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: 15.12.2015)
2. Zusatzvereinbarung mit der GWDG zur Auftragsdatenverarbeitung (Stand: 12.08.2014)
3. Tabelle der zu übernehmenden Attribute aus SAP HR (Stand: 17.12.2014)
4. Verfahrensbeschreibung gemäß §8 NDSG (Stand: 10.03.2016)
5. Datenschutzvorabkontrolle (Stand: 04.09.2013)
6. Berechtigungskonzept (Stand: 17.12.2014)
7. Übersicht der Zielsysteme (Stand: 17.12.2014)
8. Dokumentationen der Zielsysteme gemäß § 4 Abs. 6
   a) Zielsystem AD der UNI (Stand: 07.09.2013)
   b) Zielsystem SAP HR (Stand: 25.02.2016)
   c) Zielsystem SAP KIS (Stand: 25.02.2016)
   d) Zielsystem UniVZ (Stand: 07.09.2013)
   e) Zielsystem Active Directory (Verzeichnisdienst) der UMG (Stand: 26.02.2016)

Anlage 1:

Systembeschreibung Identity-Management-System

1. Übersicht

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

Als Werkzeug wurde bereits 2005 die Software Novell Identity-Manager (zwischenzeitlich von NetIQ mittlerweile von MicroFocus) ausgewählt und in einer ersten Stufe in Betrieb genommen. Schwerpunkt der ersten Phase war jedoch lediglich die Synchronisierung der verschiedenen Verzeichnisse der GWDG und der Universität (Windows AD sowie LDAP). In der jetzt anstehenden Stufe soll eine einheitliche Verwaltung von Accounts für Beschäftigte der Universität erreicht werden.

Grundsätzliche Ziele des IDM:

- Einheitliche Verwaltung von Benutzeraccounts für alle Nutzergruppen und für die wichtigsten Dienste am Wissenschaftsstandort Göttingen mit einer automatischen Generierung von Accounts (E-Mail, PC-Anmeldung),
- Abbildung des kompletten Lebenszyklus der Mitarbeiter/innen von der Ausstattung mit den notwendigen Berechtigungen bei der Einstellung bis hin zur Abgrenzung der Berechtigungen bei Vertragsende,
- Erfüllung von Anforderungen bezüglich der Ausstattung von Mitarbeiter/innen mit persönlichen Accounts,
- Integration / Erweiterung sowie Vereinheitlichung der Selbstbedienungsfunktion im Rahmen des Benutzerportals (dadurch eine Erhöhung der Effizienz der Servicebereiche) sowie
- Vorbereitung für die Etablierung des **S**ingle**S**ign**O**n (SSO).

Um die am Universitätsstandort Göttingen verfügbaren Dienste wie E-Mail, Massenspeicher usw. möglichst zeitnah und unkompliziert neuen Mitarbeiter/innen der Universität zur Verfügung zu stellen, werden mit dem IDM zukünftig eine Vielzahl von Prozessen automatisiert.
Das IDM wird zu Beginn ausschließlich Personen betreffen, die ab diesem Zeitpunkt ein Arbeits- oder Dienstverhältnis mit der Universität eingehen. Hierbei wird der Account erzeugt und weitere erforderliche Prozesse (z.B. die Generierung einer zum Account gehörenden E-Mail-Adresse) automatisiert durchlaufen, um die Person zeitnah arbeitsfähig zu machen. Die Vielzahl existierender Identitäten (Accounts) im IDM selbst sowie in den am IDM angebundenen Verzeichnissen ist hiervon unberührt. Da eine Verknüpfung zwischen den existierenden Identitäten und den Daten aus SAP HR nur sehr schwer möglich ist, wird dieser Verknüpfungsprozess zu einem späteren Zeitpunkt realisiert.

2. Produkt

Software Novell Identity-Manager (von MicroFocus)

3. Funktionsbeschreibung und Darstellung der Organisation der IT-Architektur

Die folgende Grafik beschreibt die Schritte nach Erhalt des Arbeitsvertrages bis zur Nutzung der Basisdienste:

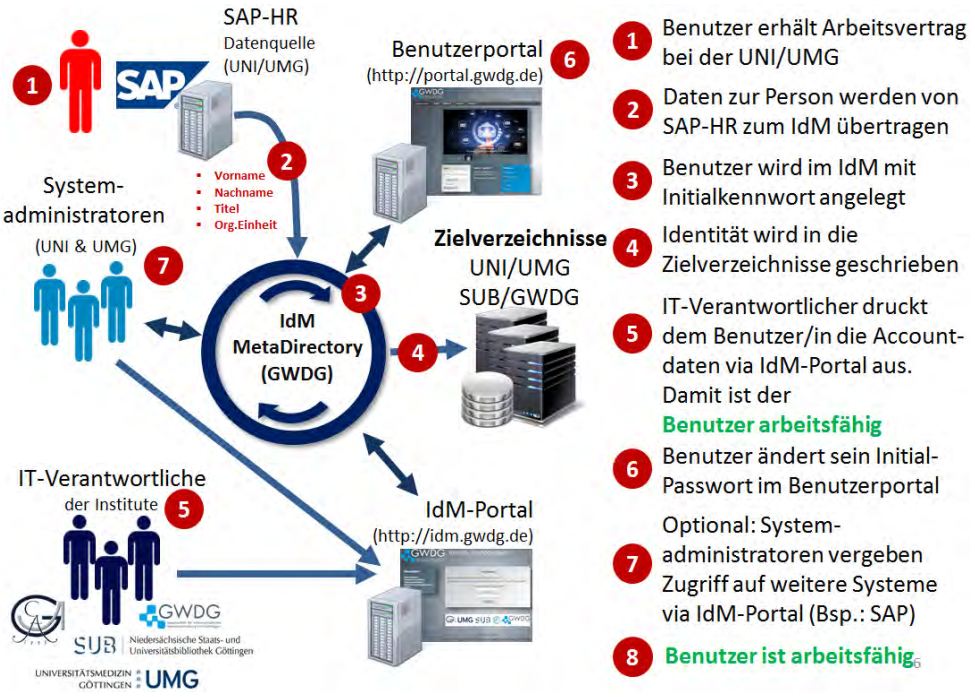


Abbildung *Schritte zur Nutzung der Basisdienste*

Die Basisdienste umfassen die Nutzung von E-Mail (Exchange), der WLAN-Dienste (EDUROAM und GoeMobile) sowie auch der Dienste von Windows Active Directory mit den entsprechenden Laufwerksfreigaben.

4. Erläuterung der Änderungen, die sich für die betroffenen Beschäftigten ergeben.

An dem IDM sind verschiedene Einheiten der Universität und der Universitätsmedizin beteiligt (UMG-IT, SUB-IT, UNI-IT und GWDG sowie die Systemadministratoren SAP HR aus den Personalabteilungen der UMG und der UNI). Darüber hinaus sind sehr viele weitere Systeme aus den beteiligten Bereichen vom IDM betroffen.

