RUHR-UNIVERSITÄT BOCHUM

RUB

NR. 1273 | 08.10.2018

AMTLICHE BEKANNTMACHUNG

Rahmen-Dienstvereinbarung über Einführung und Anwendung von Systemen der Informationstechnik (IT)

vom 20.08.2018

Rahmen-Dienstvereinbarung über Einführung und Anwendung von Systemen der Informationstechnik (IT)

zwischen dem
Personalrat der Ruhr-Universität Bochum, vertreten durch den Vorsitzenden, und der Ruhr-Universität Bochum, vertreten durch die Kanzlerin,

sowie zwischen dem
Personalrat der wissenschaftlich/künstlerisch Beschäftigten der Ruhr-Universität Bochum, vertreten durch den Vorsitzenden, und der Ruhr-Universität Bochum, vertreten durch den Rektor

wird gemäß § 70 Personalvertretungsgesetz für das Land Nordrhein-Westfalen (Landespersonalvertretungsgesetz - LPVG NW -) folgende Dienstvereinbarung abgeschlossen:

§ 1
Ziele

(1) Hochschulleitung und Personalräte der Ruhr-Universität Bochum sind sich darin einig, dass ein zukunftsorientierter Einsatz von IT-Technologien dem Wohle der gesamten Hochschule zu dienen hat. Dieses Ziel kann nur erreicht werden, wenn Hochschulleitung, Personalräte und Beschäftigte gleichermaßen die Anwendung neuer Technologien mittragen und mitgestalten.

(2) Dazu ist es notwendig,
- dass die Personalräte und die betroffenen Beschäftigten konstruktiv und qualifiziert in Entscheidungs- und Gestaltungsprozesse einbezogen werden,
- dass die Beschäftigten vor Gefahren und negativen Auswirkungen geschützt werden,
- dass rechnergestützte Systeme als Instrumente zur Unterstützung menschengerechter Arbeit auszulegen sind, insbesondere der Mensch nicht auf die Systembedienung reduziert wird,
- dass Grundrechte der Person, vor allem die "informationelle Selbstbestimmung", volle Berücksichtigung finden.

(3) Diese Vereinbarung dient dazu, Grundsätze, Regelungswege und Beteiligungsinstrumente festzulegen, die eine zügige, unbürokratische und von den Personalvertretungen sowie von den Beschäftigten mitgetragene IT-Entwicklung sichern.

§ 2
Geltungsbereich und Begriffsbestimmungen

(1) Diese IT-Rahmendienstvereinbarung gilt
- persönlich für Beschäftigte der Ruhr-Universität Bochum im Sinne der §§ 5 und 104 LPVG NW. Die Dienststelle verpflichtet sich, die Regelungen dieser Dienstvereinbarung auch auf die Beschäftigten anzuwenden, die nicht von Personalräten vertreten werden.
- sachlich für die Einführung, Anwendung und Erweiterung von IT-Systemen, die von der Mitbestimmung nach dem LPVG NRW betroffen sind.

(2) IT-Systeme im Sinne dieser Vereinbarung sind Technologien der Informationstechnik, mit denen Daten aus Prozessen in Verwaltung, Lehre und Forschung der Universität erfasst, gespeichert und verarbeitet werden. Im Übrigen gelten die Begriffsbestimmungen des Datenschutzgesetzes Nordrhein-Westfalen.

§ 3
Grundsätze

(1) IT-Systeme werden mit dem Ziel eingeführt und angewendet, die Effizienz und die Qualität der Arbeits- und Geschäftsprozesse zu erhöhen. Dabei sind Gesichtspunkte der Anwenderfreundlichkeit zu berücksichtigen, z.B. bei Zugangssicherungen.

(2) Mitarbeiterinnen und Mitarbeiter werden bei der Planung, Einführung und Anwendung von IT-Systemen, die sie betreffen, beteiligt.

(3) Bei der Einführung und Anwendung von IT-Systemen ist sicherzustellen, dass die Qualifikation der Beschäftigten gesichert und gefördert wird, ohne dass sich hierdurch Über- oder Unterforderungen ergeben. Die Arbeiten werden in ganzheitlichen, von den Beschäftigten als sinnvoll und zusammengehörend empfundenen Abläufen organisiert und so gestaltet, dass der Wechsel zwischen IT-unterstützter und IT-freier Tätigkeit möglich ist und von den Beschäftigten selbst bestimmt werden kann (Mischarbeitsplätze). Soziale Kontakte und Entscheidungsspielräume sollen erhalten werden.

