



# IT-Rahmendienstvereinbarung

---

Zwischen

der Otto-Friedrich-Universität Bamberg

und

dem Personalrat der Otto-Friedrich-Universität Bamberg

wird gemäß Art. 73 Abs. 1 in Verbindung mit Art. 75a Abs. 1 des Bayerischen Personalvertretungsgesetzes (BayPVG) in der Fassung der Bekanntmachung vom 11. November 1986 (GVBl 1986, S. 349, BayRS 2035-1-F, das zuletzt durch § 2 des Gesetzes vom 19. Februar 2021 (GVBl. S. 40) geändert worden ist) folgende Dienstvereinbarung über die Planung, Einführung und Anwendung von Systemen der Informationstechnologie (IT-Systemen) sowie über die automatisierte Verarbeitung von Daten der Beschäftigten (nachfolgend: IT-RDV) geschlossen:

## Präambel

Die IT durchdringt alle Tätigkeitsfelder einer Universität und ist in vielen Bereichen Voraussetzung für eine effektive Erfüllung der Aufgaben in Forschung, Lehre und Verwaltung. Sie ist aber nicht als Selbstzweck zu betrachten, sondern soll als Werkzeug dem Wohle der Universität und ihrer Beschäftigten dienen. Dabei sind sowohl die Interessen der Universität als auch der Beschäftigten angemessen zu berücksichtigen. Die vorliegende Vereinbarung legt die Rahmenbedingungen fest, die beim Einsatz von IT-Systemen grundsätzlich gelten. Ziel ist die zeitgemäße Einführung und Weiterentwicklung von IT-Systemen. Wichtigster Grundsatz ist, dass dabei weiterhin eine enge Abstimmung zwischen der Universitätsleitung, der Personalvertretung und der oder dem Datenschutzbeauftragten, soweit personenbezogene Daten verarbeitet werden, erfolgen muss.

## § 1 Geltungsbereich

- (1) Die IT-RDV gilt für alle Beschäftigten (Arbeitnehmerinnen und Arbeitnehmer sowie Beamtinnen und Beamte) der Universität Bamberg.
- (2) Personen, die nicht unter Absatz 1 fallen und die Zugang zu auf den IT-Systemen gespeicherte Daten haben oder denen Zugriff auf die IT-Systeme der Universität Bamberg gewährt wird, sind auf die Einhaltung der Regelungen dieser Dienstvereinbarung zu verpflichten.
- (3) Die IT-RDV gilt für den Einsatz aller IT-Systeme, die in Verbindung mit der IT-Infrastruktur der Universität verwendet werden.

- (4) Falls spezielle datenschutzrechtliche oder mitbestimmungspflichtige Bedingungen es erfordern, kann die Dienstvereinbarung für spezifische IT-Systeme ergänzt und konkretisiert werden.

## § 2 Grundsätze

- (1) Es dürfen keine Profile (z. B. Verhaltens- oder Nutzungsprofile) von Beschäftigten erstellt werden. Eine Verhaltens- oder Leistungskontrolle erfolgt nicht.
- (2) Der Personalrat ist frühzeitig über die Einführung neuer oder grundlegend veränderter IT-Systeme zu informieren. Die Nutzerinnen und Nutzer sind in geeigneter Weise in die Handhabung der IT-Systeme einzuweisen.
- (3) Die Nutzerinnen und Nutzer sind vor den Gefahren der IT zu schützen, soweit dies durch zentrale Maßnahmen gewährleistet werden kann.
- (4) Zugriffsberechtigungen sind entsprechend zu dokumentieren.
- (5) Auf die Nutzungsrichtlinien für Informationsverarbeitungssysteme der Universität Bamberg wird hingewiesen.

