UNIVERSITÄTSMEDIZIN GÖTTINGEN UMG

Dienstvereinbarung

über
den Betrieb des Identity-Management-Systems

(DV IDM)

zwischen

der Universitätsmedizin Göttingen
Stiftung Öffentlichen Rechts
- vertreten durch den Vorstand der
Universitätsmedizin Göttingen -

und

dem Personalrat der Universitätsmedizin Göttingen
(ohne Georg-August-Universität Göttingen)

§ 1
Geltungsbereich und Zielsetzung

(1) Die Dienstvereinbarung gilt für alle durch den Personalrat vertretenden Beschäftigten der Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts Universitätsmedizin Göttingen. Für die ehemaligen Beschäftigten gelten die Bestimmungen dieser Dienstvereinbarung mit Ausnahme des § 8 dieser Dienstvereinbarung (nachfolgend insgesamt Beschäftigte). Sie gilt außerdem für an der UMG beschäftigte Endnutzer mit Accounts, die mit dem Identity Management System (IDM) verknüpft sind.

(2) Das IDM dient der Schaffung und Verwaltung einer konsolidierten und ständig aktuellen Datenbasis für die Verwaltung von Identitäten und Berechtigungen innerhalb der Stiftungsuniversität. Es soll die Qualität der Datenerfassung und des Datenabgleichs mit den angeschlossenen Systemen erhöhen. Ein wesentlicher Bestandteil des IDM ist das zentrale Datenverzeichnis.

(3) Diese Dienstvereinbarung dient u.a. der Sicherstellung der Einhaltung der geltenden datenschutzrechtlichen Bestimmungen, des Arbeitsschutzgesetzes[1] (ArbSchG), der Bildschirmarbeitsverordnung[2] (BildscharbV) und des Niedersächsischen Personalvertretungsgesetzes (NPersVG) in der jeweils geltenden Fassung.

§ 2
Begriffsdefinitionen

(1) Eine **Identität** ist der eindeutige Identifikator für eine Person, Organisation, Ressource oder einen Service zusammen mit optionaler zusätzlicher Information (z.B. Berechtigungen, Attributen). Die Identität umfasst eindeutig kennzeichnende Merkmale.
(2) Ein **Account** setzt sich aus Benutzername und Kennwort zusammen und charakterisiert eine Identität.
(3) Ein **Identitäts-Management-System** (IDM) ist ein System zur Verwaltung von Identitäten sowie zur Koordinierung der Weitergabe dieser Identitäten und Berechtigungen an anderen Systeme
(4) Ein System, das über eine Schnittstelle Daten von einem anderen System bezieht, wird als **Zielsystem** bezeichnet.
(5) Ein System, das Daten zur Nutzung oder Weiterverarbeitung für ein anderes System liefert, wird als **Quellsystem** bezeichnet.
(6) Als **Endnutzer** werden Beschäftigte ohne erweiterte Zugriffsrechte auf ein System bezeichnet.
(7) Eine **Berechtigung** bzw. **Rolle** definiert Rechte, Aufgaben und Eigenschaften eines Benutzers im Bereich eines Software- oder Betriebssystems.

[1] Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit
[2] Verordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten

§ 3
Rechtsgrundlagen

(1) Diese Dienstvereinbarung erlaubt den Einsatz des IDM in der Universitätsmedizin Göttingen gem. § 78 i. V. m. § 66 Abs. 1 Ziffer 10 sowie § 67 Abs. 1 Ziffer 1 und 2 NPersVG und hinsichtlich der Verarbeitung personenbezogener Daten gem. der Bestimmungen des Nds. Datenschutzgesetzes (NDSG). Sie bildet die Rechtsgrundlage für den Einsatz des IDM in der Universitätsmedizin Göttingen.

(2) Diese Dienstvereinbarung wird auf der Grundlage der Dienstvereinbarung über die Einführung und Anwendung datenverarbeitender Systeme vom 01.12.1997 (Universitätsmedizin ohne Universität) in der jeweils geltenden Fassung abgeschlossen, die davon unberührt bleibt.