(4) Mitarbeiterinnen und Mitarbeiter, deren Aufgaben wegfallen, erhalten andere, mindestens gleichwertige und zumutbare Aufgaben. Sie werden hierfür entsprechend qualifiziert.

(5) Personenbezogene und -beziehbare Daten dürfen nicht zu Zwecken einer Verhaltens- oder Leistungskontrolle und nicht für dienstliche Beurteilungen oder Disziplinarmaßnahmen oder als Grundlage für Feststellung des Gesundheitszustandes genutzt werden. Eine Auswertung der Daten mit dem Ziel dienstrechtlicher Konsequenzen ist unzulässig.

(6) Daten, welche als Nebenprodukt des IT-Systems anfallen (z.B. aus Log- oder Account-Prozeduren) werden nur zu Zwecken der Datenschutzkontrolle, der Datensicherung (im Sinne der Datensicherheit) oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage verarbeitet und gespeichert. Sie sind soweit möglich zu anonymisieren bzw. zu pseudonymisieren und zu löschen, sowie sie nicht mehr benötigt werden. Alle übrigen personenbezogenen und -beziehbaren Daten dürfen, soweit für ihre Verarbeitung ein Mitbestimmungsrecht gegeben ist, nur für Zwecke erhoben, gespeichert und weiterverarbeitet werden, die in einer Einzeldienstvereinbarung festgelegt worden sind.

(7) Zentrale Aspekte der Administration von IT-Systemen werden in der angefügten Anlage als Teil dieser Dienstvereinbarung beschrieben.

§ 4
Rechte der Beschäftigten

(1) Jede Mitarbeiterin und jeder Mitarbeiter erhält auf Wunsch schriftliche Informationen über alle in einem IT-System zu ihrer/seiner Person aktuell gespeicherten Daten. Dazu werden alle genutzten Datenspeicher mit ihrem aktuellen Inhalt, dem Verwendungszweck jedes Speichers, die Speicherdauer und die Adressaten außerhalb der Dienststelle angegeben.

(2) Unzulässig gespeicherte Daten sind aus allen Speichern zu löschen. Falsche Daten sind zu berichtigen. Ist die Richtigkeit strittig, so sind sie zu sperren. Kann die Dienststelle die Richtigkeit einzelner Daten nicht nachweisen, so sind die Daten zu löschen. Die betroffenen Mitarbeiterinnen und Mitarbeiter sind über diese Änderungen zu informieren. Beschäftigte sind verpflichtet, die für den Nachweis der Richtigkeit erforderlichen und in ihrem Besitz befindlichen oder nur von ihnen zu beschaffenden Unterlagen unverzüglich der Dienststelle vorzulegen.

(3) Personelle Maßnahmen, die auf Informationen beruhen, die unter Verletzung dieser Rahmendienstvereinbarung oder der sie ergänzenden Einzeldienstvereinbarungen gewonnen wurden, sind unwirksam und rückgängig zu machen. Liegt ein Verdacht auf Verletzung vor, hat die Dienststelle dem Personalrat auf dessen Anforderung alle den Sachverhalt betreffende Informationen und Unterlagen umfassend und schriftlich zur Verfügung zu stellen.

§ 5
Aus- und Weiterbildung

(1) Die Mitarbeiterinnen und Mitarbeiter, die mit IT-Systemen arbeiten, werden vorab angemessen, dem System, der Aufgabenstellung und den persönlichen Voraussetzungen entsprechend geschult und eingearbeitet. Darüber hinaus findet eine laufende Betreuung am Arbeitsplatz, insbesondere durch die Supportbereiche der jeweiligen Systeme statt.

(2) Rechtzeitig vor der Durchführung von Schulungen ist dem zuständigen Personalrat ein Konzept vorzulegen. Hierin sind mindestens die Lernziele, Lerninhalte, zeitlicher Umfang, Dozenten/innen, Teilnehmer/innen, Termine und Orte der Bildungsmaßnahmen enthalten.