4.1 Abbildung entscheidender Prozesse

4.1.1 Eintritt

Wenn eine Person ein Arbeitsverhältnis bei der Universität beginnt, wird dieses zunächst in der Anlage der Stammdaten im SAP HR sichtbar. Von diesem Zeitpunkt an - basierend auf den in SAP HR angegebenen Daten - beginnt das IDM alle weiteren Schritte automatisiert in der angegebenen Reihenfolge abzuarbeiten. Ziel ist die möglichst schnelle Herstellung der Arbeitsfähigkeit einer Person durch Anlage ihres Accounts im IDM und damit in allen relevanten am IDM angebundenen Systemen.

4.1.2 Organisationswechsel

Der Wechsel einer Person von einer Einrichtung der Universität in einen anderen Bereich wird im Rahmen der abgestimmten Prozesse abgebildet. Dabei bleiben die Accountdaten (username sowie E-Mail-Adresse(n)) erhalten. Ausgenommen davon ist ein Wechsel zwischen Universität und Universitätsmedizin. Dieser Prozess wird manuell vollzogen.

4.1.3 Austritt

Bei Austritt einer Person werden unterschiedliche Prozesse in Abhängigkeit des Personenkreises durchlaufen. Hierbei wird Folgendes unterschieden:

Personenkreis	Laufzeit des Accounts nach Austritt	Sperrung in SAP-Systemen
Professor/innen	Kein Ablauf	sofort
Professor/innen bei Wechsel der Hochschule	1 Jahr	sofort
Wissenschaftliche Mitarbeiter/innen	6 Monate	sofort
MTV-Mitarbeiter/innen	Deaktivierung mit Austrittsdatum	sofort
Studierende	2 Semester	--

Tabelle 1 *Laufzeiten des Accounts nach Austritt*

Gleichzeitig werden vom IDM Benachrichtigungen (E-Mail) an die Person selbst sowie an zuständige IT-Administratoren verschickt. Diese E-Mail enthält Informationen darüber, wann der Account gesperrt wird.

4.1.4 E-Mail-Adressen

Ein Ziel des IDM ist eine Vereinheitlichung des Formates bei den E-Mail-Adressen von neuen Mitarbeiter/innen Das neue Format der E-Mail-Adresse enthält keine Angabe der Fakultät. Bereits bestehende E-Mail-Adressen, welche einer Person zugeordnet sind, bleiben im bisherigen Format bestehen, um bestehende Abläufe nicht zu beeinträchtigen. Eine etwaige bereits bestehende primäre E-Mail-Adresse bleibt unverändert. Das gilt auch für bereits existierende Proxy-Adressen (Alias) einer Person. Auch nach Einführung des IDM ist ein Hinzufügen von E-Mail-Aliassen möglich. Diese können auch die Fakultät bzw. die Zentralverwaltung (ZVW) als Bestandteil der E-Mail-Adresse enthalten. Bereits existierende Personen erhalten im IDM eine zusätzliche E-Mail-Adresse, die dem neuen

Format des IDM entspricht. Bereits bestehende E-Mail-Adressen des Benutzers bleiben dabei erhalten.
Folgende Formate für die primäre E-Mail-Adresse werden durch das IDM erzeugt:

Einrichtung	Format	Bemerkung
Universität, SUB	hans.mustermann@uni-goettingen.de	Keine Angabe der Fakultät. Möglichkeit zur Vergabe von Aliassen.
Universitätsmedizin	hans.mustermann@med.uni-goettingen.de	Angabe der Medizinischen Fakultät (med).
Studierende	hans.mustermann@stud.uni-goettingen.de	Ist bereits etabliert.

Tabelle 2 *Gültige Formate für E-Mail-Adressen*

Existiert keine E-Mail-Adresse bzw. ist das Benutzerobjekt im IDM nicht vorhanden (bei Neuanlage), wird die E-Mail-Adresse nach dem o. g. Format automatisch erzeugt. Sollte eine E-Mail-Adresse bereits existieren, wird der bestehenden E-Mail-Adresse - analog zur Gestaltung der UserID - eine Ziffer hinzugefügt, um die Eindeutigkeit zu gewährleisten.

Es besteht weiterhin die Möglichkeit, neben der durch das IDM vergebenen, auch weitere E-Mail-Adresse mit Angabe der Fakultät hinzuzufügen, so dass der Endbenutzer unter allen definierten E-Mail-Adressen erreichbar ist.

Eine E-Mail-Adresse wird innerhalb von 15 Jahren nicht neu vergeben. Dies gilt für die primäre- sowie alle weiteren E-Mail-Adressen (Aliasse) einer Person. Tritt eine Person aus der Universität aus, so wird die E-Mail-Adresse für den Zeitraum von 15 Jahren nicht mehr erneut verwendet.

4.1.5 User-ID

Das Namensschema entspricht den Namenskonventionen in SAP-Systemen.
Hierbei sind folgende Kriterien bindend:

- Benutzername entspricht dem Nachnamen (z.B. Mustermann, Klaus → mustermann),
- Umlaute und ß werden umgesetzt (z. B. aus „ö“ wird „oe“, aus „ß“ wird „ss“),
- Bei Doppelnachnamen wird nur der erste Nachname verwendet. Präfixe dürfen nicht durch Leerzeichen oder Bindestrich abgetrennt sein (z. B. Frau Mars-Venus → „mars“, Herr Mc Geiz → „mcgeiz“, Frau Al-Battani“ → „albattani“).
- Die maximale Länge des Benutzernamens beträgt 12 Stellen.
- Wenn dieser bereits vorhanden ist, wird ein Zeichen am Ende abgeschnitten und eine Zahl angefügt (z. B. Frau Musterperson, Karin → „musterperso1“). Wenn der neue Benutzername ebenfalls vorhanden ist, wird weiter hochgezählt.
  (Wenn es schon 9 Personen mit dem Namen MusterpersoX gibt, dann bekommt die neue Person den Accountnamen „musterpers10. Später kann „musterper100“ generiert werden.)

