Amtliches Mitteilungsblatt

Gesamtpersonalrat

IT-Rahmendienstvereinbarung
zwischen dem Präsidium und dem Gesamtpersonalrat der Humboldt-Universität zu Berlin,

Herausgeber:	Die Präsidentin der Humboldt-Universität zu Berlin Unter den Linden 6, 10099 Berlin	**Nr. 111/2018**
Satz und Vertrieb:	Abteilung Kommunikation, Marketing und Veranstaltungsmanagement	**27. Jahrgang/19. November 2018**

IT-Rahmendienstvereinbarung

zwischen dem Präsidium und dem Gesamtpersonalrat der Humboldt-Universität zu Berlin

Präambel

(1) Der Einsatz der Informationstechnologie (IT) ist in nahezu allen Bereichen der Humboldt-Universität ein unverzichtbares Element zur Unterstützung der Forschungs-, Lehr-, Studien- und Verwaltungsprozesse. Es muss das Ziel des IT-Einsatzes sein, Arbeitsabläufe zu vereinfachen, Arbeitsprozesse effizient zu gestalten, die Informationsinfrastruktur leistungsfähig auszulegen sowie die Universitätsleitung und die weiteren universitären Einrichtungen und die dort jeweils Beschäftigten in ihren Entscheidungen und Handlungen zu unterstützen.

(2) Bei der Gestaltung von Bildschirmarbeitsplätzen und der Neuanschaffung bzw. Weiterentwicklung von IT-Systemen wird den gesicherten arbeitsmedizinischen und arbeitswissenschaftlichen Erkenntnissen über die menschengerechte Gestaltung der Arbeit, auch hinsichtlich der Softwareergonomie, Rechnung getragen.

(3) Diese Rahmendienstvereinbarung enthält grundsätzliche Regelungen und Verfahrensweisen, um bei der Einführung und Anwendung betrieblicher IT-Verfahren diese Ziele umzusetzen. Sie gibt einen Rahmen für die Schritte, welche bei der Einführung, Änderung oder Erweiterung von IT-Verfahren erfolgen müssen.

(4) Universitätsleitung und Gesamtpersonalrat sind sich einig, die Einführung, Änderung bzw. die Anwendung der betrieblichen IT-Verfahren im Rahmen des PersVG Berlin zum Wohle der Dienstkräfte und zur Erfüllung der dienstlichen Aufgaben gemeinsam zu verfolgen. Die Mitwirkung bzw. Mitbestimmung des jeweils zuständigen Personalrates sowie der Schwerbehindertenvertretung wird dabei als ein wesentlicher Gesichtspunkt gesehen.

(5) Die Universitätsleitung und der Gesamtpersonalrat stimmen darin überein, die Beschäftigten im Rahmen des Möglichen umfassend und kontinuierlich weiterzubilden, um ihre betrieblichen Qualifikationen zu sichern und weiterzuentwickeln.

§ 1 Geltungsbereich und Regelungsgrundsätze

(1) Die Rahmendienstvereinbarung Informationstechnologie (im Folgenden: IT-RDV) gilt für alle Beschäftigten der Humboldt-Universität zu Berlin (HU), die dem Geltungsbereich des Personalvertretungsgesetztes Berlin (PersVG Berlin) unterliegen.

(2) Die IT-RDV regelt die grundsätzlichen Informations- und Verfahrensschritte bei der Einführung und Anwendung informationstechnologischer Verfahren und Methoden sowie deren Änderung oder Ausweitung, wenn sie aufgrund ihres Umfangs einer Einführung vergleichbar sind, soweit die Maßnahme der Mitbestimmungspflicht unterliegt.

(3) Die IT-RDV kann, soweit erforderlich, durch Einzeldienstvereinbarungen ergänzt werden.

§ 2 Beschäftigungssicherung und Qualifizierung

(1) Die Universität bekennt sich zu ihrer Verpflichtung, als verlässliche Arbeitgeberin ihre Beschäftigten vor dem Verlust des Arbeitsplatzes zu schützen. Das erfordert gleichzeitig die Bereitschaft der Beschäftigten, an notwendigen Qualifizierungsmaßnahmen teilzunehmen und, sofern notwendig, auch den Arbeitsplatz zu wechseln.

(2) Die Kosten der Qualifizierungsmaßnahmen trägt die Universität. Qualifizierungsmaßnahmen finden grundsätzlich an Werktagen statt; die Teilnahme gilt als Arbeitszeit. Die Durchführung der Weiterbildung nimmt bei schwerbehinderten Beschäftigten auf Art und Maß der konkreten Behinderung Rücksicht. Die Teilnahme an einer IT-bezogenen Qualifizierungsmaßnahme darf nur aus schwerwiegenden Gründen abgelehnt werden. Beschäftigte, die an einer Qualifizierungsmaßnahme teilgenommen haben, sind verpflichtet, die dadurch erreichte Qualifikation einzusetzen, soweit die Arbeitsaufgabe dies verlangt.

(3) Die Universität gewährleistet im Rahmen der Personalentwicklung und der DV Weiterbildung durch Qualifizierungsmaßnahmen die ständige Fortentwicklung des fachlichen, methodischen und sozialen Wissens im Rahmen der Aufgabengebiete (Erhaltungsqualifizierung) sowie Qualifizierungsmaßnahmen zur Übernahme anderer Arbeitsaufgaben (Mobilitätsqualifizierung).

