

## **B. Bekanntmachungen nach § 78 Abs. 2 NPersVG**

Die nachfolgende Dienstvereinbarung, unterzeichnet vom Präsidium der Gottfried Wilhelm Leibniz Universität Hannover sowie vom Personalrat der Gottfried Wilhelm Leibniz Universität Hannover, ist abgeschlossen worden und am 01.02.2017 in Kraft getreten.

Die Anlagen zu dieser Dienstvereinbarung können bei Herrn Dietrich im Sachgebiet 21 eingesehen werden.

### **Dienstvereinbarung über die Einführung und Anwendung eines Identitätsmanagementsystems mit den daran angeschlossenen Quell- und Zielsystemen an der Gottfried Wilhelm Leibniz Universität Hannover**

**zwischen der Leibniz Universität Hannover und  
dem Personalrat der Leibniz Universität Hannover**

#### **1 Präambel**

Die Leibniz Universität Hannover führt ein Identitätsmanagement ein, über das Zugänge zu zentralen IT-Diensten für Mitglieder, Angehörige und Gäste der Universität abgewickelt werden sollen. Dadurch erfolgt die Nutzerverwaltung in diesen IT-Diensten zukünftig zentralisiert und auf einheitliche Weise.

Das Identitätsmanagement (IdM) wird durch die Zentrale Einrichtung Leibniz Universität IT Services (LUI) betrieben. Aufgrund der verarbeiteten Daten steht es in engem Zusammenhang zum Campus-Management-System SAP-SLcM und dem zukünftig in SAP-HCM realisierten elektronischen Personen- und Einrichtungsverzeichnis (EPV) sowie dem Schnittstellensystem Data Integration Platform (DIP).

Ziel dieser Vereinbarung ist es, im Rahmen einer angemessenen und sinnvollen Nutzung eines zentralen Identitätsmanagements den Schutz der personenbezogenen und personenbeziehbarer Daten vor unzulässigem Gebrauch und unberechtigtem Zugriff zu gewährleisten. Eine Weitergabe von Daten unterliegt dem Grundsatz der Erforderlichkeit nach Datenschutzgesetz. Die Dienststelle und der Personalrat sind sich ferner darüber einig, dass die technischen Möglichkeiten des IDM nicht zur Überwachung des Verhaltens und der Leistung der Beschäftigten genutzt werden, vielmehr ist die Verbesserung von geregelten Zugriffen Ziel des Einsatzes des Identitätsmanagements.

#### **2 Gegenstand**

Diese Dienstvereinbarung wird gem. §§ 59, 60, 64, 66 und 67 i.V.m. § 78 NPersVG (Niedersächsisches Personalvertretungsgesetz) geschlossen. Für die Verarbeitung personenbezogener oder -beziehbarer Daten bei der Leibniz Universität gelten die Bestimmungen des Niedersächsischen Datenschutzgesetzes (NDsG) in Verbindung mit den §§ 88 ff. des Niedersächsischen Beamtengesetzes (NBG) und der Datenschutzrichtlinien der EU.

Sie definiert die Grundsätze für die Einführung und den Betrieb des IdM, das der Verwaltung von Personal-Identitäten und ihnen zugeordneter Ressourcen und Zugriffsberechtigungen, auf der Grundlage einer konsolidierten und ständig aktuellen Datenbasis, dient.

Diese Dienstverarbeitung definiert ebenfalls Grundsätze für Einführung und Betrieb von Systemen, die über Schnittstellen Mitarbeiterdaten in das IdM einspeisen (Quellen) und Systeme, die Mitarbeiterdaten aus dem IdM erhalten (Ziele). Diese Quell- und Zielsysteme haben eigene Begründungen und Grundlagen für ihren Betrieb. Im Rahmen dieser Dienstvereinbarung werden auch Regelungen über eine Dokumentationspflicht dieser angeschlossenen Systeme und der Datenweitergabe getroffen.

#### **3 Geltungsbereich**

Diese Dienstvereinbarung gilt für alle Beschäftigten der Leibniz Universität Hannover.