4.1.6 Passwort und Passwortvorgaben

Für die Nutzung eines einheitlichen Passwortes über Systemgrenzen hinaus und die Vorbereitung für eine flächendeckende Nutzung von SingleSignOn ist eine Vereinheitlichung des Passwortes in allen angebundenen Systemen erforderlich. Da SAP-Systeme der höchsten Sicherheitsanforderung unterliegen, und diese Sicherheitsvorgaben nicht abgesenkt werden können, gelten für das IDM entsprechend die SAP-Vorgaben. Diese Vorgaben gelten somit zugleich in allen anderen am IDM angebundenen Systemen. Eine Überprüfung der Passwörter und Einhaltung der Passwort-Vorgaben wird durch das IDM und die daran angebundenen Portale gewährleistet. Insbesondere bei Änderungen von Passwörtern durch den Benutzer selbst findet die Überprüfung der Gültigkeit im IDM statt, bevor das geänderte Passwort in die Zielsysteme geschrieben wird.
Eine Passwort-Übersicht der letzten 5 gesetzten Passwörter wird hierbei im IDM realisiert und überwacht. Hierdurch wird ausgeschlossen, dass bereits vergebene Passwörter durch dieselbe Person erneut verwendet werden können. Dieses Verfahren wirkt sich unmittelbar auf die angebundenen Verzeichnisse aus. Da Passwortänderungen zukünftig ausschließlich über das Benutzer-Portal im Rahmen der Selbstbedienungsfunktion des Benutzers erfolgen sollen, wäre damit auch die Passwort-Historie im IDM (Benutzer-Portal) für die angebundenen Verzeichnisse bindend.

4.1.7 Vorteile und Konsequenzen einer zentralen Passwortvorgabe

Die Einführung eines Passwortes, welches für mehrere Dienste gleichermaßen nutzbar ist, bringt insofern einen Gewinn an Sicherheit, als sich der Endnutzer für unterschiedliche Systeme nur ein Passwort merken muss und dadurch dieses Passwort hinreichend komplex gestalten kann. Entscheidend ist, dass durch die Einführung zentraler Passwort-Vorgaben auch alle am IDM angebundenen Systeme dieses Format zwingend beherrschen. Entsprechend gelten damit auch in allen angebundenen Verzeichnissen ab Einführung die zentralen Bestimmungen für Passwörter. Dies gilt insbesondere für die Regel, dass ein Passwort alle 3 Monate zu ändern ist. Das gilt allerdings nur für die Benutzer, die auch in der Vergangenheit unter diese Regel fielen.

4.1.8 Kriterien der Passwortvorgabe

1.) Vorgaben wie in den SAP-Systemen schließt Personen ein, die keinen Zugang zu SAP-Systemen erhalten. Bestehende, ggf. unsichere Passwörter bereits existierender Accounts im IDM bleiben erhalten. Lediglich bei der nächsten Passwortänderung (am IDM-Portal) muss ein Benutzer die verschärften Passwort-Vorgaben beachten.
   a. Das Password für einen SAP-Benutzer darf in den ersten drei Zeichen kein „!“ oder „?“ enthalten (siehe Anlage SAP Kennwortrichtlinien).
   b. Das Passwort für einen SAP-Benutzer darf nicht in der in SAP geführten Ausschlussliste enthalten sein.
   c. Historisierung der Passwörter.
2.) Ein einheitliches Passwort ist ferner für die Einführung von Single-Sign-On-Verfahren erforderlich. Eine Abschaltung der Änderung von Kennwörtern im SAP ist jedoch nicht möglich. Daher ist es an dieser Stelle wichtig die Endnutzer über die Prozesse zur Kennwortänderung zu informieren.
3.) Die Passwortvorgaben erfordern eine Passwortänderung alle 3 Monate. IDM wird die Benutzer automatisch per E-Mail auffordern, das Passwort zu ändern. Die Passwortänderungen geschehen ausschließlich über das Kunden-Portal durch den Benutzer selbst und betreffen alle

Bereiche der Universität.

4.) Das Passwort wird durch den Administrator nur und ausschließlich im IDM-Portal oder in der Selbstbedienungsfunktion des Benutzerportals durch den Benutzer selbst geändert.

5.) Die SAP-Passwort-Vorgaben werden im IDM-Portal bzw. Benutzerportal überwacht und eingehalten.

6.) Die Initial-Passwörter werden im IDM generiert (z. B. bei Neueinstellung einer Person). Eine Synchronisation der Passwörter aus SAP ist technisch nicht möglich und erfolgt ausschließlich vom IDM zu den SAP-Systemen.

7.) Da das Passwort im IDM abgelegt ist, wird damit eine Änderung eines Passwortes auch in allen anderen Systemen erreicht.

8.) Die frühere Möglichkeit zur gesonderten Passwortänderungen in einzelnen Systemen / Verzeichnissen wird grundsätzlich technisch ausgeschlossen. Ist dies technisch nicht möglich, so muss im Rahmen einer Handlungsanweisung in den betroffenen Systemen darauf hingewiesen werden, dass Passwortänderungen ***nicht*** in den Zielsystemen selbst vorgenommen werden dürfen.

4.1.9 Systeme/Funktionen mit hohem Schutzbedarf (zweites Passwort)

Eine Aufteilung in die Schutzklasse I sowie Schutzklasse II ist für Dienste mit höheren Schutzanforderungen bzw. von Personen in einer besonderen Rolle erforderlich. Hierbei ist ein zweites Passwort zu verwenden, um höhere Sicherheitsanforderungen zu gewährleisten. Daraus folgt ein einheitlicher Account mit einem gesonderten Passwort für Dienste / Personen / Rollen mit höheren Sicherheitsanforderungen (z. B. SAP-Hauptnutzer FI / CO / HR / ISH). Das betrifft insbesondere Personen, die Zugriff auf SAP-Systeme oder weitere Systeme erhalten, welche einem besonderen Schutz durch das Passwort bedürfen. Hintergrund sind Bedenken, dass durch Einführung nur eines Passwortes des Benutzers für alle Systeme der Zugriff auf besonders schützenswerte Daten erleichtert wird.
Eine Änderung des zweiten, sicherheitsrelevanteren Passwortes wird durch den Benutzer über das Kundenportal nur durch ein weiteres Sicherheitskriterium (Bsp.: Bestätigung via SMS) möglich sein.

1. Berechtigungskonzept

Dieses Kapitel stellt das Berechtigungskonzept für die folgenden Komponenten dar:

- Identity-Management-System (IDM), Metadirectory von NetIQ/MicroFocus bei der GWDG,
- IDM-Portal bei der GWDG sowie
- Endnutzer-Portal bei der GWDG.

Für die Komponenten des IDM sowie die daran angeschlossenen Portale existieren drei grundlegende Rollen:

1.) **IDM-Administrator:** besitzt uneingeschränkten Zugriff auf alle Bereiche mit allen Attributen des IDM.

2.) **Institutsadmin:** sind Administratoren der jeweiligen Instituts- sowie Abteilungs- und Stabsstellenbereiche. Diese Personen bekommen lesenden Zugriff auf alle in dem Institut

oder der Abteilung oder Stabsstelle zugehörigen Daten der Institutsadministrator hat aber nur für ein Teil der Daten Schreibrechte (z.B. Initialisierung eines neuen Kennwortes).