§ 4
Aufgaben und Ziele des IDM

(1) Der durch das IDM ermöglichte Zugriff von Zielsystemen auf Daten, die von den Quellsystemen übernommen werden, darf nur für die nach dieser Dienstvereinbarung zulässigen Zwecke **(Anlage 8)** genutzt werden.

(2) Das IDM ordnet jeder/jedem Beschäftigten der Universitätsmedizin auf der Basis tagesaktueller Personen- und Organisationsdaten eine eindeutige digitale Identität zu. Diese digitale Identität umfasst die folgenden Angaben der/des Beschäftigten: Vorname, Nachname, Titel, Funktion/Beschäftigungsart, Zugriffsberechtigungen für die Nutzung von Informations- und Kommunikationstechnik-Systemen (IT-Systemen). Diese digitale Identität ist die Basis für die automatisierte Zuteilung von Zugriffsberechtigungen. Die Beschäftigten können durch Nachweis ihrer jeweiligen digitalen Identität und entsprechend ihrer Berechtigungen auf personalisierte IT-Dienste der Stiftungsuniversität zugreifen.

(3) Um über tagesaktuelle Informationen von allen Beschäftigten zu verfügen, bezieht das IDM personenbezogene Daten aus dem Personalverwaltungssystem SAP ERP HCM **(Anlage 3)**.

(4) Mit dem Betrieb des IDMs werden darüber hinaus insbesondere folgende Ziele verfolgt:
- Standardisierung von Administrations- und Verwaltungsvorgängen bzgl. der Zugangsverwaltung zu den personalisierten IT-Systemen,
- Erhöhung der Datenqualität der Identitätsdaten,
- Erhöhung des Datenschutzes durch Transparenz bzgl. der Speicherung von personenbezogenen Daten und der zugrundeliegenden Datenflüsse,
- Erhöhung des Datenschutzes durch gezielte Verwaltung von Nutzungsrechten,

- Erhöhung der Sicherheit durch eindeutige digitale Identitäten sowie
- Vermeidung von Mehrfachdatenhaltung in den verschiedenen IT-Systemen.

§ 5
Aufbau, Änderung und Erweiterung des Systems

(1) Eine aktuelle System-Dokumentation zur Administration des IDM ist bei der Betreiberin des IDM, der Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen mbH (GWDG) als Universitätsrechenzentrum, einsehbar.

(2) Die in der **Anlage 3** beschriebenen Daten werden von SAP ERP HCM über eine Schnittstelle an das IDM übergeben und können von Zielsystemen gemäß **Anlage 8** genutzt werden.

(3) Bei der Änderung der Funktionalität und der Prozesse des IDM sowie von Schnittstellen für Quell- und Zielsysteme ist die Inbetriebnahme nur nach vorheriger Zustimmung des Personalrates zulässig.

(4) Die Weitergabe von Account-Daten an die Zielsysteme und die Zuteilung von Ressourcen oder Berechtigungen müssen dem Grundsatz genügen, dass nur diejenigen Daten, Ressourcen und/oder Berechtigungen übergeben werden, die in den Zielsystemen für die Zweckerreichung der jeweiligen Systeme erforderlich sind.

(5) Jedes Zielsystem ist in den **Anlagen 7 und 8** dieser Dienstvereinbarung zu dokumentieren. Diese Dokumentation muss folgende Informationen enthalten:
- Name des Systems und dessen Funktion als Ziel- und / oder Quell-System
- Kurzbeschreibung des Verzeichnisdienstes / der Datenbank und Format der Daten
- Legitimation für den Zugang zum System
- Angabe der für die Anbindung relevanten Attribute sowie deren mögliche Inhalte (Länge, Zeichensatz), die vom/zum IDM übertragen werden
- Angabe möglicher Zielsysteme, die über das IDM versorgt werden
- Ansprechpartner für das System und Abhängigkeiten zu anderen Systemen
- Umfang/Anzahl der existierenden bzw. zu erwartenden Accounts/Objekte
- Datenschutz/Sicherheitsrelevanz und Passwort Vorgaben
- Etwaige redundante Systeme

