereinbarung soll sichergestellt werden, dass die MitarbeiterInnen vor einer technisch möglichen Überwachung ihrer Leistung und/oder ihres Verhaltens geschützt werden. Die Betriebsvereinbarung hat dabei zum Ziel, die Nachvollziehbarkeit und Überprüfbarkeit der personenbezogenen ArbeitnehmerInnendatenverwendung für alle gegenwärtig und in Zukunft verwendeten Systeme sicherzustellen und dadurch dem Betriebsausschuss die ihm gemäß den gesetzlichen Grundlagen zustehenden Rechte zu sichern.

2. Die MUW und der Betriebsausschuss sind sich darüber einig, dass die Rahmenbetriebsvereinbarung dazu dient, die Umsetzung von rechtlichen Bestimmungen zur Verhinderung des Datenmissbrauchs oder sonstiger Gesetzesverstöße zu unterstützen.

Ein weiteres Ziel dieser Vereinbarung ist es, die gesetzlichen Erfordernisse nach dem DSGVO 2000 zu erfüllen und dabei eine effiziente und fehlerfreie Datenbewirtschaftung sicherzustellen.

3. 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.

4. Die Rechtsgrundlagen dieser Betriebsvereinbarung sind insbes.:

- a) das Arbeitsverfassungsgesetz (ArbVG),
- b) das ArbeitnehmerInnenschutzgesetz (ANSchG),
- c) das Datenschutzgesetz 2000 (DSG 2000) und
- d) das Telekommunikationsgesetz (TKG)

in der jeweils geltenden Fassung.

#### **IV. Beschreibung der Datenverwendung**

1. Die vorliegende Rahmenbetriebsvereinbarung bezieht sich auf die Verwendung personenbezogener ArbeitnehmerInnendaten der MUW. Der Betriebsausschuss und die Datenschutzkommission (Punkt XI) sind unverzüglich über bestehende und neue Systeme, Systemänderungen oder Systemergänzungen zu informieren. Systeme, die mit personenbezogenen Daten operieren, sind in Anlage 2 aufzulisten; erforderlichenfalls sind Zusatzbetriebsvereinbarungen darüber abzuschließen. Diese Anlage ist bei Systemänderungen oder -ergänzungen in Abstimmung mit der Datenschutzkommission (Punkt XI) zu aktualisieren. Die MUW und der Betriebsausschuss stimmen überein, dass die Systeme ehestmöglich entsprechend der in gegenseitiger Absprache vorgenommenen Priorisierung das in dieser Betriebsvereinbarung festgelegte Prozedere durchlaufen, das unter Punkt XI (2) beschrieben ist.

2. In der Anlage 2 werden auch sämtliche personenbezogenen Standardauswertungen (Reports, etc.) dokumentiert, wobei die Hierarchie des Berechtigungskonzepts und die Bedeutung der standardisierten Auswertungen abzubilden sind. Eine Erweiterung dieser Auswertungen (neue Reports) ist dem Betriebsausschuss und der Datenschutzkommission zur Kenntnis zu bringen und auf Wunsch mit ihnen hierüber zu beraten. In den gesetzlich vorgesehenen Fällen ist vorher die Zustimmung des Betriebsausschusses zu erwirken.

3. SQL-Abfragen, ausgenommen solche betriebstechnischer Natur, werden dokumentiert und an den Betriebsausschuss und die Datenschutzkommission übermittelt. In den gesetzlich vorgesehenen Fällen ist die Zustimmung des Betriebsausschusses zu erwirken.

## V. Umfang der Datenverwendung

1. Personenbezogene ArbeitnehmerInnendaten dürfen – auf Basis der rechtlichen Grundlagen – von der MUW nur im Rahmen dieser Rahmenbetriebsvereinbarung verwendet werden. Erfolgt die Datenverwendung darüber hinaus aus anderen Gründen, ist davon der Betriebsausschuss zu informieren und auf Verlangen mit ihm über die Notwendigkeit und die Art und Weise dieser Datenverwendung zu beraten.

2. Eine Übermittlung von personenbezogenen ArbeitnehmerInnendaten an Dritte darf ohne Zustimmung des/der betroffenen Mitarbeiters/In nur im Rahmen gesetzlicher, kollektivvertraglicher oder standesrechtlicher Verpflichtungen erfolgen. In der regelmäßig zu aktualisierenden Anlage 3 wird jeweils angeführt, welche Daten an welche Institutionen weitergeleitet werden.

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

- Einhaltung der Bestimmungen des § 14 DSGVO 2018 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 Systeme.