3.) **Endnutzer:** sind die Mitarbeiterinnen und Mitarbeiter, welche im Rahmen der Selbstbedienungsfunktion einige der zur eigenen Person gehörenden Attribute (Datenfelder einer Identität) ändern können. Dieses ist insbesondere die Adresse, Telefonnummern sowie das/die Passwörter. Änderungen an Vor- sowie Nachname, UserID, primärer eMail-Adresse des Benutzers sind weder durch den Benutzer noch durch den Administrator oder den zuständigen Institutsadministrator möglich.

Berechtigungskonzept IDM (MetaDirectory)

Identity-Management (IDM, MetaDirectory)					
Personen	**Institution**	**Rolle**	**Anzahl der Personen**	**Zugewiesene Rechte**	**Zielbereich**
IDM-Administratoren	GWDG	Administrator	3	• Lesen • Schreiben • Ändern • Löschen	Alle Objekte / alle Attribute im gesamten IDM
Administratoren der einzelnen Institute und Abteilungen der Universität	UNI	Instituts-administrator	186, für die jeweiligen 186 Institutsbereiche	• Lesen • Schreiben • Ändern • Einfügen von Identitäten	Nur Objekte des jeweiligen Institutsbereiches

Tabelle 3 *Berechtigungskonzept IDM*

Berechtigungskonzept IDM-Portal

IDM-Portal (http://idm.gwdg.de)					
Personen	**Institution**	**Rolle**	**Anzahl der Personen**	**Zugewiesene Rechte**	**Zielbereich**
IDM-Administratoren	GWDG	Administrator	3	• Lesen • Schreiben • Ändern • Löschen	Alle Objekte / alle Attribute im gesamten IDM
Administratoren der einzelnen Institute und Abteilungen der Universität	UNI	Instituts-admin	186, für die jeweiligen 186 Institutsbereiche	• Lesen • Schreiben • Ändern • Einfügen von Identitäten	Nur Objekte des jeweiligen Institutsbereiches

Tabelle 4 *Berechtigungskonzept IDM-Portal*

Endnutzerportal (http://portal.gwdg.de)					
Personen	**Institution**	**Rolle**	**Anzahl der Personen**	**Zugewiesene Rechte**	**Zielbereich**
IDM-Administratoren	GWDG	Administrator	3	• Lesen • Schreiben • Ändern • Löschen	Alle Objekte / alle Attribute im gesamten IDM
Endnutzer	UNI	Endnutzer	Alle Personen von UNI / GWDG	• Lesen • Schreiben • Ändern	Nur Attribute des eigenen Benutzerobjektes. Geändert werden können hierbei nur die Attribute: • Passwort • Passwort-Vergessen-Funktion • zusätzliche eMail-Adressen • zusätzliche Adressen • zusätzliche Telefonnummern

Tabelle 5 *Berechtigungskonzept Benutzerportal*

2. Zusätzliche Dokumente

Zusatzvereinbarung zur Auftragsdatenverarbeitung personenbezogener Daten zwischen der Georg-August-Universität Göttingen/Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts und der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen vom 24.11.2014.

7. Anwendungen

7.1 IDM Quell- und Zielsysteme

Als primäre Datenquelle für das IDM wird ausschließlich das SAP-System HR verwendet werden.

Insbesondere im SAP HR gibt es verschiedene standardisierte Abläufe, um Daten in Abhängigkeit von einem eingetretenen Ereignis zu pflegen (sogenannte „Maßnahmen“). Eine solche Maßnahme hat Auswirkungen auf den Account sowie auf Berechtigungen einer Person in weiteren Systemen. Die zu berücksichtigenden Maßnahmen sind:

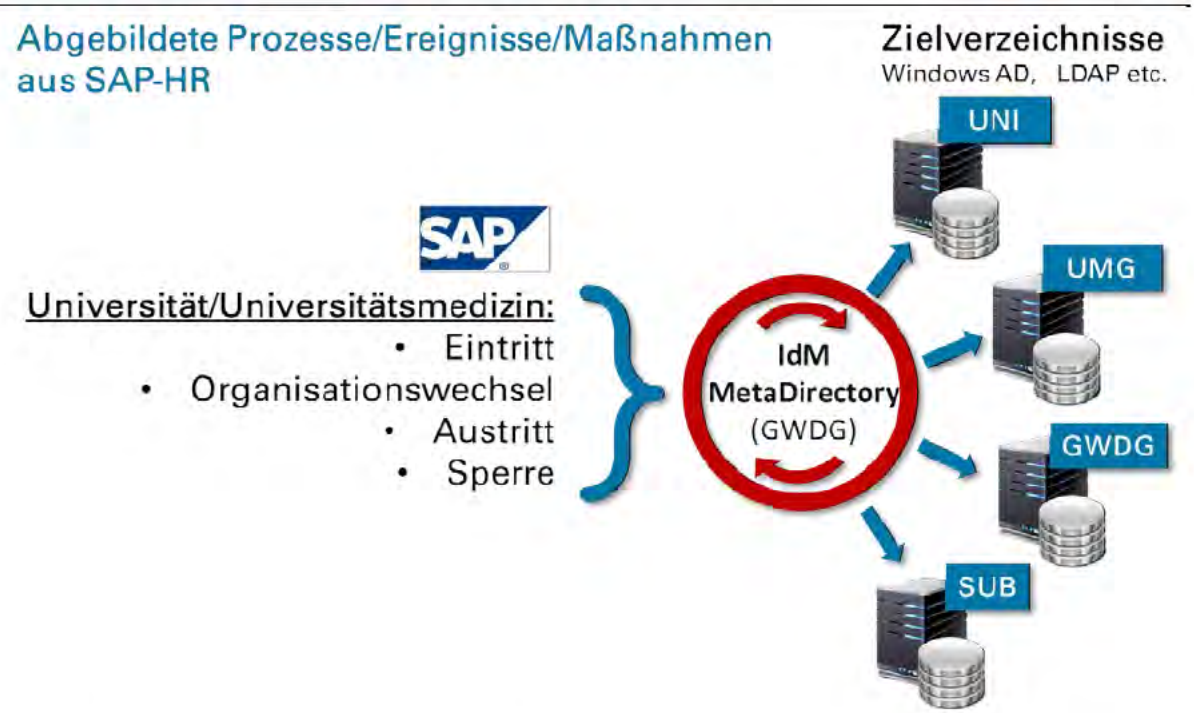


Abbildung Fehler! Es wurde keine Folge festgelegt. *Berücksichtigte Maßnahmen aus SAP-HR*

Der Organisationswechsel muss nicht zwingend in SAP HR als Maßnahme (standardisierter Ablauf) durchgeführt werden, sondern kann auch im IDM anhand der Änderung des Inhaltes von Organisationsschlüssel bzw. von Organisationseinheit (Änderung Stammdaten) als Ereignis (iDOC) erkannt werden. Ein Organisationswechsel zwischen den Bereichen Universität und UMG wird nicht automatisiert abgebildet.