§ 6
Betreiber des Systems, Auftragsdatenverarbeitung

Das IDM wird von der Gesellschaft für wissenschaftliche Datenverarbeitung (GWDG) als Universitätsrechenzentrum betrieben (nachfolgend: Betreiberin). Systembeschreibung, Zusatzvereinbarung mit

der GWDG, Datenübernahme aus SAP ERP HCM, Verfahrensbeschreibung gemäß § 8 NDSG (Niedersächsisches Datenschutzgesetz), Berechtigungskonzept und Funktionalitäten sind abschließend in den **Anlagen 1 bis 8** dokumentiert und werden bei Bedarf und mit Zustimmung des Personalrats aktualisiert. Die Betreiberin aktualisiert ggf. das Berechtigungskonzept nach **Anlage 6**.

§ 7
Datenschutz

(1) Nach den Anforderungen des § 7 NDSG ist u.a. gewährleistet, dass
- überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist,
- die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können,
- personenbezogene Daten bei der Verarbeitung, Übertragung sowie beim Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können; dies erfolgt entweder durch Verschlüsselung der Daten, deren Entschlüsselung nur dem Absender und der/m Empfänger/in ermöglicht wird oder durch Anbindung von Quellsystemen auf Basis einer sicheren Verbindung (z.B. VPN),
- überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

(2) Nicht mehr benötigte personenbezogene Daten sowie alle Protokolldateien werden spätestens nach sechs Monaten endgültig, sicher und physikalisch von der Betreiberin gelöscht. Die Löschung ist zu protokollieren.

§ 8
Berechtigungen, Pflichten und Gebote

(1) Art und Umfang der Berechtigungen (Personenkreise, Rollen) sind sowohl für das IDM selbst als auch für das Online-Portal des IDM in **Anlage 6** dargestellt und sind laufend durch die Betreiberin zu aktualisieren (s. § 5 Abs. 1).

(2) Die in der **Anlage 6** genannten Administratoren sind verpflichtet, die allgemeinen datenschutzrechtlichen Bestimmungen einzuhalten und über Probleme des Datenschutzes beim Betrieb des IDM umgehend den jeweiligen Datenschutzbeauftragten zu informieren.

(3) Für den Geltungsbereich dieser Dienstvereinbarung gelten die gültigen Rechtsvorschriften der Stiftungsuniversität Göttingen. Das IDM wird nicht eingesetzt, um das Verhalten und die Leistung von Beschäftigten zu kontrollieren oder deren Arbeitsleistung zu intensivieren. Es werden insbesondere keine Auswertungen über Leistungen oder Verhalten einzelner Personen durchgeführt. Verbindliche Dienstanweisungen für die Nutzung und Arbeit mit dem IDM erhält der Personalrat zur Kenntnis.

(4) Alle Endnutzer des Systems erhalten die erforderlichen Einweisungen und Schulungen für die Nutzung des IDM.

§ 9
Rechte der Personalvertretung

(1) Der Personalrat hat das Recht, sich durch einen fachkundigen Administrator alle Funktionen anzeigen und in geeigneter Form (z.B. als Screenshot) dokumentieren zu lassen, welche zur Klärung des jeweiligen Sachverhaltes beitragen.

(2) Gemäß § 30 Abs. 4 Nr. 2 NPersVG hat der Personalrat das Recht, sachkundige Personen seiner Wahl zur Beratung zu den Sitzungen hinzuzuziehen.

§ 10
Schlussbestimmungen, Inkrafttreten, Kündigung

(1) Änderungen dieser Dienstvereinbarung bedürfen der Schriftform.

(2) Diese Dienstvereinbarung tritt mit der Veröffentlichung in den Amtlichen Mitteilungen I in Kraft. Sie kann beim Personalrat, dem Geschäftsbereich Personal oder dem Geschäftsbereich IT eingesehen werden.

(3) Sollten einzelne Punkte dieser Dienstvereinbarung undurchführbar oder unwirksam sein oder werden, so wird dadurch die Durchführbarkeit oder Wirksamkeit dieser Dienstvereinbarung im Übrigen nicht berührt. An die Stelle der undurchführbaren oder unwirksamen Bestimmung soll diejenige durchführbare oder wirksame Regelung treten, die dem möglichst nahe kommt, was die Vertragsparteien mit der undurchführbaren oder unwirksamen Bestimmung beabsichtigten.