(3) Mitglieder der Personalräte sind berechtigt, zur Wahrnehmung ihrer Aufgaben aus dieser Rahmendienstvereinbarung und den ergänzenden Einzeldienstvereinbarungen an Weiterbildungsveranstaltungen zu den hier geregelten Themen teilzunehmen. Die Kosten trägt die Dienststelle.

§ 6
Rechte der Personalräte

(1) Die Personalräte und der behördliche Datenschutzbeauftragte (bDSB) haben das Recht, die Einhaltung dieser Rahmendienstvereinbarung und der ergänzenden Einzeldienstvereinbarungen zu überprüfen und dazu Stichproben zu machen. Zu diesem Zweck ist ihnen im Rahmen der gesetzlichen Möglichkeiten der erforderliche Zugang zu allen Stellen zu gewähren, an denen Daten der IT-Systeme erhoben, verarbeitet und/oder genutzt werden. Die Personalräte können erforderlichenfalls dazu externe Sachverständige ihrer Wahl hinzuziehen. Unter Beachtung der sparsamen Haushaltsführung werden die Kosten hierfür von der Dienststelle getragen. Die Personalräte können auf allen Ebenen der Systeme (Betriebssysteme, Datenbanksysteme, Kommunikationssysteme, Protokolle) die vereinbarte Verwendung und die Einhaltung des Datenschutzes kontrollieren. Dazu können sie auch in alle von den Systemen gespeicherten Daten und Protokolle Einblick nehmen. Alle zu den Systemen gehörenden Handbücher und Systemunterlagen sind ihnen auf Wunsch zu überlassen.

(2) Die Personalräte haben das Recht, alle Personen, die mit der Verarbeitung und Nutzung von Daten der IT-Systeme beschäftigt sind, bezüglich der rechtmäßigen und vereinbarten Verwendung zu befragen. Diese sind gegenüber den Personalräten zur Auskunft berechtigt. Auf Verlangen haben sie Funktionen auf der Ebene der Betriebssysteme und Datenbankanwendungen zu Prüfzwecken durchzuführen. Auf Wunsch werden für die Personalräte Ausdrucke erzeugt.

§ 7
Datenschutz / IT-Sicherheit

(1) Die Dienststelle gewährleistet die organisatorischen und technischen Maßnahmen, die die im Landesdatenschutzgesetz geforderten Ziele sicherstellen. Alle Beteiligten sind angehalten, die durch die Leitlinie zur Informationssicherheit der Ruhr-Universität vorgegebenen Regelungen einzuhalten.

(2) Bei der Ermittlung von Ursachen für das Versagen von IT-Sicherheitssystemen sind die Personalräte zu beteiligen.

§ 8
Regelungswege

(1) Die Personalräte sind im Sinne einer prozessbegleitenden Mitbestimmung an IT-bezogenen Überlegungen und Planungen zu beteiligen. Informationen haben so rechtzeitig zu erfolgen, dass Alternativlösungen noch realistisch berücksichtigt werden können, d.h., bevor sich die Dienststelle gegenüber Dritten bereits verbindlich festlegt. In den Diskussionsprozess sind auch Systemalternativen sowie absehbare personelle und arbeitsorganisatorische Auswirkungen einzubeziehen.

(2) Ziel der Mitbestimmung sind systembezogene Einzeldienstvereinbarungen. IT-Systeme dürfen grundsätzlich erst nach dem jeweiligen Abschluss solcher Vereinbarungen genutzt werden. Erprobungsläufe sind nach einvernehmlicher Vereinbarung möglich. Wird Einvernehmen darüber hergestellt, dass zu einem IT-System eine Einzeldienstvereinbarung nicht nötig ist, ist dies – ggf. unter Angabe von Bedingungen – zu protokollieren.