(4) Bei der Einführung eines IT-Verfahrens sind Qualifizierungsmaßnahmen zur Erfüllung der veränderten Anforderungen im fortbestehenden Arbeitsgebiet (Anpassungsqualifizierung) mit ausreichend Zeit für Qualifizierungsmaßnahmen und eine Einarbeitung vorzusehen. Bei umfangreichen oder komplexen IT-Verfahren sind ggf. neben Grundschulungen vertiefende und ggf. ergänzende Aufbauschulungen vorzusehen. Fallen Arbeitsgebiete weg, dient die Mobilitätsqualifizierung der Übernahme anderer gleich- oder höherwertiger Arbeitsaufgaben.

(5) Betriebsbedingte Beendigungskündigungen infolge von Einführung und Betrieb von IT-Systemen sowie damit verbundenen Organisations- und Betriebsveränderungen sind ausgeschlossen.

(6) Im Zusammenhang mit der Einführung eines IT-Verfahrens ist die einvernehmliche Übertragung eines niedriger wertigen Aufgabengebietes unter Wahrung des Besitzstandes im Rahmen der Regelungen des Kuratoriumsbeschlusses 71/05 vom 18.11.2005 möglich.

(7) Lehnen Beschäftigte eine zumutbare Qualifizierungsmaßnahme oder die Übernahme einer zumutbaren anderen Arbeitsaufgabe die nicht im Wege des Direktionsrechtes übertragen werden kann, ohne hinreichenden sachlichen Grund ab, sind Änderungskündigungen möglich. Es gilt hier auch die im Tarifvertrag über den Rationalisierungsschutz für Angestellte (RatschTV Ang) in § 4 (Fortbildung, Umschulung) festgehaltene Protokollnotiz zu Abs. 1 Unterabs. 2.

§ 3 Ausschluss von Verhaltens- und Leistungskontrollen

(1) Individualisierbare Leistungs- und Verhaltenskontrollen mit Hilfe von IT-Systemen sind unzulässig, es sei denn, diese sind mit der zuständigen Personalvertretung vorab vereinbart worden; die Beschäftigten sind im Rahmen der gesetzlichen datenschutzrechtlichen Bestimmungen darüber zu informieren, welche Daten für die Kontrolle erzeugt, erfasst, gespeichert oder verarbeitet werden. Unabhängig davon sind Auswertungen zur Qualitätssicherung der erfassten Daten und deren Zuordnung zu den erfassenden und/oder verarbeitenden Beschäftigten durch die Vorgesetzten und Administratoren (m/w/d) zulässig.

(2) Die Einsichtnahme durch Vorgesetzte sowie Administratorinnen und Administratoren in Datenbestände richtet sich nach dem Grundsatz der aufgaben- und zuständigkeitsbezogenen Berechtigung. Insbesondere

a) stehen jeder Zugriffsebene nur solche Daten zur Verfügung, die zur Wahrnehmung ihrer Aufgaben benötigt werden,

b) darf in Vorgänge, zu denen sich Beschäftigte in dem von ihnen bedienten IT-System den genehmigten, alleinigen Zugriff vorbehalten haben („persönliche Ablage"), grundsätzlich nur mit ihrer Zustimmung Einsicht genommen werden.

(3) Daten, die gemäß Absatz 1 für Zwecke der Überwachung der Leistung und/oder des Verhaltens der Beschäftigten bzw. zur Qualitätssicherung verarbeitet werden, sind gemäß den anzuwendenden datenschutzrechtlichen Bestimmungen unverzüglich zu löschen, sobald ihre Kenntnis für die Erfüllung dieses Verarbeitungszwecks nicht mehr erforderlich ist.

(4) Daten über Leistung und Verhalten von Beschäftigten, die nicht ordnungsgemäß entsprechend den vorstehenden Absätzen gewonnen worden sind, dürfen arbeits- oder dienstrechtlichen Maßnahmen gegen Beschäftigte nicht zugrunde gelegt werden. Gleichwohl vorgenommene Maßnahmen sind zurückzunehmen. Daten sind unverzüglich zu löschen, nachdem ihre Verarbeitung als unzulässig erkannt worden ist. Dabei ist nach den anzuwendenden datenschutzrechtlichen Bestimmungen zu verfahren.

§ 4 Zulässige Kontrollmaßnahmen

Abweichend von § 3 können Kontrollmaßnahmen durchgeführt werden, wenn Tatsachen bekannt werden, die den Verdacht einer erheblichen Dienst- bzw. Arbeitspflichtverletzung rechtfertigen. Die Dienststelle informiert vorher die zuständige Personalvertretung in diesen Fällen über die vorliegenden Tatsachen und Verdachtsmomente sowie die geplanten Kontrollmaßnahmen.

§ 5 Phasenorientiertes Beteiligungsverfahren

(1) Die Einführung neuer IT-Verfahren oder Änderung von IT-Verfahren, die in ihrem Umfang einer Neueinführung gleichkommen, erfolgen unter Berücksichtigung von § 5 grundsätzlich, sofern sich die Vertragsparteien nicht auf ein anderes Vorgehen einigen, in Form eines phasenorientierten Beteiligungsverfahrens gemäß der in dieser Vereinbarung getroffenen Regelungen. Bei kleineren IT-Verfahren können, sofern es den Vertragsparteien angemessen erscheint, auch Vorgehensweisen gewählt werden, die direkt vom Testbetrieb zu einem regulären Betrieb übergehen.