## § 3 Datenschutz

- (1) IT-Systeme unterliegen den datenschutzrechtlichen Bestimmungen. Die erteilten Freigaben aller mitbestimmungspflichtigen IT-Systeme können bei der oder dem Datenschutzbeauftragten eingesehen werden.
- (2) Die gespeicherten personenbezogenen Daten dürfen nur für die Zwecke verarbeitet werden, für die sie erhoben wurden.
- (3) Das Grundrecht der informationellen Selbstbestimmung ist zu beachten.
- (4) Die IT-Systeme und deren Daten sind vor unberechtigtem Zugriff zu schützen.
- (5) Verantwortliche Stellen, insbesondere Systemadministratorinnen und Systemadministratoren, dürfen die auf den IT-Systemen gespeicherten Daten nur dann einsehen, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Eine darüberhinausgehende Übermittlung oder Nutzung ist nicht zulässig. Gleiches gilt sinngemäß auch für alle anderen Nutzerinnen und Nutzer.
- (6) Es erfolgt kein Austausch personenbezogener Daten zwischen unterschiedlichen IT-Systemen, außer wenn dies zur Erfüllung der Aufgaben notwendig und datenschutzrechtlich freigegeben ist oder zu Zwecken der Benutzerverwaltung und Authentisierung dient.
- (7) Zugriff über eine Fernwartungssoftware darf nur nach der direkten Zustimmung des betroffenen Beschäftigten erfolgen.

## § 4 Datennutzung

- (1) Jedem Mitglied der Universität Bamberg wird durch das Identity- und Accessmanagement (nachfolgend: IAM) eine eindeutige digitale Identität zugeordnet. Das IAM bezieht die Daten zur Person aus IT-Systemen (beispielsweise Personalsystem, Organisationsmanagement), bei denen die Daten zur Person primär erfasst werden.
- (2) Die IT-Systeme werden zur dienstlichen Aufgabenerfüllung zur Verfügung gestellt.
- (3) Es ist jede Datennutzung zu unterlassen, die geeignet ist, den Interessen der Universität Bamberg oder deren Ansehen in der Öffentlichkeit zu schaden, die Sicherheit der IT-Systeme zu beeinträchtigen oder die gegen geltende Rechtsvorschriften und die Nutzungsrichtlinie für Informationsverarbeitungssysteme verstößt.
- (4) Die private Nutzung der IT-Systeme ist lediglich in untergeordnetem Umfang geduldet, soweit die dienstlichen Belange, insbesondere die Arbeitszeit, nicht beeinträchtigt werden. Mit der privaten Nutzung willigt die Nutzerin und der Nutzer ein, dass die private Nutzung von der Universität Bamberg in gleicher Weise wie die dienstliche Nutzung behandelt wird.

## § 5 Personenbezogene und aufgabenbezogene Dienste

- (1) Es wird grundsätzlich zwischen personenbezogenen und aufgabenbezogenen Diensten unterschieden.
- (2) Für die Wahrnehmung der dienstlichen Aufgaben, für die eine Vertretung bei Abwesenheiten (Urlaub, Dienstreise, Krankheitsfall usw.) gewährleistet sein muss, sind grundsätzlich sogenannte aufgabenbezogene Dienste (z. B. Fileserver, E-Mail-Adressen) zu verwenden.
- (3) Personenbezogene Dienste dienen der Verarbeitung von Informationen, die eine einzelne Person und deren persönliches Dienstverhältnis zur Universität betreffen (z. B. Schriftverkehr einer oder eines Bediensteten mit der Personalverwaltung oder dem Personalrat, Abrechnungsunterlagen über private Telefongespräche, Informationen über die Gesundheit).
- (4) Aufgabenbezogene Dienste fallen im Rahmen der Erfüllung einer Aufgabe aus dem Tätigkeitsbereich einer Einrichtung an. Aufgabenbezogene Informationen enthaltende Daten sind zur Erfüllung einer Aufgabe der Einrichtung erforderlich. Der Zugang zu aufgabenbezogenen Daten wird deshalb in der Regel mehreren Personen gewährt, um die Aufgabenerfüllung in der Gruppe sowie im Vertretungsfall zu ermöglichen. Über die Zugangsberechtigung entscheiden die Leiterin oder der Leiter der Einrichtung, deren Aufgaben zu erfüllen sind.
- (5) Im Rahmen der personenbezogenen Dienstenutzung anfallende Daten dürfen nicht auf aufgabenbezogene Speicherbereiche gespeichert werden, da dort keine auf eine Person bezogene Vertraulichkeit besteht.