7.1.1 Zu übertragende Attribute aus SAP HR

Wegen der Anbindung an SAP-HR verwendet IDM SAP-HR-Attribute. Ein geringerer Teil der Attribute wird im IDM selbst gespeichert. Eine noch kleinere Teilmenge davon wird auch in die an dem IDM angebundenen Zielverzeichnisse geschrieben (z. B. Windows AD der Universität).

Von den Attributen, die zur Bearbeitung der Prozesse erforderlich sind, werden im IDM bzw. im Zielverzeichnis die folgenden aufgeführten Attribute gespeichert.

Feldname	For-mat	Inhalt	Bemerkung

Persnr	C 8	Personalnummer IT0001-PERSNR	Dient zur Identifikation der jeweiligen Person (Bei Änderung in der Namensgebung)
Werks	C 4	Personalbereich IT0001-WERKS	Dient zur Unterscheidung der Personen aus den verschiedenen Organisationseinrichtungen (z. B. UMG, UNI)
Persg	C 1	Mitarbeitergruppe IT0001-PERSG	Dient zur Identifikation der aktiven Mitarbeiter bzw. emeritierten Profs.
Persk	C 2	Mitarbeiterkreis IT0001-PERSK	Dient zur Einschränkung der Personalstammdaten die an das IDM weitergeleitet werden (z.B. werden Sterbegeldempfänger im IDM nicht angelegt)
Nachn	C 40	Nachname IT0002-NACHN	Basisinformationen
Vorna	C 40	Vorname IT0002-VORNA	Basisinformationen
Namzu	C 15	Namenszusatz IT0002-NAMZU	Basisinformationen
Vorsw	C 15	Namensvorsatz IT0002-VORSW	Basisinformationen
Titel	C 15	Akad. Titel IT0002-TITEL	Basisinformationen
Geschlecht	C 1	Geschlecht IT0002-GESCH	Basisinformationen
Telnr	C 30	Telefonnummer IT0105-USRID, Subtyp 9200	Nur die dienstliche Telefonnummer - dient der Qualitätssteigerung in den verschiedenen Zielsystemen.
Matrikelnr	C 30	Matrikelnummer IT0105-USRID, Subtyp 8000	Dient der Identifikation einer bereits im IDM vorhanden Person um sicherzustellen, dass jede Person nur eine Identität im IDM erhält. Dabei kann die Identität mehrere Accounts haben (z. B. Abgleich Studierender). Dieses Matching kann jedoch nicht das Matching über Name, Geburtsdatum und Geburtsort ersetzten, da keine vollständige Datenhaltung im SAP existiert.
SUB_Barcode	C 8	Barcodenummer für Zutritt SUB IT0050-ZAUSW	Basisinformation für SUB-Dienste und -systeme.
Kostenstelle	C 12	Kostenstelle IT0001-KOSTL	Die primäre Kostenstelle, die zur Person in SAP HR zugeordnet wurde. Für die Benutzerverwaltung in den SAP-Systemen relevant.
Feldname	**Format**	**Inhalt**	**Bemerkung**

SAP_Kennung	C 30	SAP Kennung IT0105-USRID, Subtyp 0001	Dient zur Identifikation im IDM von existierenden SAP HR-Accounts. Diese Information wird nur bei einigen Personen (die bereits einen SAP-Account haben) übertragen.
NHG	C 1	Gruppe NHG IT9000-WAHL_NHG	Dieses Attribut ermöglicht die Identifikation von Hochschullehrern/ Hochschullehrerinnen, von wissenschaftlichen Beschäftigten und von MTV-Beschäftigten. Es gibt unterschiedliche Nutzungsszenarien bzgl. der Accounts bei Beendigung des Arbeitsverhältnisses.
Orgeh_sh	C 12	Kürzel Organisationseinheit IT1000-SHORT	Beinhaltet auf Universitätsseite die Kostenstelle bzw. die Innenauftragsnummer der jeweiligen Einrichtung
Inst_sh	C 12	Kürzel Institut IT1000-SHORT (Für die Uni: in der OM-Hierarchie das erste O-Objekt mit dem Feld IT1000-SHORT mit einem '-' an der vierten Stelle)	Beinhaltet auf Universitätsseite die Kostenstellengruppe der jeweiligen Einrichtung. Dient bei UniVZ der automatischen Zuordnung von Personen zu Einrichtungen.
Fak_sh	C 12	Kürzel Fakultät IT1000-SHORT (Für die Uni: in der OM-Hierarchie das erste O-Objekt mit dem Feld IT1000-SHORT mit einem '-' an der dritten Stelle)	Basisinformation.
Maßnahme	C 2	Eintritte, Austritte sowie Organisationswechsel	Dient der automatischen Weiterleitung für Deaktivierungen von Accounts an die Zielsysteme (Sperrung von Zugriffen nach Austritt von MA)
IDM-Status	C 2	Statusfeld für Schnittstelle HR2IDM	Attribut zur Steuerung der Übertragung von Daten an das IDM (z. B. können Accounts in Ausnahmefällen von der Personalabteilung gesperrt werden oder die Übertragung von Stammdaten bestimmter Personen ausgesetzt werden).
Personen-ID	C 8	Eindeutiger Schlüssel zur Identifikation von Personen im HR	Dient der Sicherstellung der Zusammenführung von verschiedenen Personalnummern pro Person. Dieses Attribut wird voraussichtlich im Jahr 2013/2014 eingeführt.

Die folgende Tabelle enthält alle Attribute, die im IDM gespeichert sowie teilweise in einige Zielverzeichnissen übertragen werden.

Beschreibung	Attribut im IdM	Attribut in den Zielverzeichnissen
Vorname	Vorname	Vorname
Nachname	Nachname	Nachname
Personalnummer	Personalnummer	Personalnummer
Titel	Titel	Titel
Geschlecht	-	-
Telefonnummer	Telefonnummer	Telefonnummer
Org.Schlüssel/Org.Einheit	Org.Schlüssel/Org.Einheit	Org.Schlüssel/Org.Einheit/[indirekt durch OU]
Kostenstelle	Kostenstelle	Kostenstelle /[indirekt durch OU]
Unterscheidung: Professoren/Wissenschaftl. Mitarbeiter/Mitarbeiter	NHG	NHG
Personalbereich (UNI/UMG)	Werks	Mandant
E-Mail-Adresse(n)	eMail	eMail
User-ID	uid	UID
Beschäftigungsstatus	userStatus	userStatus
Eintrittsdatum	Eintrittsdatum	Eintrittsdatum
Austrittsdatum	Austrittsdatum	Austrittsdatum

7.1.2 HR Rückfluss von Attributen aus dem IDM

Aus dem IDM müssen selbstverständlich auch Werte zurückfließen. Nach der Generierung des Accounts im IDM wird die E-Mail-Adresse erzeugt und zum SAP HR übertragen.
Weiterhin werden auch die im IDM generierte UserID (UID), die auch gleichzeitig den SAP-Usernamen darstellt, und das Passwort übertragen. Für die Personalverwaltungen ist die vom IDM zurückgeschriebene UID sowie die E-Mail-Adresse ein Hinweis für die erfolgreiche Anlage der Identität im IDM.