(2) Das phasenorientierte Beteiligungsverfahren beinhaltet drei Phasen, nämlich: Testbetrieb, Pilotbetrieb und regulärer Echtbetrieb.

(a) Als Testbetrieb im Sinne dieser RDV werden Tests eines Softwaresystems verstanden, die getrennt von dem ordnungsgemäßen Betrieb des Verfahrens und unter Ausschluss personenbezogener Echtdaten stattfinden.

(b) Als Pilotbetrieb im Sinne dieser RDV wird ein befristeter, ordnungsgemäßer Betrieb mit Echtdaten im Rahmen eines fortwährenden Beteiligungsverfahrens verstanden, der neben der betrieblichen Aufgabenerfüllung einer Evaluation und Optimierung des Verfahrens dient.

(c) Als regulärer Echtbetrieb im Sinne dieser RDV wird ein unbefristeter, ordnungsgemäßer Betrieb des Verfahrens verstanden.

(3) Die Aufnahme des Pilotbetriebs unterliegt der Mitbestimmung. Im Rahmen der Durchführung des Beteiligungsverfahrens nach § 5 dieser Vereinbarung wird geprüft, ob alle Voraussetzungen hierfür erfüllt sind. Im Rahmen des Beteiligungsverfahrens wird geprüft, ob alle Voraussetzungen hierfür erfüllt sind. Hierzu ist eine aktuelle Systemdokumentation gemäß § 6 dieser RDV und gegebenenfalls der Bericht des Testbetriebs vorzulegen.

(4) Die Aufnahme des regulären Echtbetriebs unterliegt der Mitbestimmung und setzt grundsätzlich die erfolgreiche Durchführung des Pilotbetriebs voraus. Im Rahmen des Beteiligungsverfahrens wird geprüft, ob alle Voraussetzungen hierfür erfüllt sind.

§ 6: Schritte zur Einführung, Änderung bzw. Neugestaltung von IT-Verfahren

Die Information und Beteiligung des zuständigen Personalrats sowie der Schwerbehindertenvertretung erfolgt durch die Präsidentin oder den Präsidenten bzw. das zuständige Präsidiumsmitglied unter Einbeziehung der fachlich und technisch für das System Verantwortlichen.

Als Schritte zur Einführung von IT-Verfahren ist Folgendes vorgesehen:

1) Zuständige Einrichtung: Vorabstimmung zur Einführung des IT-Verfahrens

a. Vorabinformation an behDSB

b. Abstimmung zum weiteren Verlauf mit zuständigem Personalrat

c. *Verzeichnis von Verarbeitungstätigkeiten* und *Sicherheitskonzept* an behDSB geben (evtl. vorab zur Abstimmung, dann auf Papier mit Unterschrift)

d. Vorabinformation an Schwerbehindertenvertretung

I. Terminangebot (soweit schon zugänglich)

II. Vorstellung des IT-Verfahrens

e. Vorabinformation an zuständigen Personalrat:

I. Fragebogen IT-Verfahren

II. Abstimmung gewünschte Unterlagen und Prozedere

III. Terminangebot zur Vorstellung

IV. Vorstellung des IT-Verfahrens

V. Prüfung auf Abschluss einer Einzeldienstvereinbarung

f. Aufbereitung von Informationen zum IT-Verfahren für die Nutzenden

2) Beteiligung Schwerbehindertenvertretung durch die zuständige Einrichtung

a. Schwerbehindertenvertretung: Termin zu Vorstellung und Testung des IT-Verfahrens

3) Zuständiges Präsidiumsmitglied betreibt Abstimmungsverfahren

a. evtl. Akademischer Senat bzw. Senatskommissionen, studentische Vertretungen: Information

b. Aufforderung der Schwerbehindertenvertretung zu einer Stellungnahme im Rahmen der Beteiligung

c. Aufforderung der behDSB zu einer Stellungsnahme

4) Eingang Stellungnahme behDSB (evtl. mit Auflagen)

→ Auflagen des behDSB umsetzen

5) Eingang Stellungnahme Schwerbehinderten-vertretung

→ Auflagen der Schwerbehinderten vertretung umsetzen

→ Nachweis der Umsetzung der Auflagen

6) Inhaltliche Abstimmung zwischen zuständiger Einrichtung und zuständigem Personalrat

7) Zuständige Einrichtung schreibt an zuständiges Präsidiumsmitglied mit Bitte an den zuständigen Personalrat um Wahrnehmung der Mitbestimmung mit Stellungnahmen von behDSB und SBV.

8) Zuständiger Personalrat hat ggf. Rückfragen, beantragt ggf. Fristverlängerung

9) Zuständiger Personalrat entscheidet über Antrag (evtl. mit Auflagen)

10) Zuständige Einrichtung bearbeitet Auflagen, Information, Öffentlichkeitsarbeit für das IT-Verfahren

Bei wesentlichen Änderungen von IT-Verfahren (Definitionen siehe Anlage 1) oder der phasenweisen Einführung gilt dieser Ablauf in gleicher Weise. Beizubringende Dokumente, die sich nicht geändert haben, müssen nicht erneut eingereicht werden. Wesentliche Änderungen in den Dokumenten sind zu kennzeichnen.