Alle Mitglieder oder Angehörigen der Hochschule, sowie alle sonstigen Nutzer des Systems (z.B. Externe, Gäste) werden in geeigneter Form über diese Dienstvereinbarung informiert.

#### **4 Systembeschreibung, Leistungsumfang**

Das IdM der Universität verwaltet Zugänge zu unterschiedlichen IT-Diensten. Den bei den verschiedenen IT-Diensten bestehenden Zugängen derselben Person werden konsistente und aktuelle Personendaten aus dem IdM zugeordnet. Für den sicheren Betrieb von IT-Diensten ist eine eindeutige Identität einer Person Best Practice. Bei dem IdM handelt es sich also um ein IT-System, welches den Zugriff zu unterschiedlichen IT-Systemen mit einer Authentifizierung (Feststellung einer Person) ermöglicht. Dazu gehören auch die an die Identität gebundenen Nutzungsberechtigungen für die einzelnen IT-Dienste der Universität. Die Berechtigungen leiten sich aus der Art der Zugehörigkeit einer Person zur Universität ab.

Kernstück des IdM ist eine Datenbank mit angeschlossenen IT-Verzeichnisdiensten. Verzeichnisdienste werden dazu verwendet, Benutzerdaten zentral zu verwalten und den berechtigten IT-Systemen zur Verfügung zu stellen. Im IdM werden Verzeichnisdienste nur für den lesenden Zugriff zur Verfügung gestellt. In der Regel werden sie nur zur Passwortüberprüfung genutzt. Einzelne Dienste nutzen aber auch weitere Informationen wie z.B. Gruppenzugehörigkeit und Teile der Stammdaten. Alle angeschlossenen Zielsysteme sind in Anlage 6 dokumentiert. Siehe auch Ziff. 10 dieser Dienstvereinbarung.

Eng gekoppelt an die Datenbank ist eine WEB-Oberfläche mit der die jeweils Berechtigten Nutzer ihre Daten im IdM einsehen oder ihre Zugänge zu IT-Diensten selbst verwalten können. Außerdem stellt diese WEB-Oberfläche für Dienstbetreiber und Mitarbeiter Verwaltungsfunktionen im Rahmen ihrer im IdM definierten Rollen und Rechte bereit. Der Zugang zu den angeschlossenen Systemen erfolgt ebenfalls nur auf Grundlage der dort festgelegten Rollen und Rechte.

Eine detaillierte Auflistung und Beschreibung des IdM und seine Verankerung innerhalb der Systemarchitektur der Universität ergibt sich aus dem Fachkonzept **Anlage 1**, mit Beschreibung von Aufbau, Funktionen und der grundsätzlichen Arbeitsweise.

#### **5 Ziel und Zweckbestimmung des IdM**

Universität und Personalrat stimmen darin überein, dass der Einsatz des IdM folgenden Zielen und Zwecken dient:

- Automatische Einrichtung persönlich zugeordneter EDV-Ressourcen (IT-Dienste) bei der Einstellung und später als Self-Service
- Automatischer Entzug der EDV-Ressourcen, wenn die Person aus der LUH ausscheidet
- Datensparsamkeit: Jeder Dienst erhält nur die wirklich benötigten personenbezogenen Daten im erforderlichen Zeitraum
- konsistente und aktuelle Zuteilung von Berechtigungen
- regelmäßige Aktualisierung in angeschlossenen Diensten
- Transparenz: Es ist für die Nutzer einsehbar, zu welchem Dienst welche seiner Daten fließen
- Erhöhung der Sicherheit durch personenbezogene Nutzungsrechte und eindeutige Identitäten
- Zentrale Bereitstellung der Nutzeraccounts durch das IdM verringert den administrativen Aufwand in den anderen Einrichtungen der Leibniz Universität

#### **6 Schutz der Persönlichkeitsrechte, Datenschutz**

Anfallende Daten im Sinne dieser Dienstvereinbarung dürfen nur für die hier vereinbarten Zwecke verarbeitet werden.