Eine Auswertung der Aufzeichnungen der Systemsoftware (Protokolle) im Hinblick auf das BenutzerInnenverhalten einzelner Personen ist untersagt, es sei denn sie ist im Einzelfall zur Fehleranalyse erforderlich. Der Betriebsausschuss ist berechtigt, in begründeten Fällen unter Zuhilfenahme der Systemadministration (ITSC) Einsicht in die Protokolle zu nehmen.

4. Bei begründetem schweren Verdacht des Missbrauchs der genannten Systeme oder bei begründetem schweren 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

entweder auf ausdrücklichen Wunsch des/der Mitarbeiters/In oder aber unter Beiziehung des Betriebsausschusses in die entsprechenden Protokolle Einsicht genommen. Die MUW hat dabei möglichst schonend vorzugehen und die Einsichtnahme auf den konkreten Verdacht des Missbrauchsfalls zu beschränken.

5. In jenen Fällen, in denen die MUW aufgrund einer richterlichen oder verwaltungsbehördlichen Anordnung verpflichtet ist, entsprechende Aufzeichnungen und Auswertungen vorzunehmen oder an diese Stellen Daten von ArbeitnehmerInnen zu übermitteln, ist der Betriebsausschuss zu informieren und mit ihm unbeschadet der richterlichen oder verwaltungsbehördlichen Anordnung über die zu treffenden Maßnahmen zu beraten.

6. Bei der Entwicklung und Wartung von Auswertungsprogrammen muss mit speziellen Simulationsdaten (Testdaten) gearbeitet werden. Falls eine Anonymisierung nicht möglich ist, werden diese Daten wie Echtdaten behandelt.

## **VI. Fernwartung**

Für Wartungszwecke kann ein kontrollierter Zugang installiert werden. Der externe Zugang ist ausschließlich für Wartungszwecke eingerichtet. Diesfalls stellt die MUW eine eigene User-ID für den Zugriff zur Verfügung. Der Zugriff auf die Produktionsinstanz wird nur in begründeten, äußerst dringenden Fällen durch das ITSC freigeschaltet. Alle Personen, die mit einer Applikation, in der personenbezogene Daten gespeichert sind, in inhaltlichen oder in technischen und betriebsrelevanten Aufgaben arbeiten, müssen vor der Aktivierung der entsprechenden Berechtigungen eine Datenschutz- und Verschwiegenheitserklärung unterschreiben.

Dem Betriebsausschuss und der Datenschutzkommission ist über den Stand der Fernwartungsvereinbarungen regelmäßig, mindestens aber einmal jährlich, Bericht zu erstatten.

## **VII. Datenschutz**

1. Die MUW erklärt, bei der Verarbeitung personenbezogener ArbeitnehmerInnen Daten die gesetzlichen Bestimmungen, insbesondere das Datenschutzgesetz (DSG 2000) zu beachten. Insbesondere verpflichtet sich die MUW, personenbezogene ArbeitnehmerInnen Daten wirksam gegen Verlust, Verfälschung und den Zugriff Unbefugter zu sichern. Sämtliche mit der Verwendung von personenbezogenen ArbeitnehmerInnen Daten beschäftigten MitarbeiterInnen der MUW werden hinsichtlich ihrer diesbezüglichen Verpflichtungen bzw. ihrer diesbezüglichen Verantwortlichkeiten belehrt.

2. Sämtliche MitarbeiterInnen, die eine Position bekleiden, welche zur Verwendung von personenbezogenen Daten – außer den eigenen - berechtigt, sind nachweislich auf die Sensibilität personenbezogener Daten, das Bestehen der gegenständlichen Betriebsvereinbarung und die Konsequenzen eines Datenmissbrauchs hinzuweisen.

## **VIII. Löschung und Aufbewahrung von Daten**

Personenbezogene Daten dürfen nur für jene Dauer aufbewahrt werden, die aufgrund rechtlicher, insbesondere steuer- und/oder arbeitsrechtlicher Vorschriften und/oder aufgrund haftungsrechtlicher Gründe notwendig sind. Ist die Aufbewahrung aus betrieblichen Gründen für einen längeren Zeitraum unbedingt erforderlich, sind der Betriebsausschuss und die Datenschutzkommission darüber zu informieren.

