



IT-Rahmendienstvereinbarung (IT-RDV)

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 § 5 des Gesetzes vom 23. Juni 2023 (GVBl. S. 251) und § 1 des Gesetzes vom 7. Juli 2023 (GVBl. S. 318) 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, dem Personalrat und dem oder der 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 gespeicherten Daten haben und 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 Verhaltens- oder Nutzungsprofile von Beschäftigten erstellt werden.
- (2) Daten, die für eine Verhaltens- und Leistungskontrolle geeignet sind, werden nicht dafür genutzt, das Verhalten oder die Leistung von Beschäftigten zu beobachten, zu messen, zu beurteilen, zu vergleichen oder auf andere Weise zu kontrollieren. Eine Ausnahme davon gilt nur
 - a. bei Anfragen von Strafverfolgungsbehörden zum Zweck der Sachverhaltsaufklärung sowie
 - b. bei konkreten, tatsächengestützten Verdachtsfällen auf Dienstpflichtverletzungen, insb. Verstöße gegen die Nutzungsrichtlinien für Informationsverarbeitungssysteme der Universität Bamberg sowie gegen Vorgaben dieser IT-Rahmendienstvereinbarung,sofern eine Sachverhaltsaufklärung mit mildereren Mitteln nicht zu erreichen ist. Der Personalrat sowie die bzw. der Datenschutzbeauftragte sind mit einer Vorlaufzeit von mindestens 24 Stunden unter Angabe der dokumentierten Anhaltspunkte in Textform über eine beabsichtigte Auswertung technischer Einrichtungen zu informieren; ihnen ist Gelegenheit zu geben, an der Auswertung teilzunehmen.
- (3) Der Personalrat ist frühzeitig über die Einführung neuer oder grundlegend veränderter IT-Systeme zu informieren. Die Nutzerinnen bzw. Nutzer sind in geeigneter Weise in die Handhabung der IT-Systeme einzuweisen.
- (4) Die Nutzerinnen bzw. Nutzer sind vor den Gefahren der IT zu schützen, soweit dies durch zentrale Maßnahmen gewährleistet werden kann.
- (5) Zugriffsberechtigungen sind entsprechend zu dokumentieren.
- (6) Auf die Nutzungsrichtlinien für Informationsverarbeitungssysteme der Universität Bamberg wird hingewiesen.

§ 3 Datenschutz

- (1) IT-Systeme unterliegen den datenschutzrechtlichen Bestimmungen.
- (2) Die gespeicherten personenbezogenen Daten dürfen nur für die Zwecke, für die sie erhoben worden sind, sowie im Rahmen zulässiger Zweckänderungen verarbeitet werden.
- (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 Systemadministratoren, dürfen die auf den IT-Systemen gespeicherten Daten nur dann einsehen, wenn dies zur Erfüllung ihrer Aufgaben

erforderlich ist. Eine darüber hinausgehende Verarbeitung, insbesondere Übermittlung, 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 erforderlich und datenschutzrechtlich zulässig ist.
- (7) Zugriff über eine Fernwartungssoftware darf nur nach der direkten Zustimmung des betroffenen Beschäftigten erfolgen.

§ 4 Systemnutzung

- (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 universitären Nutzungsrichtlinien 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 bzw. der Nutzer ein, dass die private Nutzung von der Universität Bamberg in gleicher Weise wie die dienstliche Nutzung behandelt wird.

§ 5 Aufgabenbezogene und personenbezogene Dienste

- (1) Es wird grundsätzlich zwischen aufgabenbezogenen und personenbezogenen Diensten unterschieden.
- (2) Für die Wahrnehmung der dienstlichen Aufgaben und die damit verbundene Speicherung aufgabenbezogener Daten sind grundsätzlich aufgabenbezogene Dienste (z. B. hinsichtlich Fileserver, E-Mail-Adressen) zu verwenden, damit insbesondere bei Abwesenheiten (wegen Urlaub, Dienstreise, Krankheit, Austritt usw.) der Datenzugriff durch die Vertretung gesichert ist. Der Zugang zu aufgabenbezogenen Diensten wird zudem in der Regel mehreren Personen parallel gewährt, um die Aufgabenerfüllung in der Organisationseinheit sicherzustellen. Über die Zugangsberechtigung entscheiden die Leiterin bzw. der Leiter der Organisationseinheit. Aufgabenbezogene Daten dürfen nicht auf personenbezogenen Speicherbereichen abgelegt werden, da sonst andere mit der Erfüllung der Aufgaben betraute Personen nicht auf die Daten zugreifen können.