Die zum Erreichen der Zweckbestimmung dieser Dienstvereinbarung erforderlichen Personendaten die im IdM erhoben, verarbeitet und genutzt werden, sind in **Anlage 2** mit ihrer Zweckbestimmung abschließend aufgeführt und dokumentiert (Datenkatalog)..

Die datenschutzrechtlichen Bestimmungen insbesondere der §§ 88 ff. des NBG sowie des NDSG werden eingehalten. Darüber hinaus verpflichtet sich die Universität zu einem Umgang mit den persönlichen Beschäftigtendaten, der dem Grundsatz der unbedingten Erforderlichkeit der Datenerhebung, -verarbeitung und -nutzung folgt.

Das Datenschutzkonzept mit Beschreibung der Mechanismen, die das IdM vor unberechtigten Zugriffen schützen, das Lösch- bzw. Archivierungskonzept, sowie die Bestätigung des Datenschutzbeauftragten, dass er das System IdM nach datenschutzrechtlichen Vorgaben abgenommen und freigegeben hat, ergeben sich aus **Anlage 3** und der Verfahrensbeschreibung in **Anlage 7**.

Bei Beauftragung externer Dienstleister, die die Auftragsdatenverarbeitung gem. § 6 des NDSG einschließt, ist eine schriftliche Auftragserteilung mit den Mindestinhalten des § 6 Abs. 2 und 3 NDSG notwendig.

## **7 Leistungs- und Verhaltenskontrolle**

Die Nutzung zu weiteren Zwecken, insbesondere für Zwecke der Leistungs- und Verhaltenskontrolle oder zu Zwecken einer Ermittlung von Grundlagen für dienstliche Beurteilungen, Disziplinarmaßnahmen oder als Grundlage für die Feststellung des Gesundheitszustandes ist ausgeschlossen. Daten die aus einer unzulässigen Nutzung stammen, dürfen nicht für arbeitsrechtliche Maßnahmen herangezogen werden. Maßnahmen die auf Informationen beruhen, die unter Verletzung dieser Dienstvereinbarung gewonnen werden, werden nicht durchgeführt.

Wird eine missbräuchliche Nutzung festgestellt, ist die Hochschule verpflichtet, die Ursachen dafür unverzüglich abzustellen und erforderliche Maßnahmen unverzüglich einzuleiten.

Die Universität stellt sicher, dass die Administratoren, Manager und Key-User des IDM-Systems s. **Anlage 4** auf die Einhaltung dieser Dienstvereinbarung verpflichtet werden.

## **8 Berechtigungskonzept - Zugriffsbestimmungen**

Der Zugriff auf die Daten des IdM durch Administratoren, Key-User und Nutzer erfolgt über Zugriffsberechtigungen. Alle Sammel- und Einzelrollen, Berechtigungsprofile, Berechtigungen und Berechtigte sind auf die Fachaufgaben einzugrenzen. Sie sind in dem Berechtigungskonzept geregelt, dass sich aus der **Anlage 4** ergibt.

## **9 Berichte und Auswertungen**

Alle im Zusammenhang mit der Administration des IdM anfallenden Berichte, Auswertungen und Protokoll-daten die im Sinne dieser Vereinbarung personenbezogene Beschäftigtendaten enthalten, dienen ausschließlich den Zwecken der Gewährleistung der Systemsicherheit und der Analyse und Korrektur technischer Fehler. Der Zugriff auf die entsprechenden Programmfunktionen (Accounting-, Monitoring- und Syslog-Funktionen) ist im Berechtigungskonzept geregelt. Diese Daten unterliegen der strikten Zweckbindung gem. § 10 Abs. 4 NDSG.

Alle Berichte, Auswertungen und Protokolle in der Nutzung des IdM sind in **Anlage 5** abschließend aufgeführt. Die Löschung erfolgt entsprechend der Anlagen 3, 5 und 7 und nach den gesetzlichen Fristen.