## **IX. Information und Kontrollrechte des Betriebsausschusses**

1. Bei wesentlichen Änderungen der bestehenden Systeme (Hard- und/oder Software) sind der Betriebsausschuss und die Datenschutzkommission von der MUW zu informieren, falls es dadurch zu einer wesentlichen Änderung bei der Ermittlung, Verarbeitung oder Übermittlung von personenbezogenen ArbeitnehmerInnen Daten kommen könnte. Der Betriebsausschuss ist dabei vor der Implementierung, d.h. vor der Einführung bzw. Veränderung des Systems in Kenntnis zu setzen und auf Wunsch ist mit ihm hierüber zu beraten. In den gesetzlich vorgesehenen Fällen ist die Zustimmung des Betriebsausschusses zu erwirken.

2. Dem Betriebsausschuss und der Datenschutzkommission sind auf Verlangen Auskünfte und Erläuterungen über die verwendete Hard- und/oder Software zu erteilen, die für die Wahrnehmung der von ihm nach dieser Rahmenbetriebsvereinbarung und aufgrund anderer Rechtsgrundlagen zustehenden Rechte erforderlich sind.

3. Die MUW verpflichtet sich, durch geeignete Maßnahmen die Kontrolle der Einhaltung dieser Rahmenbetriebsvereinbarung durch den Betriebsausschuss zu ermöglichen.

## **X. Datenschutzbeauftragter**

Die MUW hat dem Betriebsausschuss gegenüber eine/n Datenschutzbeauftragte/n (DB) namhaft zu machen. Dem/der DB obliegt die Wahrnehmung insbesondere folgender Aufgaben:

- Überprüfung der Einhaltung der datenschutzrechtlichen Bestimmungen sowie dieser Betriebsvereinbarung;
- Erstellung eines Datenschutzkonzepts;
- Erstellung eines jährlichen Datenschutzreports;
- AnsprechpartnerIn für sämtliche Fragen hinsichtlich der Verwendung personenbezogener ArbeitnehmerInnendaten.

Ist für die Erfüllung der Aufgaben des/der DB die Mitwirkung einzelner Einrichtungen der MUW notwendig, so hat der/die DB das Rektorat über diesen Umstand zu informieren und Vorschläge zur Erfüllung dieser Aufgaben zu unterbreiten.

## **XI. Inneruniversitäre Datenschutzkommission**

1. Zur Beratung aller Fragen, die sich im Zusammenhang mit der Einführung, dem Betrieb und den Änderungen von Informations- und Kommunikationssystemen oder mit Auswertungen ergeben, richtet die MUW eine inneruniversitäre Datenschutzkommission (DK) ein. Die Entscheidungskompetenzen des Rektorats und des Betriebsausschusses gemäß ArbVG bleiben davon unberührt. Die Beratungen und Ergebnisse der DK dienen dem Rektorat und dem Betriebsausschuss als Entscheidungsgrundlagen.

2. Aufgabe der DK ist es, einen Interessenausgleich zwischen Rektorat und Betriebsausschuss herbeizuführen. Die DK ist auch zu befassen wenn bei Fragen im Zusammenhang mit dieser Betriebsvereinbarung keine Einigung erzielt wird. Die DK ist insbesondere vor Änderung oder Einführung von Systemen, die die Verwendung personenbezogener Daten ermöglichen, entsprechend zu informieren. In der Datenschutzkommission ist für die eingesetzten Systeme auch zu klären, bei welchen Daten ein Personenbezug vorliegt.

Bei Planung, Einführung und Adaptierung von Systemen mit personenbezogenen Daten sind folgende Informationen zur Verfügung zu stellen:

- a) Umfassende Projektbeschreibung inkl. allgemein verständlicher Kurzfassung,
- b) Zielsetzung, Zeitplan sowie geplante Auswirkungen des Projekts, insbesondere auf Personalausmaß, Veränderung von Arbeitsabläufen und Arbeitsgestaltung,
- c) technische Systembeschreibung (Hard- und Softwarebeschreibung),
- d) die Verwendungszwecke im Hinblick auf die entsprechenden Datenkategorien,
- e) die SystembenutzerInnen (User) und deren Zugriffsberechtigungen sowie die Benutzerkategorien,
- f) die Systemdokumentation (Programmbezeichnung; im System angebotener und vorgesehener (zu nutzender) Leistungsumfang),
- g) die erfassten Daten,
- h) die Verarbeitungsdokumentation (für standardisierte Verarbeitungen) (Bezeichnung und Beschreibung der Auswertung; Verwendungszweck, Rechtsgrundlage bzw. Auftraggeber; Muster von Bildschirmmasken, Listen, etc.) und
- i) die Schnittstellen (Abfragestatements; Beschreibung des externen Empfängers / Empfängersystems; rechtliche Grundlagen (falls existent); Periodizität)

Wo es sinnvoll erscheint, sollte eine Illustration durch Musterdatensätze erfolgen.