- (6) Aufgabenbezogene Daten dürfen nicht auf personenbezogene Speicherbereiche gespeichert werden, da sonst andere mit der Erfüllung der Aufgabe betraute Personen nicht auf die Daten zugreifen können.
- (7) Die Einsichtnahme der Leiterin oder des Leiters der Einrichtung in Datenbestände, die im Rahmen einer aufgabenbezogenen Nutzung angefallen sind, richtet sich nach dem Grundsatz der aufgaben- und zuständigkeitsbezogenen Berechtigung und Verantwortung. Insbesondere stehen jeder Zugriffsebene nur solche Daten zur Verfügung, die zur Wahrnehmung ihrer Aufgaben benötigt werden.

## § 6 Protokollierung

- (1) Die Nutzung der IT-Dienste darf ausschließlich zu folgenden Zwecken protokolliert werden:
  - a. Herstellung der Betriebssicherheit und Integrität der Systeme,
  - b. Nachweis über die Einhaltung der datenschutzrechtlichen Bestimmungen,
  - c. technische Fehlersuche in den Systemen,
  - d. Sicherstellung und Aufrechterhaltung der Betriebsbereitschaft der Systeme, insbesondere der Datensicherung
  - e. zu Abrechnungszwecken.
- (2) Die mit Auswertungen befassten Personen werden über ihre Pflichten aus dieser IT-RDV belehrt. Außerdem werden sie hingewiesen auf ihre Pflicht zur Verschwiegenheit und mögliche arbeits- und strafrechtliche Konsequenzen bei Verstößen. Die Belehrung auf den Datenschutz erfolgt in Schriftform und wird von den Beschäftigten mit Unterschrift gegengezeichnet.
- (3) Der Umgang mit systemimmanent anfallenden Daten in bestimmten Anwendungen, die über eine Protokollierung hinausgehen, wird in der Verarbeitungstätigkeitsbeschreibung nach dem Bayerischem Datenschutzgesetz (BayDSG) in der Fassung der Bekanntmachung vom 15. Mai 2018 (GVBl. S. 230, BayRS 204-1-I, das zuletzt durch § 6 des Gesetzes vom 18. Mai 2018 (GVBl. S. 301) geändert worden ist) oder speziellen Regelungen für solche Anwendungen festgelegt.

## § 7 Schlussbestimmungen

- (1) Diese Dienstvereinbarung tritt mit ihrer Bekanntgabe in Kraft.
- (2) Diese Dienstvereinbarung kann von beiden Seiten mit einer Frist von 3 Monaten gekündigt werden.
- (3) Einvernehmliche Änderungen der Dienstvereinbarung sind jederzeit möglich.
- (4) Die Dienstvereinbarung über den Betrieb der Telekommunikationsanlage Siemens Hicom 300 (ISDN-Kommunikationssystem) vom 24.09.1996 tritt außer Kraft.



- (5) Nach einer Kündigung der Dienstvereinbarung gilt bis zum Abschluss einer neuen Dienstvereinbarung diese weiter. Die Universitätsleitung Bamberg und der Personalrat verpflichten sich, nach Eingang der Kündigung unverzüglich Verhandlungen über eine neue Dienstvereinbarung aufzunehmen.

Bamberg, den 1. Juli 2021

*Ua. Fischbach* / *D. Steuer-Flieser* *Franziska Stahl*

Prof. Dr. Fischbach

Dr. Steuer-Flieser

Stahl

Präsident

Kanzlerin

Vorsitzende des Personalrats