## **10 Schnittstellen**

Schnittstellen im Sinne dieser Dienstvereinbarung sind technische Übergabepunkte und Verfahren, durch die Daten des IdM an andere Systeme, Funktionen oder Fremdsysteme übergeben werden (Zielsysteme), oder durch die andere Systeme Zugang auf das hier geregelte System erhalten (Quellsysteme).

Quellsysteme des IdM sind Systeme oder Verzeichnisse, die das IdM als Datengrundlage nutzt. Die Speicherung von Daten muss soweit erfolgen, dass eine Identität eindeutig erkannt und zugeordnet werden kann und vom IdM zentral alle Zielsysteme mit den für sie jeweils notwendigen Daten versorgt werden können. Die erfassten Daten werden jeweils pro Quellsystem ermittelt und sind dem zuvor genannten Zweck angepasst. In der Anlage 2 sind die aus den jeweiligen Quellsystemen übernommenen Datenfelder abschließend aufgeführt.

Zielsysteme des IdM sind Systeme oder Verzeichnisse, die das IdM zur Authentifizierung nutzen. Es werden nur diejenigen Daten übergeben, die für die Zweckbestimmung des Zielsystems erforderlich und im Rahmen dieser Dienstvereinbarung für das Zielsystem geregelt sind.

Jedes angeschlossene Zielsystem wird in Form eines Verfahrensverzeichnis, welches dieser Dienstvereinbarung als **Anlage 6** beigelegt wird, dokumentiert. Diese Dokumentation muss folgende Informationen enthalten:

- a) eine grundsätzliche Beschreibung des Systems,
- b) eine Darlegung der Ziele, die mit dem System verfolgt werden,
- c) eine Aufstellung der vom Identitätsmanagement weitergegebenen Datenfelder,
- d) eine Beschreibung, wie das System administriert wird,
- e) eine Beschreibung, wie in dem System Datenschutz gewährleistet wird,
- f) eine Beschreibung und Begründung der Regeln, die der Weitergabe der Daten oder der Zuteilung einer Ressource oder einer Berechtigung zugrunde liegen. Insbesondere ist darzulegen, ob die Regeln grundsätzlich auf einem Automatismus basieren oder durch einen zusätzlichen Administrationsvorgang beeinflusst werden.

Für jedes neu an das IdM anzuschließende System wird die Anlage 6 durch ein entsprechendes Verfahrensverzeichnis ergänzt. Diese Ergänzung unterliegt der Mitbestimmung des Personalrats, welcher das

Recht hat, die Vorlage ergänzender Informationen zu verlangen. Die Mitbestimmung für das anzuschließende System selbst ist dadurch nicht verbraucht.

### **11 Rechte der Beschäftigten, Qualifizierung**

Alle Nutzer des IdM werden rechtzeitig und in geeigneter Art und Weise über die Einführung und Funktionsweise informiert. Sie erhalten auf Anfrage Auskunft über alle zu ihrer Person gespeicherten Daten.

Beschäftigte, deren Aufgaben sich durch die Einführung des IdM ändern, werden rechtzeitig und umfassend geschult und dabei auch über die aus dem Einsatz folgenden Veränderungen der betrieblicher Abläufe informiert. Hierzu werden geeignete Schulungsangebote unterbreitet, die mit dem Personalrat abgestimmt sind. Die Beschäftigten werden mindestens gleichwertig eingesetzt und dafür entsprechend qualifiziert. Herabgruppierungen oder betriebsbedingte Kündigungen sind im Rahmen des Einsatzes von IdM ausgeschlossen.

### **12 Rechte der Personalvertretungen**

Entsprechend § 59 Abs. 2 NPersVG hat der Personalrat die Pflicht und das Recht, die Einhaltung aller einschlägigen Gesetze und Normen zu überwachen. Jede zukünftige Änderung und Erweiterung des in den **Anlagen 1 - 7** dokumentierten Systems unterliegt der Mitbestimmung und Kontrolle des Personalrats. Insbesondere werden keine Funktionen aktiviert, die nicht in den Anlagen dokumentiert sind.