Erläuterungen zu § 6:

Zu 1) c.: siehe § 7, b) 2. und 3. sowie Anlagen 2 und 3

Zu 1) e.: Es wird geprüft, bei welcher Personal-vertretung der Antrag auf Zustimmung zur Einführung oder Änderung des IT-Verfahrens eingereicht werden muss:

- *Sind ausschließlich studentische Beschäftigte betroffen, ist es der Personalrat der studentischen Beschäftigten (PRstudB),*
- *sind ausschließlich hauptberufliche Beschäftigte betroffen, ist es der Personalrat Hochschulbereich (PR HSB),*
- *sind beide Beschäftigtengruppen betroffen, ist es der Gesamtpersonalrat (GPR).*

Zu 1) e. II.: Siehe § 7

Zu 1) e. V.: Auf der Grundlage dieser Rahmen-dienstvereinbarung können weitere Einzelheiten oder Besonderheiten zu IT-Verfahren in Form von Einzeldienstvereinbarungen geregelt werden.

Zu 6): Diese inhaltliche Abstimmung dient der Klärung offener Fragen und der Definition von Vorgehensweisen, um Zeitverzögerungen beim formellen Beteiligungsverfahren zu vermeiden. Falls sich bis Punkt 6) bereits herausgestellt hat, dass besondere Formen der Einführung erforderlich sind, werden diese hier abgestimmt. Möglich sind z.B. die Einführung über einen Testbetrieb, die Einführung in mehreren Phasen oder ein befristeter Betrieb.

Zu 7): Das zuständige Präsidiumsmitglied fordert die Personalvertretung offiziell auf, der Einführung des IT-Verfahrens zuzustimmen. Eingereicht werden hier z.B. die offizielle Stellungnahme des behDSB, der Nachweis der Beteiligung der SBV sowie weitere unter § 7 genannte Unterlagen.

Zu 10): Bei einer Zustimmung mit Auflagen informiert die zuständige Einrichtung das Präsidiumsmitglied und die zuständige Personal-vertretung über die Erfüllung der Auflagen.

§ 7 Dokumentation des IT-Verfahrens

a) Grundsätzliches

Ziel der Dokumentation ist es, Struktur und Leistungsumfang der betrieblichen IT-Verfahren für Personalräte und Beschäftigte transparent zu machen. Die Dokumentation soll knapp sowie verständlich sein und muss kontinuierlich gepflegt werden.

Für IT-Verfahren, die personenbezogene Daten verarbeiten, muss ein Sicherheitskonzept erstellt werden. Wenn personenbezogene Daten in mitbestimmungspflichtigen IT-Verfahren verar-beitet werden, werden dem zuständigen Personalrat die Stellungnahme bzw. das Ergebnis der Vorabkontrolle des behördlichen Datenschutz-beauftragten zur Verfügung gestellt.

Bei der Einführung von neuen IT-Verfahren für Nutzer sind Soft- und Hardwareergonomie sowie die Barrierefreiheit zu berücksichtigen und die Schwerbehindertenvertretung nachweislich zu beteiligen.

b) Basisdokumente für einen Mitbestimmungs-antrag

Für einen Mitbestimmungsantrag sind dem zuständigen PR durch das zuständige Präsidiums-mitglied folgende Dokumente vorzulegen:

1. Systemdokumentation: Diese Doku-mentation muss folgende Inhalte unter anderem abdecken (sofern diese nicht schon im Sicherheitskonzept enthalten sind):

- Ziel und Zweck mit Anwendungsbereich
- Bezeichnung des abzulösenden Systems
- Organisationskonzept (u.a. fachliche und technische Verantwortung, administrativer Zugriff, Wartung der Hard- und Software)
- Hardwarekomponenten des Systems (in begründeten Fällen z.B. Spezialhardware)
- Softwareverzeichnis mit Systembeschreibung
- Schnittstellenspezifikationen, soweit andere IT-Systeme angebunden werden

2. Es bedarf einer Risikoanalyse und ggf. auch eines Sicherheitskonzeptes. Ein Sicherheitskonzept ist nicht erforderlich, wenn die Risikoanalyse ergibt, dass keine Sicherheitsmaßnahmen erforderlich sind, da keine Gefahren bei Verarbeitung und Betrieb in Hinsicht auf Vertraulichkeit, Integrität oder Verfügbarkeit bezüglich personenbezogener oder sonstiger sensibler Daten (z.B. wegen strategischer, wissenschaftlicher oder finanzieller Bedeutung) drohen. Die Risikoanalyse ist beizulegen.

3. Das Sicherheitskonzept hat mindestens die in der Risikoanalyse aufgeführten Risiken aufzugreifen. Werden weitere Risiken offenbar, ist es zu erweitern. Im Sicherheitskonzept sind Angaben zum Verfahren zu machen, Gefahren sowie die ergriffenen technisch-organisatorischen Maßnahmen darzustellen und darzulegen, dass das Restrisiko des Verfahrens auf ein tragbares Maß reduziert wurde. Das Sicherheitskonzept ist sowohl auf fachlicher wie auf technischer Seite von der jeweils die verantwortliche Leitungsstelle zu unterzeichnen. In Anlage 2 wird erläutert, welche Aspekte regelmäßig in ein Sicherheitskonzept zu integrieren sind.