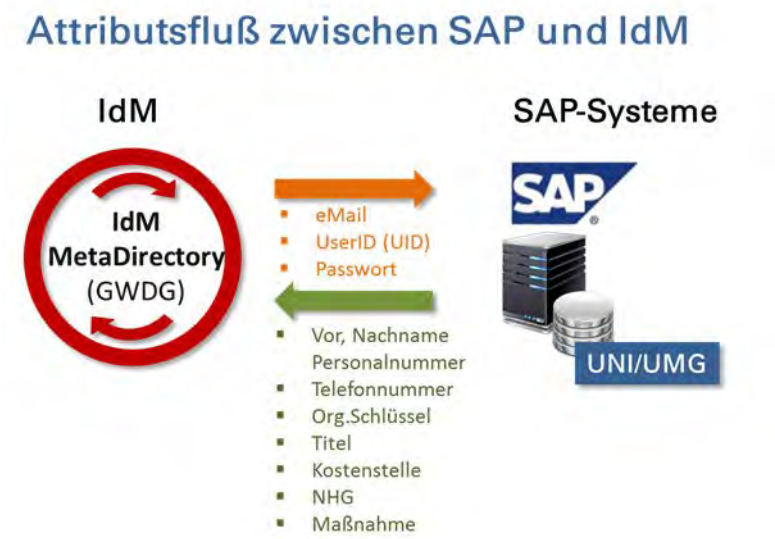


Abbildung 3 *Attributfluss zwischen SAP und IDM*

7.1.3 **Anschluss von Zielsystemen**

Über das IDM ist eine Vielzahl von Zielverzeichnissen angebunden, in die nach definierten Regeln die Daten geschrieben werden. *Abbildung 4* zeigt die Quell- und Zielverzeichnisse, welche am IDM der GWDG angebunden sind.

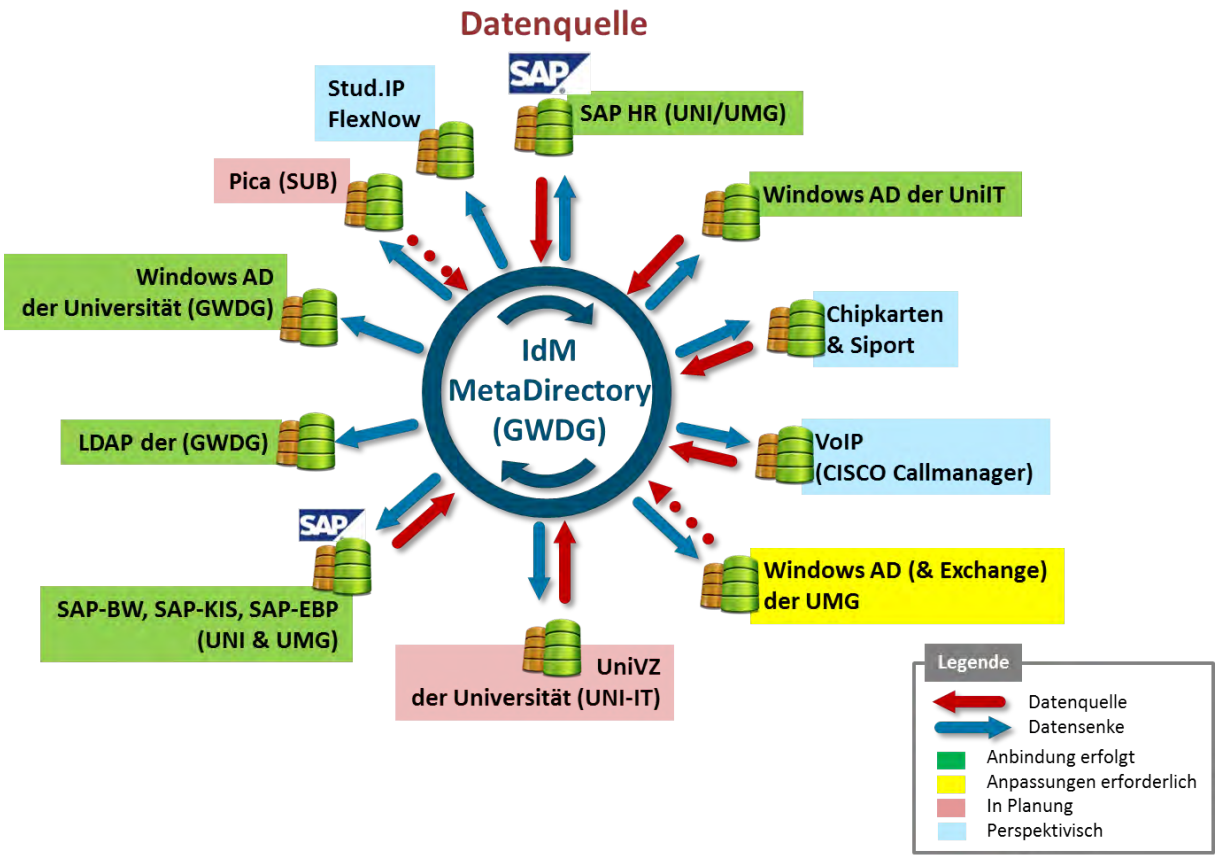


Abbildung 4 *Quell- und Zielverzeichnisse am IDM (Stand: 7/2015)*

Da unterschiedliche Zielverzeichnisse am IDM angebunden sind, müssen auch die Besonderheiten dieser Zielverzeichnisse berücksichtigt werden. Diese Aufgabe übernimmt zentral das MetaDirectory des IDM bei der GWDG.
Am IDM angebundene Zielverzeichnisse profitieren von dem Projekt durch die zeitnahe Abarbeitung von Prozessen. Zukünftig können weitere Zielverzeichnisse am IDM angeschlossen werden, da die Grundlage für das Bereitstellen von IT-Ressourcen sowie Entziehen von IT-Ressourcen von Accounts mit Hilfe des IDM umgesetzt werden.