(4) Diese Dienstvereinbarung kann von beiden Seiten schriftlich mit einer Frist von vier Monaten zum Ende eines Kalendermonats von jeder Vertragspartei gekündigt werden. Einvernehmliche Änderungen sind jederzeit möglich und bedürfen der Schriftform.

(5) Nach Kündigung verpflichten sich Personalrat und Dienststelle, binnen 3 Monaten Vertragsverhandlungen über eine sachgerechte Neuregelung aufzunehmen. Ziel dieser Verhandlungen ist, innerhalb eines Jahres eine einvernehmliche Regelung zu finden und eine neue Dienstvereinbarung abzuschließen. Nach Abschluss dieses Jahres ist das IDM im Falle einer Nichteinigung binnen einer Frist von 3 Monaten nach endgültigem Scheitern der Verhandlungen außer Betrieb zu nehmen. Bis dahin gelten die Regelungen dieser Dienstvereinbarung sinngemäß weiter.

(6) Die Anlagen dieser Vereinbarung werden fortlaufend aktualisiert und können ohne Kündigung dieser Vereinbarung geändert werden. Der Personalrat wird bei jeder Änderung informiert und ggf. entsprechend dem NPersVG beteiligt.

Göttingen, 23.03.2016

Für die Universitätsmedizin Göttingen
(ohne Universität)

Prof. Dr. Heyo K. Kroemer
Vorstand Forschung und Lehre
Sprecher des Vorstands

Dr. Martin Siess
Vorstand Krankenversorgung

Dr. Sebastian Freytag
Vorstand Wirtschaftsführung und
Administration

Göttingen, 24.03.2016

Für den Personalrat der Universitätsmedizin
(ohne Universität)

Erdmuthe Bach-Reinert
Vorsitzende des Personalrats

Anlagen

1. Systembeschreibung des IDMs (Stand 12.12.2015)
   (Änderung 04.08.2016 im Punkt 7.1.1)
   (Änderung 10.10.2016 im Punkt 7.1.1)
   (Änderung 04.03.2019 im Punkt 7.1.1)
   (Änderung 10.02.2020 im Punkt 7.1.1, sowie 7.1.2)
2. Zusatzvereinbarung mit der GWDG zur Auftragsdatenverarbeitung (Stand: 12.08.2014)
3. Tabelle der zu übernehmenden Attribute aus SAP HR (Stand: 17.12.2014)
   (Änderungen 04.08.2016 Seite 1)
   (Änderungen 10.10.2016 Seite 1)
   (Änderungen 04.03.2019 Seite 1)
   (Änderungen 10.02.2020 Seite 1)
4. Verfahrensbeschreibung gemäß §8 NDSG (Stand 10.03.2016)
5. Datenschutzvorabkontrolle (Stand: 04.09.2013)
   (Änderungen 04.08.2016 Seite 4)
   (Änderungen 10.10.2016 Seite 4)
   (Änderungen 04.03.2019 Seite 4)
   (Änderungen 10.02.2020 Seite 4)
6. Berechtigungskonzept (Stand: 17.12.2014)
7. Übersicht der Zielsysteme (Stand: 17.12.2014)
8. Dokumentation der Zielsysteme gemäß §4 Abs.6
   a. Zielsystem AD der Uni (Stand: 07.09.2013)
   b. Zielsystem SAP HR (Stand: 25.02.2016)
      (Änderungen 04.08.2016 Seite 2)
      (Änderungen 10.10.2016 Seite 2)
      (Änderungen 04.03.2019 Seite 2)
      (Änderungen 10.02.2020 Seite 2)
   c. Zielsystem SAP KiS (Stand: 25.02.2016)
   d. Zielsystem UniVZ (Stand: 07.08.2013)
   e. Zielsystem Active Directory (Verzeichnisdienst) der UMG (Stand: 26.02.2016)