Den Personalräten wird die Teilnahme an allen Sitzungen der an den Projekten beteiligten Arbeits- und Projektgruppen sowie sonstigen Gruppen, die sich mit IdM oder der Anbindung an IdM befassen, ermöglicht.

Die Personalvertretungen haben das Recht, an Fortbildungen, Schulungen und Einweisungen teilzunehmen, soweit diese Kenntnisse vermitteln, die für die Prüfung der Einhaltung dieser Dienstvereinbarung erforderlich sind.

Die Beteiligung von Personalratsmitgliedern in Arbeits- und Projektgruppen ersetzt nicht die Mitbestimmung. Mitbestimmungspflichtige Maßnahmen dürfen erst durchgeführt werden, wenn der Personalrat seine Zustimmung dazu erteilt hat.

Der Personalrat hat das Recht, die Einhaltung dieser Dienstvereinbarung jederzeit zu überprüfen. Außerdem sind ihm auf Wunsch dazu alle zum System gehörenden Handbücher und Systemunterlagen in der aktuellen Version zeitweise zu überlassen. Dazu kann er bei begründetem Bedarf einen externen Sachverständigen seiner Wahl zur Beratung hinzuziehen. Der Sachverständige unterliegt der fachlichen Weisung des Personalrates.

### **13 Schlussbestimmungen, Inkrafttreten, Kündigung**

Durch den Abschluss dieser Dienstvereinbarung und durch die jeweils erteilte Zustimmung des Personalrates zur Produktivsetzung des IdM gilt die Mitbestimmung gem. NPersVG - im Hinblick auf Neueinführung, Änderungen und Erweiterungen – nicht als verbraucht.

Alle in dieser Dienstvereinbarung bzw. der Anlagenübersicht aufgeführten Anlagen sind Bestandteil dieser Vereinbarung. Sie werden regelmäßig aktualisiert und mit Versionsnummer und Erstell- bzw. Änderungsdatum dieser Dienstvereinbarung beigelegt.

Diese Dienstvereinbarung mit Anlagen tritt am 01.02.2017 in Kraft. Sie kann einseitig unter Einhaltung einer Kündigungsfrist von 6 Monaten, frühestens jedoch zum 31.12.2017, gekündigt werden. Sollten einzelne Bestimmungen dieser Vereinbarung insbesondere wegen Verstoßes gegen § 82 NPersVG, nichtig sein oder werden, so berührt dies nicht die Gültigkeit der übrigen Bestimmungen. Anstelle der unwirksamen Bestimmungen, oder zur Ausfüllung eventueller Lücken der Vereinbarung soll eine angemessene Regelung treten, die dem am Nächsten kommt, was die Parteien nach ihrer Zwecksetzung gewollt haben. Die einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform. Im Übrigen gilt § 78 Abs. 4 NPersVG.

Nach Beendigung der Dienstvereinbarung wirken deren Rechtsnormen so lange weiter, bis sie durch neue Regelungen, denen der Personalrat zugestimmt hat, ersetzt werden.

Die Dienstvereinbarung ist allen Beschäftigten in geeigneter Weise bekannt zu machen.

Hannover, den 19.01.2017

Hannover, den 25.01.2017

Leibniz Universität Hannover

Leibniz Universität Hannover

Das Präsidium

Personalrat

gez. Prof. Dr. iur. Volker Epping,  
Präsident

gez. Elvira Grube,  
Vorsitzende

**Anlagenübersicht, Vers.tt.mm.jj**

Anlage 1	Fachkonzept	12.12.2016
Anlage 2	Datenkatalog	12.12.2016
Anlage 3	Datenschutz	12.12.2016
Anlage 4	Berechtigungskonzept	12.12.2016
Anlage 5	Protokolle und Listen	12.12.2016
Anlage 6	Zielsysteme	12.12.2016
Anlage 7	Verfahrensbeschreibung	16.02.2016