4. Stellungnahme des Behördlichen Datenschutzbeauftragten (soweit vorhanden)

5. Schriftlicher Nachweis der Beteiligung der Schwerbehindertenvertrauensperson zur Barrierefreiheit

6. Beschreibung der wesentlichen erwartbaren Änderungen von Arbeitsinhalten, -anforderungen und -abläufen sowie eine Abschätzung der betroffenen Arbeitsplätze.

7. Aussagen zur Personalsituation bzgl. der Betreuung des IT-Verfahrens

8. Bei begründetem Bedarf müssen der zuständigen Personalvertretung im Rahmen des Mitbestimmungsverfahrens nach § 6 durch das zuständige Präsidiumsmitglied auf Anforderung ggf. zusätzliche Unterlagen vorgelegt werden.

c) Abschluss einer Einzeldienstvereinbarung (bei Bedarf)

Gegebenenfalls wird vor Beendigung des Mitbestimmungsverfahrens eine Einzeldienstvereinbarung abgeschlossen. Über die IT-Rahmendienstvereinbarung hinausgehende Regelungen sind dabei möglich.

Protokollnotiz zu § 7, b) Ziffer 8:

Die Parteien haben einvernehmlich festgehalten, dass bei einem „begründeten Bedarf" während eines laufenden Mitbestimmungsverfahrens nach den Voraussetzungen der Ziffer 8 zusätzliche Unterlagen zur Verfügung zu stellen sind.

Ein solcher Fall ist in der Regel anzunehmen, wenn nachfolgend genannte Unterlagen zur Beurteilung des Mitbestimmungsverfahrens durch die zuständige Personalvertretung notwendig sind. Dazu zählen:

1. Liste der Zugriffsberechtigten (Namen oder Stellenzeichen) unter Beachtung von Anlage 3

2. Einführungskonzept (inklusive Zeitplan und ggf. Stufen der Planung des Erprobungs- und des darauf folgenden Einführungsprozesses)

3. Schulungskonzept

4. Angaben/Übersicht zu Arten und Zweck von in das IT-Verfahren integrierten Auswertungen von personenbezogen Daten, bei denen nicht anonymisierte Beschäftigtendaten verwendet werden (Kurzbeschreibung und enthaltene Daten)

5. Stellungnahmen oder Gutachten zur softwareergonomischen Gebrauchstauglichkeit und Barrierefreiheit

6. Maßnahmenpläne zur Prüfung und Gewährleistung der Gebrauchstauglichkeit und Barrierefreiheit (insb. Begutachtungen oder Befragungen)

7. Bedienungsanleitung

8. Bezugnahme zu Auflagen bzw. deren Umsetzungsstand

9. Prozedere für die Fernwartung bei Auftragsdatenverarbeitung

§ 8 Kontrollrechte und sonstige Rechte des zuständigen Personalrates

(1) Die Universitätsleitung informiert den GPR im Rahmen eines mindestens jährlich stattfinden Gesprächs umfassend über die geplanten zentralen IT-Vorhaben.

(2) Die zuständigen Personalräte sind berechtigt, die Einhaltung der Dienstvereinbarung zu überprüfen. Sie sind dabei zu unterstützen und ihnen sind weitere Hilfsmittel, beispielsweise bestehende Auswertungen zu IT-Verfahren, Evaluierungen (wie zur Softwareergonomie) usw. auf Anforderung zur Verfügung zu stellen.

§ 9 Datenschutz und Datensicherheit/ Fristen für Datennutzung und Datenlöschung bei personenbezogenen Daten

(1) Personen, die entsprechend ihrer betrieblichen Aufgaben Zugang zu IT-Verfahren haben, die personenbezogene Daten verarbeiten, sind insbesondere auf ihre Pflichten im Rahmen der folgenden Gesetze hinzuweisen:

- EU-Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Berliner Datenschutzgesetz (BlnDSG)
- Personalvertretungsgesetz (PersVG Berlin)

(2) Ist die Datenverarbeitung an der HU nicht möglich ist, müssen die Gründe schriftlich dargelegt werden. Daten der Hochschulverwaltung, die im Rahmen von Cloudlösungen nicht in Rechenzentren der Hochschulen gespeichert und verarbeitet werden, dürfen ausschließlich auf Servern gespeichert und verarbeitet werden, welche ein nach Art. 45 DSGVO angemessenes Schutzniveau bieten. Sofern die Verarbeitung durch einen Dritten im Rahmen einer Auftragsdatenverarbeitung erfolgt bzw. erfolgen muss (Art. 28 DSGVO, § 26 +27 BlnDSG), ist sicherzustellen, dass ausreichende technische Kompetenzen zur Begleitung des Verfahrens (z.B. Unterstützung Fachbereich bei Einführung und Mitbestimmungsverfahren; Kontrollaufgaben bei Betrieb, Wartung gem. Art. 28 DSGVO, § 26 + 27 BlnDSG) auf Seiten der Humboldt-Universität vorhanden sind.

(3) Der GPR erhält das Ergebnis der Vorabkontrolle von IT-Verfahren gem. Art. 35 DSGVO, § 5 Abs. 3 BlnDSG.

(4) Protokolldateien mit personenbezogenen Daten sind spätestens nach 14 Tagen zu löschen. Müssen Protokolldateien länger aufbewahrt werden, dann ist der zuständige Personalrat darüber zu informieren. Gründe können z.B. sein:

- gesetzliche oder andere regulatorische Pflichten (z.B. LHO)
- technische Systemfunktionalität
- Nachweisführung in anhängigen Rechtsverfahren.