(3) IT-Systeme sind dann erneut dem IT-Ausschuss vorzulegen, wenn wesentliche Anwendungsänderungen vorgenommen werden sollen, insbesondere dann, wenn sie eine Ausweitung des betroffenen Personenkreises oder der erfassten Daten, maßgebliche Veränderungen von Arbeitsabläufen und -inhalten oder Veränderungen von Arbeitsplatzbeschreibungen und -bewertungen zur Folge haben. Als unwesentliche Änderungen sind z. B. anzusehen:
- Updates/Releasewechsel ohne neue wesentliche Funktionalitäten,
- Hardwarewechsel ohne wesentliche Auswirkungen auf Arbeitsabläufe, -inhalte etc.,
- Anwendungen, die ausschließlich dem Betrieb der IT- Systeme dienen (z.B. Betriebssysteme und betriebssystemnahe Software).

§ 9
IT-Ausschuss

(1) Der IT-Ausschuss ist das Gremium, über das die Beteiligung der Personalräte in IT-Angelegenheiten im Geltungsbereich dieser Dienstvereinbarung realisiert wird. Er ist Ausdruck der vertrauensvollen Zusammenarbeit zwischen Dienststelle und Personalräten.

(2) Im IT-Ausschuss werden Einzeldienstvereinbarungen mit dem Ziel der Einigung erarbeitet und Verhandlungen darüber geführt, ob Einzeldienstvereinbarungen nötig sind.

(3) Der IT-Ausschuss hält Meinungsbilder fest und spricht Empfehlungen aus. Hochschulleitung sowie Personalräte erklären innerhalb eines Monats, ob sie diese Empfehlung anerkennen. Hat die Empfehlung des IT-Ausschusses den Charakter einer Einzeldienstvereinbarung, so wird diese Bestandteil dieser Rahmendienstvereinbarung. Im Falle der Ablehnung der Empfehlung des IT-Ausschusses kann ein Mitbestimmungsverfahren nach § 66 LPVG NRW eingeleitet werden.

(4) Der IT-Ausschuss berät über Erfahrungen und Beschwerden im Zusammenhang mit IT-Systemen. Dazu berichtet die Dienststelle regelmäßig über angestrebte Maßnahmen und beschreibt technische und organisatorische Änderungen und Weiterentwicklungen.

(5) Der IT-Ausschuss setzt sich paritätisch aus folgenden stimmberechtigten Mitgliedern zusammen:
- 4 Mitglieder der Dienststelle,
- je 2 Mitglieder der Personalräte.

Beratende Mitglieder sind der behördliche Datenschutzbeauftragte, ein Vertreter des Nutzerrates von IT.SERVICES und ein Vertreter der Stabsstelle für Informationssicherheit. Auf Wunsch eines der Mitglieder nach Satz 1 kann der IT-Ausschuss Gäste hinzuziehen.

§ 10
Einzeldienstvereinbarungen

(1) Einzeldienstvereinbarungen enthalten, bezogen auf das jeweilige IT-System, die folgenden Inhalte:
- Systembeschreibung;
- Aussagen zum Umgang mit personenbezogenen Daten, zum Berechtigungskonzept und zur Vernetzung mit anderen Systemen. Gegebenenfalls reichen Verweise auf Dokumente, die gemäß der Datenschutzgrundverordnung erstellt worden sind (z.B. Verfahrensverzeichnis, Dokumentation zur Notwendigkeit einer Datenschutzfolgenabschätzung, Datenschutzfolgenabschätzung);
- Zweckbestimmungen;
- Systemspezifische und ergänzende Regelungen;
- Unterschiften der Dienststelle und der Personalräte;
- Gültigkeitsvermerke.

(2) Einzeldienstvereinbarungen werden als fortlaufender Anhang zur dieser Dienstvereinbarung dauerhaft dokumentiert und für die Beschäftigten online zur Verfügung gestellt. In diese Dokumentation sind auch die Protokollnotizen nach § 8 Abs. 2 aufzunehmen. Sie sind einzeln kündbar, ohne dass damit die Rahmenvereinbarung als gekündigt gilt.

(3) Falls Anlagen von Dienstvereinbarungen oder sonstige Regelungen im Widerspruch zu einer Dienstvereinbarung stehen, gilt der Text der Dienstvereinbarung.

§ 11
Inkrafttreten, Laufzeit

Die vorstehende Dienstvereinbarung tritt am Tag der Unterzeichnung in Kraft und ersetzt die Rahmen-Dienstvereinbarung über Einführung und Anwendung von Systemen der Informationstechnik (IT) vom 26. Juni 2009. Sie kann mit einer Frist von 6 Monaten gekündigt werden. Im Falle einer Kündigung gilt die Nachwirkung als vereinbart.