- (3) Personenbezogene Dienste dienen der Verarbeitung von Informationen und Daten, die einen selbst bzw. das persönliche Dienstverhältnis zur Universität betreffen (z. B. Schriftverkehr einer oder eines Bediensteten mit der Abteilung Personal oder dem Personalrat). Die im Rahmen der personenbezogenen Nutzung anfallenden Daten sollen nicht auf aufgabenbezogenen Diensten gespeichert werden, da dort keine auf eine einzelne Person bezogene Vertraulichkeit besteht.
- (4) Die Einsichtnahme der Leiterin bzw. des Leiters der Organisationseinheit 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 jeweiligen Aufgaben benötigt werden.
- (5) Die Einsichtnahme in Datenbestände, die in personenbezogenen Diensten, in Nutzerprofilen oder in lokalen, benutzerbezogenen Verzeichnissen enthalten sind, ist bis auf die Fälle des § 2 Abs. 2 grundsätzlich nicht gestattet. Eine Ausnahme kann im Einzelfall (z. B. bei längerfristiger Arbeitsverhinderung, nach Austritt oder im Todesfall) gestattet sein, sofern Anhaltspunkte vorliegen, dass aufgabenbezogene Informationen auf personenbezogenen Diensten gespeichert wurden und die Einsichtnahme in diese Daten zur Aufrechterhaltung des Dienstbetriebs erforderlich ist. Die Zustimmung des Personalrats sowie der bzw. des Datenschutzbeauftragten ist einzuholen. Diesen ist zudem Gelegenheit zu geben, an der Einsichtnahme teilzunehmen, um sicherzustellen, dass sich die Einsichtnahme auf das zwingend erforderliche Maß und diejenigen Nachrichten beschränkt, die nicht offensichtlich als privat erkennbar sind. Die jeweiligen Dienstvorgesetzten sind zu informieren.

§ 6 Protokollierung

- (1) Die Nutzung der IT-Dienste darf ausschließlich zu folgenden Zwecken im Rahmen der Erforderlichkeit protokolliert werden:
 - a. Herstellung und Aufrechterhaltung der Vertraulichkeit, Verfügbarkeit und Integrität der Systeme,
 - b. Sicherheit der Datenverarbeitung nach Maßgabe des Datenschutzes,
 - c. Erfüllung datenschutzrechtlicher Melde- und Benachrichtigungspflichten,
 - d. Nachweis über die Einhaltung datenschutzrechtlicher Bestimmungen,
 - e. technische Fehlersuche in den Systemen,
 - f. Betrugsbekämpfung sowie Aufdeckung von Dienstvergehen und Straftaten,
 - g. Lizenzinventarisierung und -bewirtschaftung sowie
 - h. Abrechnungszwecke.
- (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 Bestätigung über die erfolgte Belehrung ist zu dokumentieren.

§ 7 Schlussbestimmungen

- (1) Diese Dienstvereinbarung tritt mit ihrer Bekanntgabe in Kraft.
- (2) Diese Dienstvereinbarung kann von beiden Seiten mit einer Frist von drei Monaten gekündigt werden.
- (3) Einvernehmliche Änderungen der Dienstvereinbarung sind jederzeit möglich.
- (4) 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 4.05.2026

Handwritten signature of Prof. Dr. Fischbach in blue ink.

Prof. Dr. Fischbach
Präsident

Handwritten signature of Dr. Steuer-Flieser in blue ink.

Dr. Steuer-Flieser
Kanzlerin

Handwritten signature of Dr. Depietri in blue ink.

Dr. Depietri
Vorsitzender des Personalrats