7.2 Portale

Für die Administration sowie für die Selbstbedienungsfunktion der Mitarbeiter/innen stehen zwei unterschiedliche Portale zur Verfügung: IDM-Portal (Administratoren) und Kundenportal (Beschäftigte).

7.2.1 IDM-Portal

Das IDM-Portal dient ausschließlich der Administration von Identitäten. Verantwortlich ist die/der IT Beauftragte der jeweiligen Einrichtung. Das Portal ist unmittelbar mit dem IDM verbunden. Änderungen an Benutzerobjekten wirken sich auch auf alle am IDM angebundenen Systeme aus (SAP, Windows AD, LDAP etc.). Auf das IDM-Portal haben lediglich die Administrato/innen

Zugriff.

Es wird Anforderungen wie z. B. Mandantentrennung und gesonderter Berechtigungssteuerung gerecht. Das Portal verfügt über mehrere Bereiche - die sogenannten Arbeitsumgebungen.
Das Portal ist vollständig mandantenfähig, wodurch Institutsadministratoren nur die für sie relevanten Objekte (Benutzer und Verteiler) sehen und bearbeiten können.
Neben der reinen Benutzerverwaltung stehen über das Portal noch die Funktionen der LDAP- und Exchange Verteilerlisten zur Verfügung.
Über den Endnutzer hinausgehend stehen für Institutsadministratoren weitere Arbeitsumgebungen zur Verfügung, in denen sie Benutzer verwalten können.
Die Änderungen wirken sich direkt auf das zentrale Verzeichnis - das Metadirectory - aus und werden hieraus in die beteiligten Systeme verteilt.

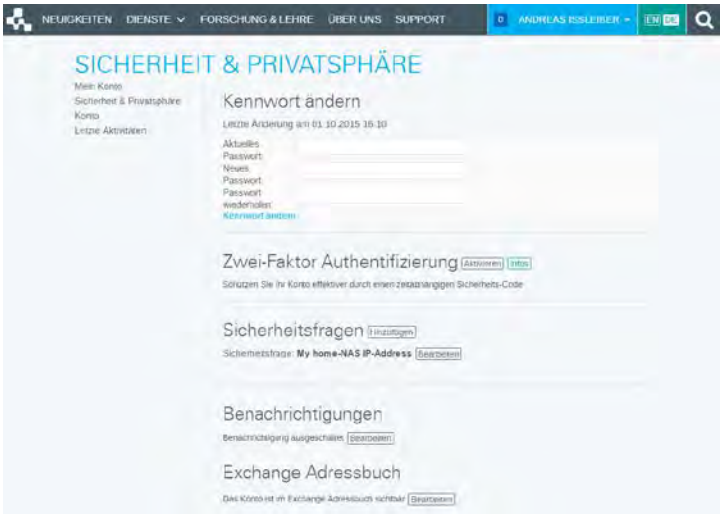
Funktionen des IDM-Portals:

- Portal für Administratoren der Institute (Anlage, Änderungen von Accounts),
- Zentrales Portal für die Benutzerverwalter aus den Personalverwaltungen um Accounts in den SAP-Zielsystemen zu erzeugen/entfernen.
- Portal für die Systemverantwortlichen,
- Prüfung der Kennwortkonvention für alle Systeme (incl. SAP-Systeme),
- Sperrung sowie Entsperrung von Benutzern über Administratoren der Institute und über die Systemverantwortlichen,
- Passwort ändern,
- E-Mail Aliase hinzufügen / ändern / löschen,
- Primäre E-Mail-Adresse ändern,
- Weiterleitungsadressen hinzufügen / ändern / löschen,
- Ausblenden aus den Exchange-Adresslisten,
- Entfernen der Active Directory Kurzzeitsperre,
- Sperrung eines Benutzers,
- Löschen eines Benutzers mit E-Mail-Benachrichtigung und 14-tägiger Karenzzeit sowie
- Löschen eines Benutzers zu einem definierten Zeitpunkt.

7.2.2 Kundenportal

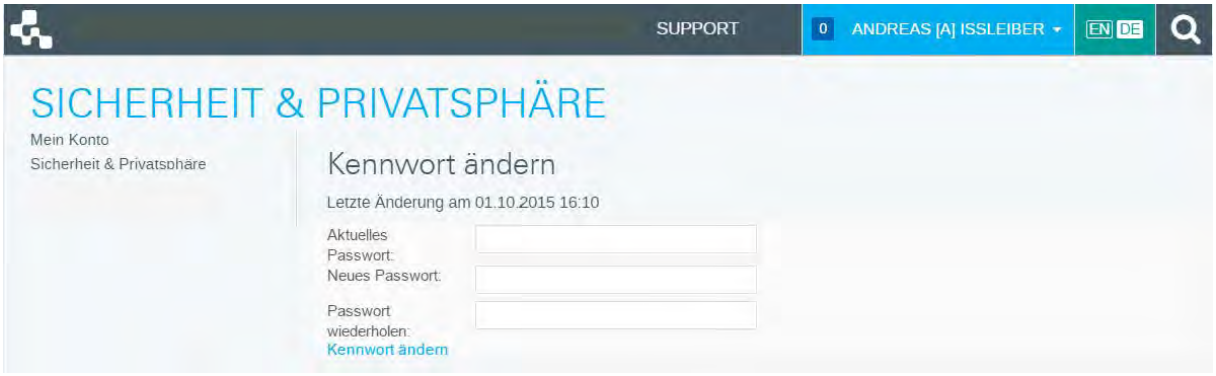
Für die Universität

Im Kundenportal kann der Anwender im Wege der Selbstbedienungsfunktion Änderungen innerhalb des eigenen Account vornehmen, z. B. die Änderung des Passwortes sowie die Ergänzung zusätzlicher Telefonnummern oder die Änderung der Raumnummer.



Für die Universitätsmedizin

Für den Bereich UMG sind die im Kundenportal verfügbaren Bereiche auf Wunsch der UMG soweit eingeschränkt, dass lediglich die Passwortänderungen möglich sind.



Der Zugriff auf weitere Dienste oder Webseiten, über das Portal wird hierbei verhindert.

Änderungen des Passwortes

Die Änderung eines Passwortes erfolgt über das Portal: passwort.med.uni-goettingen.de.
Hierbei ist zunächst eine erfolgreiche Anmeldung des Benutzers mit seinem bisherigen Passwort erforderlich. Anschließend kann der/die Benutzer/in sein Passwort ändern. Eine Überprüfung des Passwortes hinsichtlich der auch im SAP geforderten Passwortrichtlinien erfolgt hierbei im Portal selbst.

Auch des zweiten Passwortes eines Benutzers erfolgt in diesem Portal. Das zweite Passwort kann hierbei nur dann geändert werden, wenn das bisherige zweite Passwort im Portal korrekt angegeben

wurde. Hiermit wird verhindert, dass lediglich mit den ersten Passwort auch einen Änderung des zweiten Passwortes möglich ist.