Bochum, den 20.08.2018

für die Dienststelle:

Der Rektor	**Die Kanzlerin**
Prof. Dr. Axel Schölmerich	**Dr. Christina Reinhardt**

für die Personalräte:

für den Personalrat der wissenschaftlich/künstlerisch Beschäftigten	**für den Personalrat**
Der Vorsitzende	**Der Vorsitzende**
Dr. Michael Jost	**Frank Markner**

Anlage zur Rahmendienstvereinbarung
über Einführung und Anwendung von Systemen der Informationstechnik (IT):

Grundregeln zur Administration von IT-Systemen

§ 1
Begriffsbestimmungen und Zweckbestimmungen

(1) Diese Anlage regelt zentrale Aspekte der Administration von IT-Systemen in Bezug auf Rechte, Pflichten und Verantwortlichkeiten der Administratoren und Administratorinnen und Leitungen von Einrichtungen sowie deren Umgang mit personenbezogenen und sowie persönlichen bzw. privaten Daten. Die Administration orientiert sich an den Zielen der Usability, Vertraulichkeit, Verfügbarkeit und Integrität.

(2) Eine Administratorin bzw. ein Administrator verwaltet eine ihr oder ihm anvertraute IT-Umgebung mit mehreren Nutzern und sorgt für deren störungsfreien Betrieb. Dies beinhaltet z.B. die Beschaffung, die Installation, die Konfiguration, die Wartung, die Überwachung des Betriebs sowie die Entsorgung der dort enthaltenen IT-Systeme. Zur Erfüllung dieser Aufgaben verfügt die Administratorin bzw. der Administrator über die notwendigen Rechte auf den zu administrierenden Systemen.

(3) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse entsprechend der Datenschutzgesetze. Persönliche Daten sind solche Daten, deren Nutzungsrecht erkennbar auf eine oder mehrere Personen beschränkt ist.

§ 2
Bestellung und Verantwortlichkeiten

(1) Die Leitung einer Organisationseinheit trägt die Gesamtverantwortung für die von ihr betriebenen IT-Systeme einschließlich IT-Sicherheit und Datenschutz. Unbeschadet dieser Gesamtverantwortung kann die Leitung einer Organisationseinheit IT-Administratorinnen bzw. Administratoren mit der Administration dieser IT-Systeme beauftragen. Die IT-Administratorin bzw. der Administrator führt die Administrationsaufgaben an den anvertrauten IT-Systemen nach Anweisung der Leitung der Organisationseinheit und am Bedarf der Einrichtung orientiert eigenständig und fachgerecht aus.

(2) Die Administratorin bzw. der Administrator verfügt über das notwendige Fachwissen, um die übertragenen Tätigkeiten ausführen zu können. Dies kann durch anerkannte Zertifikate oder Erfahrung im jeweiligen Arbeitsgebiet nachgewiesen werden.

(3) Die Einrichtung stellt die zur fachgerechten Administration der IT-Systeme erforderlichen Ressourcen zur Verfügung. Für Administratorinnen bzw. Administratoren stehen Weiterbildungsmöglichkeiten bereit, damit sie ihre Aufgaben nach dem aktuellen Stand der Technik und den Compliance-Anforderungen erfüllen können.

(4) Eine Bestellung zur Administratorin bzw. zum Administrator wird unter Angaben der Aufgaben und der Qualifikationen dokumentiert und den Beteiligten zur Kenntnis gegeben, die Dokumentation wird bei Bedarf aktualisiert. Die ZBE IT.SERVICES führt eine Liste aller Administratorinnen und Administratoren der RUB.

§ 3
Rechte und Pflichten von Administratorinnen und Administratoren

(1) Die Administratorin bzw. der Administrator stellt den Betrieb der von ihr bzw. ihm betreuten IT-Systeme in angemessener Weise sicher.