3. Die DK hat auch sensible Daten zu definieren und geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Einhaltung, betreffend die Verwendung von Informations- und Kommunikationssystemen, im Zusammenhang mit den jeweils geltenden gesetzlichen Bestimmungen und dieser Betriebsvereinbarung, überprüfen und sicherstellen zu können.

4. Rektorat und Betriebsausschuss verpflichten sich, im Konfliktfall erst dann den Rechtsweg zu beschreiten, wenn nach Beratung in der DK keine Einigung zustande gekommen ist bzw. ein innerbetrieblicher Schlichtungsversuch erfolglos blieb. Dies wird dann als gegeben angenommen, wenn im Zuge der Beschlussfassung keine Einigung vorliegt oder ein Beschluss innerhalb von zwei Monaten ab der ersten Befassung in der DK nicht zustande gekommen ist.

5. Der DK gehören an:

- vier VertreterInnen des Rektorats (und bis zu vier Ersatzmitglieder) und
- vier VertreterInnen des Betriebsausschusses (und bis zu vier Ersatzmitglieder), wobei der Betriebsrat für das wissenschaftliche Universitätspersonal und der Betriebsrat für das allgemeine Universitätspersonal je zwei VertreterInnen stellen. Den Vorsitz führen abwechselnd für jeweils ein Kalenderjahr ein Mitglied des Betriebsausschusses und ein/e VertreterIn des Rektorats. Im ersten Jahr führt das Mitglied des Betriebsausschusses den Vorsitz.

Der/Die Datenschutzbeauftragte hat das Recht, an allen Sitzungen der DK als nicht stimmberechtigtes Mitglied teilzunehmen und ist nachweislich zu diesen einzuladen.

6. Zur Bewältigung der organisatorischen Abläufe hat die DK eine Geschäftsordnung mit folgendem Mindestinhalt zu beschließen:

- Vorsitzführung
- Protokollführung
- Art der Beschlussfassung
- Art der Einberufung
- Tagungsintervall

Die Konstituierung der DK und die Wahl eines/einer Vorsitzenden sowie eines/einer Stellvertreter/in haben innerhalb von drei Monaten nach Abschluss dieser Betriebsvereinbarung zu erfolgen.

7. Die DK ist beschlussfähig, wenn von Seite des Rektorats zumindest zwei Mitglieder und von Seite der beiden Betriebsräte zumindest je ein Mitglied anwesend sind. Gültige Beschlüsse können nur einstimmig gefasst werden und sind zu protokollieren.

8. Die DK tagt zumindest vierteljährlich. Der/Die Vorsitzende kann darüber hinaus jederzeit bei Bedarf eine Sitzung einberufen. Der/die Vorsitzende hat jedenfalls auf begründetes Verlangen eines Kommissionsmitgliedes binnen fünf Arbeitstagen eine Sitzung einzuberufen.

Jede Einberufung hat eine schriftliche Tagesordnung zu enthalten und ist spätestens zwei Arbeitstage vor der Sitzung allen Kommissionsmitgliedern zu übermitteln.

## **XII. Rechte der Bediensteten, Informationspflichten**

1. Alle MitarbeiterInnen der MUW werden über ihre Rechte und Pflichten in Bezug auf die elektronische Datenverwendung und diese Betriebsvereinbarung informiert.

2. Sind MitarbeiterInnen über die Zulässigkeit einer Verarbeitung oder Übermittlung personenbezogener Daten im Zweifel, sind sie berechtigt, vor Durchführung den Arbeitsauftrag schriftlich zu dokumentieren und bei der DK Informationen einzuholen. Dem/der ArbeitnehmerIn dürfen hierdurch keine Nachteile entstehen.

3. Das Auskunftsrecht sowie das Richtigstellungs- und Löschungsrecht nach DSGVO sind zu beachten.

4. Die MUW wird dafür Sorge tragen, das Bewusstsein der MitarbeiterInnen der MUW hinsichtlich eines sicheren und verantwortungsvollen Umgangs mit elektronischen Medien im Allgemeinen und mit personenbezogenen Daten (insbesondere MitarbeiterInnen-, PatientenInnen- und Studierendendaten) im Besonderen zu fördern. In diesem Zusammenhang wird insbesondere auf die im Internet unter <http://www.meduniwien.ac.at/itsc/policies/richtlinien> abrufbaren Richtlinien (insb Richtlinie 001 für die Verwendung der MUW-UserID sowie Richtlinie 002 für den Anschluss von Rechnern an das Datennetz der MUW in ihrer jeweils gültigen Fassung) hingewiesen, deren Inhalt allen MitarbeiterInnen der MUW gegenüber als Dienstanweisung zu beachten ist. Die Policies-Richtlinien und jede Änderung der Policies-Richtlinien sind dem Betriebsausschuss vorab zu übermitteln und auf Verlangen zu beraten.