(5) Sicherheitskonzepte und diesbezügliche Stellungnahmen der/des behördlichen Datenschutzbeauftragen sind nicht öffentlich und werden per E-Mail nur verschlüsselt verschickt sowie gegen unberechtigten Zugriff geschützt aufbewahrt.

§ 10 Fremdvergabe der Datenverarbeitung, Fernwartung, Weitergabe der Daten an Dritte

(1) Die IT-RDV gilt unabhängig davon, ob die Einführung, der Betrieb, die Erweiterung und die Änderung von IT-Verfahren durch die Humboldt-Universität direkt oder im Auftrag der HU durch andere Personen oder Firmen erfolgt.

(2) Werden Beschäftigtendaten an Dritte regelmäßig, einmalig oder periodisch übermittelt, ist von Seiten des Arbeitgebers das Mitbestimmungsrecht des zuständigen Personalrats nach PersVG zu beachten. Rechtsgrundlage und Zweck der Übermittlung, empfangene Stelle, Übermittlungsart und zeitlicher Übermittlungsrhythmus sind anzugeben sowie eine Dateibeschreibung zu erstellen.

(3) Werden bei der Dienstleistung personenbezogene Daten verarbeitet, stellt die Universitätsleitung die Einbeziehung der/des Behördlichen Datenschutzbeauftragten sicher und überreicht dem zuständigen Personalrat unaufgefordert den schriftlichen Auftrag nach Art. 28 DSGVO, § 26 + 27 BlnDSG.

(4) Bei Fernwartung durch Dritte haben diese grundsätzlich keinen Zugriff auf personenbezogene Daten. Bei Ausnahmen ist der zuständige Personalrat zu beteiligen.

(5) Ein Fernwartungszugriff auf Systeme mit personenbezogenen Daten darf nur unter Kontrolle durch den jeweiligen Systemverantwortlichen und mittels eines befristeten Zugangs erfolgen.

§ 11 Beteiligung und Rechte der Beschäftigten

(1) Die betroffenen Mitarbeiterinnen und Mitarbeiter werden

a) vor der Einführung von IT-Verfahren,

b) während der Entwicklung,

c) vor geplanten, für den Arbeitsablauf wichtigen Änderungen,

d) und vor der Entscheidung über IT-Verfahren

rechtzeitig und ausreichend informiert.

(2) Werden personenbezogene Daten erstmalig in dem jeweiligen IT-System automatisiert verarbeitet, sind die Betroffenen gemäß Art. 13 und 14 DSGVO zu informieren. Dies umfasst insbesondere die Verarbeitungsform und Verwendungszwecke des Systems, die Datenarten, die verarbeitende Einrichtung bzw. Organisationseinheit sowie die Verwendungszwecke der Daten.

(3) Betrifft die Verarbeitung nach Absatz 2, Satz 1 Personalaktendaten, so erfolgt die Information gegenüber den Mitarbeiterinnen und Mitarbeitern in vertraulicher Form.

(4) Im Übrigen gelten die Rechte der Mitarbeiterinnen und Mitarbeiter gemäß Kapitel 3 der DSGVO, Kapitel 3 BlnDSG.

(5) Werden von den Beschäftigten Vorschläge zur menschengerechten und gesundheitsförderlichen Gestaltung von Arbeitsplätzen, -verfahren und -abläufen unterbreitet, so sind diese zu prüfen. Eine eventuelle Ablehnung der Vorschläge ist in geeigneter Form zu begründen.

§ 12 Gestaltung der Bildschirmarbeitsplätze und Arbeitsumgebung, Ergonomie, Barrierefreiheit sowie Gesundheitsschutz

(1) Bei der Gestaltung von Bildschirmarbeitsplätzen und der Neuanschaffung bzw. Weiterentwicklung von IT-Systemen werden die ergonomischen Bedingungen des Arbeitsplatzes geprüft.

(2) Die Bedingungen des Arbeitsplatzes werden, soweit mit vertretbarem Aufwand möglich, an die individuellen Anforderungen der/des jeweiligen Beschäftigten angepasst.

(4) Die Gestaltung von Bildschirmarbeitsplätzen erfolgt unter Beteiligung der/des daran Beschäftigten und des zuständigen Personalrats sowie ggf. der Schwerbehindertenvertretung.

(5) Beschaffungsstellen und DV-Verantwortliche/ DV-Beauftragte der Bereiche werden bezüglich der Auswahl von Arbeitsmitteln unter Beachtung der Ergonomie geschult.

(6) Bei der Einführung neuer IT-Verfahren/ Beschaffung neuer IT-Systeme ist in der Ausschreibung die Einhaltung softwareergonomischer Regeln als Kriterium aufzunehmen. Der Anbieter sollte mit der Einreichung seines Angebots, soweit möglich, entsprechende Stellungnahmen und Nachweise erbringen und sich bereit erklären, bedarfsweise ergänzende Nachweise im Rahmen des Pilotbetriebs zu erbringen sowie Nachprüfungen des Auftraggebers zu unterstützen.

(7) Die HU strebt bei der Einrichtung und Gestaltung von Arbeitsplätzen an, ausschließliche Bildschirmtätigkeiten zu vermeiden.