(2) Die Administratorin bzw. der Administrator verhält sich regelkonform (compliant) und ist im besonderen Maße zur Vertraulichkeit verpflichtet. Die Compliance bezieht sich auf die einschlägigen gesetzlichen Vorgaben (z.B. Datenschutzgesetze, Telekommunikationsgesetz

und Telemediengesetz) und insbesondere auf IT-relevante Dienstvereinbarungen sowie Regelungen des Rektorats der Ruhr-Universität Bochum zur Informationssicherheit. Die Einhaltung der rechtlichen Regelungen dürfen von der Beauftragten bzw. dem Beauftragten für Informationssicherheit und der Datenschutzbeauftragten bzw. dem Datenschutzbeauftragten überprüft werden.

(3) Das regelkonforme Verhalten einer Administratorin bzw. einem Administrator hat Vorrang gegenüber der Weisungsbefugnis einer/s Vorgesetzten. Bei Konflikten kann eine Schlichtungsstelle angerufen werden, die vom Koordinierungsausschuss für Informationssicherheit gebildet wird. Dies gilt auch bei sonstigen Konflikten im Spannungsfeld von Nutzeranforderungen, Ergonomie, Informationssicherheit und der Gewährleistung rechtlicher Anforderungen. Beschäftigte können sich auch an die Beschwerdestelle der RUB oder die Personalräte wenden.

(4) Administratorinnen bzw. Administratoren machen ihre Tätigkeit gegenüber den Nutzern des IT-Systems in angemessener Weise transparent. Dazu gehören rechtzeitige und angemessene Informationen über Aktivitäten, die Einfluss auf die Arbeit der Nutzer haben können. Auf Anfrage geben die Administratoren bzw. Administratorinnen den Nutzern Auskunft über personenbezogene Daten, die in dem von der Administratorin bzw. dem Administrator betriebenen System erfasst werden.

(5) Administratorinnen bzw. Administratoren greifen auf die übrigen personenbezogenen Daten nach § 3 Abs. 6 Satz 3 der Rahmen-DV (außerhalb von Log- oder Account-Daten) grundsätzlich nur mit Genehmigung des Besitzers bzw. der Besitzerin der Daten zu. Ohne diese Genehmigung sind die oder der behördliche Datenschutzbeauftragte und die Personalräte vor Beginn und sodann während der Maßnahme zu beteiligen.

(6) Administratoren bzw. Administratorinnen dürfen personenbezogene Daten ohne Zustimmung des Besitzers bzw. der Besitzerin nur auf Anfrage der bzw. des Datenschutzbeauftragten oder der bzw. des zentralen Sicherheitsbeauftragen weitergeben. Die anfragenden Personen haben dabei die Beteiligung der Personalräte nachzuweisen. Gleiches gilt, falls der Besitzer bzw. die Besitzerin der Daten nicht erreichbar ist. Die Vorfälle nach diesem Absatz sind von den Beteiligten zu dokumentieren; die Dokumentation wird bei der oder dem IT-Sicherheitsbeauftragten aufbewahrt. Die Weitergabe von Daten im Missbrauchsfall an Externe richtet sich im Übrigen nach den bei der bzw. dem IT-Sicherheitsbeauftragten dokumentierten Meldewegen der RUB

(7) Administratorinnen bzw. Administratoren geben Vorgesetzten auf Anfrage über den Stand des Betriebs Auskunft, soweit nicht personenbezogene Daten oder personenbezogene Aussagen zur Nutzung von Systemen betroffen sind. Eine Auskunftspflicht besteht auch gegenüber der bzw. dem IT-Sicherheitsbeauftragten, den Datenschutzbeauftragten und den Personalräten, wenn dies für die Erfüllung deren Aufgaben erforderlich ist.

(8) Die Administratorin bzw. der Administrator informiert die zuständigen Stellen der Organisationseinheit (Leitung) umgehend über schwerwiegende Störungen, insbesondere über solche, die die Informationssicherheit und den Datenschutz betreffen.

(9) Administratorinnen bzw. Administratoren betreiben die Systeme dem Stand der Technik entsprechend. Dafür bilden sie sich angemessen weiter. Die zentrale Betriebseinheit IT.SERVICES unterstützt die Administratorinnen bzw. Administratoren bei der Ausübung ihrer Aufgaben im Rahmen der zur Verfügung stehenden Ressourcen.