5. Ausdrücklich festgehalten wird, dass jede/r MitarbeiterIn verpflichtet ist, personenbezogene Daten von Dritten (insbesondere MitarbeiterInnen-, PatientInnen- und

Studierendendaten), die ihm/ihr im Zuge der Beschäftigung bei der MUW anvertraut oder sonst bekannt oder zugänglich wurden, entsprechend den Bestimmungen des Datenschutzgesetzes 2000 geheim zu halten und diese nur im Rahmen seiner dienstlichen oder gesetzlichen Pflichten zu verwenden. Die MUW verpflichtet sich, die einzelnen MitarbeiterInnen nachweislich über diese Pflichten zu informieren. Insbesondere ist eine Übermittlung von Daten an Dritte nur aufgrund einer ausdrücklichen Anordnung bzw. nach Einholung einer ausdrücklichen Zustimmung der MUW zulässig. Das Datengeheimnis ist auch nach Beendigung des Beschäftigungsverhältnisses zu wahren (§ 15 DSG 2000). Es wird in diesem Zusammenhang darauf hingewiesen, dass eine Verletzung des Datengeheimnisses – neben allfälligen arbeits- bzw. dienstrechtlichen Konsequenzen – insbesondere gem. §§ 51, 52 DSG 2000 eine strafbare Handlung darstellen kann.

Wien, am (...)

Für die Medizinische Universität Wien:

.....

Rektor o.Univ.-Prof. Dr. W. Schütz

Für den Betriebsrat für das  
allgemeine Universitätspersonal:

.....

Für den Betriebsrat für das  
wissenschaftliche Universitätspersonal:

.....

**Anlage /1**  
**Anlage /2**  
**Anlage /3**

## **Anlage 1:**

### **Terminologie in Anlehnung an des DSG 2000 und Kategorien personenbezogener Daten**

A1.a) Informations- und Kommunikationssystem: jedes System (Datenanwendung), das personenbezogene Daten verwendet

A1.b) „Daten“ („personenbezogene Daten“): Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für eine/n AuftraggeberIn, DienstleisterIn oder EmpfängerIn einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, dass diese/r AuftraggeberIn, DienstleisterIn oder ÜbermittlungsempfängerIn die Identität des/der Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;

A1.c) „sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;

A1.d) „Betroffene/r“: jede vom/von der AuftraggeberIn verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden;

A1.e) „AuftraggeberIn“: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hierzu einen anderen heranziehen. Als AuftraggeberIn gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der/die AuftragnehmerIn die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem/der AuftragnehmerIn anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat der/die AuftragnehmerIn die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Landesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 DSG2000 eigenverantwortlich zu treffen, so gilt der/die mit der Herstellung des Werkes Betraute als datenschutzrechtliche/r AuftraggeberIn;

A1.f) „DienstleisterIn“: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden;

A1.g) „Datei“: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;

A1.h) „Datenanwendung“ (früher: „Datenverarbeitung“): die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);

A1.i) „Verwenden von Daten“: jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten als auch das Übermitteln von Daten;

A1.j) „Verarbeiten von Daten“: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den/die AuftraggeberIn oder DienstleisterIn mit Ausnahme des Übermittels von Daten;

A1.k) „Ermitteln von Daten“: das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;

A1.l) „Überlassen von Daten“: die Weitergabe von Daten vom/von der AuftraggeberIn an eine/n DienstleisterIn;

A1.m) „Übermitteln von Daten“: die Weitergabe von Daten einer Datenanwendung an andere EmpfängerInnen als den/die Betroffenen, den/die AuftraggeberIn oder eine/n DienstleisterIn, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des/der Auftraggebers/In;

A1.n) „Informationsverbundsystem“: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere AuftraggeberInnen und die gemeinsame Benützung der Daten in der Art, dass jede/r AuftraggeberIn auch auf jene Daten im System Zugriff hat, die von den anderen AuftraggeberInnen dem System zur Verfügung gestellt wurden;

**Anlage 2:**

**Systeme, die mit personenbezogenen Daten (zu denen auch Photos, Filmmaterial und Evaluierungsergebnisse zählen) operieren.**

**Anlage 3:**

**Daten an Dritte (Welche Institution erhält welche Daten)**