(8) Die IT-Verfahren und IT-Arbeitsplätze sind unter Berücksichtigung der Prinzipien der Barrierefreiheit so zu gestalten, dass behinderten Beschäftigten der Zugang und somit die volle Teilhabe am universitären Leben ermöglicht wird. Die Schwerbehindertenvertretung ist rechtzeitig einzubeziehen.

(9) Um Beeinträchtigungen und Schädigungen der Gesundheit vorzubeugen, werden gesundheitliche Ausgleichsmaßnahmen (z.B. Entspannungsübungen unter fachlicher Anleitung) während der Arbeitszeit nach Beteiligung des Gesamtpersonalrates in ausreichender Menge und kostenfrei für die Beschäftigten angeboten.

(10) Der Arbeitgeber führt eine Gefährdungsbeurteilung hinsichtlich der Bildschirmarbeitsplätze gemäß Arbeitsschutzgesetz und Arbeitsstättenverordnung durch. Diese wird kontinuierlich geprüft und fortgeschrieben.

§ 13 Arbeitsorganisation

(1) Bei der Einführung und Anwendung von IT-Maßnahmen ist stets die Gesamtbelastung der/des damit befassten Beschäftigten zu berücksichtigen. Eine Leistungsverdichtung ist durch Reduzierung oder Verlagerung von Aufgaben zu vermeiden.

(2) Beim Betrieb von IT-Verfahren müssen sowohl die Betreuung wie auch die Benennung von Ansprechpartnerinnen und/-partnern inklusive der Vertretung gewährleistet sein.

(3) Eine Erreichbarkeitserwartung außerhalb der gesetzlich und in der DV Gleitzeit festgelegten Arbeitszeiten ist ausgeschlossen.

§ 14 Salvatorische Klausel

(1) Sollten Teile der Dienstvereinbarung für unwirksam erklärt werden, wird die Wirksamkeit der übrigen Teile nicht berührt. Die Humboldt-Universität zu Berlin und der Gesamtpersonalrat verpflichten sich, anstelle der unwirksamen Regelung in vertrauensvoller Zusammenarbeit eine dem Ziel möglichst nahekommende Regelung zu treffen.

§ 15 Abschließende Regelungen

(1) Diese Dienstvereinbarung tritt am Tage nach Unterzeichnung durch beide Parteien oder Letztunterzeichnung in Kraft.*

(2) Die Beschäftigten werden nach Inkrafttreten dieser Vereinbarung in der HU-Information und auf der Startseite der HU informiert. Sie wird zusätzlich allgemein zugänglich gemacht.

(3) Alle Anlagen gemäß Anlagenverzeichnis sind Bestandteil der Vereinbarung.

(4) Die Dienstvereinbarung wird auf unbestimmte Zeit geschlossen. Sie kann unter Einhaltung einer Frist von zwölf Monaten zum Monatsende gekündigt werden. Die Kündigung bedarf der Schriftform. Dienststelle und Gesamtpersonalrat verpflichten sich, spätestens im auf die Kündigung folgenden Monat Verhandlungen zum Abschluss einer neuen Dienstvereinbarung aufzunehmen. Wird eine neue Dienstvereinbarung nicht spätestens drei Monate vor Ablauf der Kündigungsfrist abgeschlossen oder erklärt eine Seite die Verhandlungen für gescheitert, kann die Einigungsstelle für Personalvertretungssachen angerufen werden. Die Dienstvereinbarung wirkt in diesem Fall bis zum Beschluss der Einigungsstelle nach, längstens jedoch neun Monate nach Ablauf der Kündigungsfrist.

Anlageverzeichnis:

Anlage 1
Definition Release und Update/Wesentliche Änderungen

Anlage 2
Regelmäßig in ein Sicherheitskonzept zu integrierende Bestandteile

Anlage 3
Hinweise zum Zugriffsberechtigungskonzept

Anlage 4
Gesund bleiben am Bildschirmarbeitsplatz

* Die Dienstvereinbarung ist am 27. Oktober 2018 in Kraft getreten.

Anlage 1: Definition Release und Update/Wesentliche Änderungen

Release: Eine neue veröffentlichte Version einer Software wird als „Release" im Sinne dieser Dienstvereinbarung bezeichnet, wenn seit der letzten Veröffentlichung wesentliche Änderungen an der Software durchgeführt worden sind.

Updates: Wenn in der veröffentlichten Version ausschließlich Änderungen erfolgten, die keine wesentlichen Änderungen darstellen, dann gilt diese Version der Software nicht als „Release" im Sinne dieser Dienstvereinbarung, sondern als *Update.*

Wesentliche Änderungen sind insbesondere:

- Grundsätzlich alle Änderungen an der Architektur, die eine inhaltliche Veränderung des Sicherheitskonzepts erforderlich machen,
- Grundlegende Änderungen bei der Verwendung der gespeicherten Daten,
- Änderungen an den Anwenderoberflächen, die für die Verwendung durch die Endanwender bestimmt sind, soweit diese Änderungen (wesentliche/nicht unerhebliche) Veränderungen der Arbeitsabläufe zur Folge haben,
- Anbindung neuer bzw. Veränderungen bestehender Schnittstellen zu weiteren IT-Verfahren.

Keine wesentlichen Änderungen sind u. a.:

- Fehlerkorrekturen (insbesondere Behebung von Sicherheitslücken),
- Optimierung der Benutzerschnittstellen,
- Änderungen an der Software, die der Verbesserung von technischen Parametern (z. B. erhöhte Geschwindigkeit, Optimierung der Ressourcenverwendung, etc.) der Software dienen,
- Aktualisierung und Veränderung der für den Betrieb und die Entwicklung verwendeten Hardware (z. B. Serversysteme, Netzwerkinfrastruktur, etc.) und Software (z. B. Betriebssysteme, Entwicklungs-umgebungen, Hilfsprogramme, etc.), sofern sie nicht das Sicherheitskonzept inhaltlich verändern.

Anlage 2: Regelmäßig in ein Sicherheitskonzept zu integrierende Bestandteile:

- Beschreibung der Verfahrensabläufe, Beschreibung, Verknüpfung und Lokalisierung der Komponenten
- Angaben zur Verantwortlichkeit für die Datenverarbeitung in fachlicher und technischer Hinsicht (bei Auftragsdatenverarbeitung hinsichtlich der Kontrollausübung), ggf. unterteilt hinsichtlich einzelner Bereiche oder Verfahrensschritte
- Angaben zur Rechtsgrundlage der Datenverarbeitung
- verständliche Auflistung der verarbeiteten personenbezogenen Daten, Einschätzung des Schutzbedarfs
- Angaben zu Abhängigkeiten des Systems/Verfahrens von/zu weiteren Systemen
- Angaben zur Kritikalität des Verfahrens/Systems hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit
- Dauer der Aufbewahrung von Daten, Weitergabe von Daten an Dritte, Datenempfang von Dritten
- Zugriffsmöglichkeiten, Rollen- und Rechtekonzept, einschließlich der Verfahren zur Vergabe und Entziehung (siehe Anlage 6)
- Umgang mit Protokoll- und technischen Loginformationen, Löschfristen, Löschkonzepten
- Darstellung der Betriebsgefahren, möglicher Gefährdungsereignisse und des hieraus resultierenden Schadenspotentials, der vorgesehenen Sicherheitsmaßnahmen sowie eine Einschätzung des sodann verbleibenden Restrisikos
- Darstellung anwendungs- oder verfahrensbedingter Besonderheiten/Gefährdungen (z.B. Virtualisierungslösungen, IaaS, SaaS, Cloudbetrieb, Erforderlichkeit und Ablauf von Fernwartungen, Besonderheiten wegen eingeschränkter Kontroll- oder Löschmöglichkeiten, Einbindung außereuropäischer Dienstleister, besondere gesetzliche Anforderungen)
- Angaben zum Notfallmanagement und tolerabler Ausfall-/Reaktionszeiten
- Ansprechpartnerinnen und Ansprechpartner bezüglich der Umsetzung von Auskunftsrechten und Informationspflichten nach DS-GVO und BlnDSG (z.B. Art. 12, 13, 15, 34 DS-GVO, § 27 + 42 + 43 BlnDSG)
- Abschließende Bewertung der Restrisiken unter Einbeziehung der vorgesehenen Sicherheits-maßnahmen
- Unterschriften der fachlichen und technischen Verantwortlichen

Anlage 3: Hinweise zum Zugriffsberechtigungskonzept:

Im Rahmen des Sicherheitskonzepts erfolgt die Einrichtung eines datenschutzkonformen Zugriffsberechtigungskonzepts. Hierbei ist ein hierarchieabhängiger, demgemäß unterschiedlich ausgeprägter Informationsbedarf bei einem gleichzeitig zunehmenden Datenanonymisierungsgebot bei höherer Hierarchiestufe zu berücksichtigen.

- Dabei sind Zugriffsberechtigungen restriktiv und ausgerichtet auf die jeweils individuell erforderliche Aufgabenwahrnehmung zu vergeben sowie eine klare Funktionstrennung zwischen Nutzer-und Administrator-Rechten vorzusehen.
- Die Berechtigungsprofile aller Nutzer (Liste der Benutzerstämme, Sammelprofile, Einzelprofile und Verknüpfungen mit Berechtigungsobjekten, Berechtigungen sowie zugewiesene Felder und Aktivitäten) sind jeweils im System dokumentiert. Die Vergabe, Änderung und Löschung von Berechtigungen wird dokumentiert. Eine Einsicht in Berechtigungslisten wird dem zuständigen Personalrat, im Rahmen der gesetzlichen Bestimmungen, am System ermöglicht.

Anlage 4: Gesund bleiben am Bildschirmarbeitsplatz

Beschäftigte an Bildschirmarbeitsplätzen sind durch spezifische körperliche, visuelle und psychische Belastungen gesundheitlich gefährdet.

Die Arbeitgeberin hat nach § 5 ArbSchG die Pflicht, diese Gefährdungen zu ermitteln, entsprechende Schutzmaßnahmen festzulegen und über die Gefahren und deren Verhütung die Mitarbeiterinnen und Mitarbeiter einmal jährlich zu unterweisen.

Sie hat auch eine arbeitsmedizinische Vorsorgeuntersuchung nach der BildschArbV anzubieten, welche im Arbeitsmedizinischen Zentrum der Charité wahrgenommen werden kann.

Bei dieser Untersuchung wird u. a. ein Sehtest zur Prüfung der Sehleistung auch speziell im Bildschirmabstand durchgeführt und die Beschäftigten erhalten Informationen zur ergonomischen Gestaltung ihres Arbeitsplatzes.

Weitere Informationen auf der Webseite der HU unter A bis Z:

- Arbeits- und Umweltschutz

oder

- Betriebsärzte