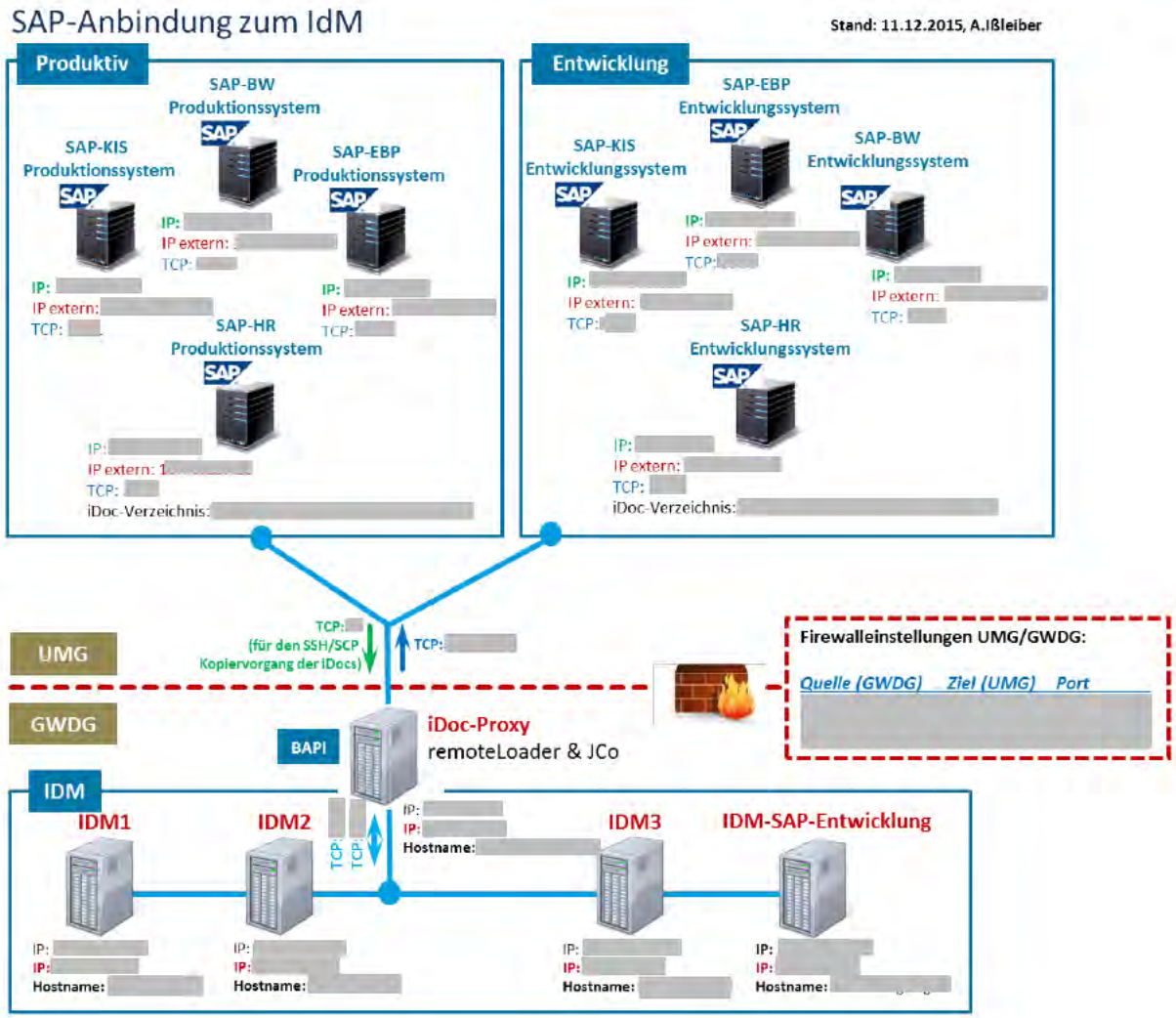
Passwortänderungen über das Portal sind in der Regel innerhalb von max. 1 Minute in allen angeschlossenen Systemen durch das IdM durchgeführt.

8. Ablage und Speicherung der Daten (iDocs)

Die Daten zu allen relevanten Ereignissen (Maßnahmen) aus SAP-HR wie, Eintritt, Austritt, Organisationswechsel werden aus dem SAP-HR in Form von iDocs erzeugt.

Diese werden zunächst unmittelbar auf dem SAP-HR-System abgelegt und durch ein weiteres Programm auf einen speziellen Server (iDoc-ProxyServer) kopiert, welcher in einer sicheren Umgebung die iDocs speichert. Dieser Kopiervorgang erfolgt verschlüsselt, automatisiert alle 10 Minuten. Anschließend werden alle kopierten iDocs auf dem SAP-HR Server wieder gelöscht. Auf dem iDocsProxyServer werden die iDocs unmittelbar verarbeitet und für max. 30 Tage aufbewahrt. iDocs, die älter als 30 Tage sind, werden irreversibel gelöscht.

Zugriff auf den iDocsProxyServer besitzen ausschließlich das SAP-HR System, sowie das IdM System, welches die Daten verarbeitet. Weitere Zugriffe auf den iDocsProxyServer sind nicht möglich und nicht vorgesehen.



9. Sicherungskonzepte

Im Rahmen der Auftragsdatenverarbeitung führt die GWDG regelmäßig inkrementelle und vollständige Sicherungen durch.

10. Dokumentationsverfahren

Die GWDG führt im Rahmen der Auftragsdatenverarbeitung eine entsprechende Dokumentation zum System.

11. IT-Sicherheitskonzept

Im Rahmen der Vorabkontrolle erfolgte auch die Betrachtung der Gefahren- und der Risikoanalyse. Diese Punkte können im entsprechenden Teil der Dienstvereinbarung eingesehen werden.

Siehe dazu: IT-RDV IDM RA Anlage Datenschutzvorabkontrolle.docx

Anlage 2

Zusatzvereinbarung zur Auftragsdatenverarbeitung

zwischen der

Georg-August-Universität Göttingen Stiftung öffentlichen Rechts Universitätsmedizin (UMG), Robert-Koch-Str. 40,37075 Göttingen,
vertreten durch den Vorstand

(nachstehend Auftraggeber genannt)

und der

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG),
Am Faßberg 11, 37077 Göttingen,
vertreten durch die Geschäftsführung

(nachstehend Auftragnehmerin genannt)

Unter Bezugnahme auf die Rahmenvereinbarung über Auftragsdatenverarbeitung personenbezogener Daten zwischen der Georg-August Universität Göttingen und der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

wird folgendes vereinbart:

Bereitstellung eines Identity-Management-Systems (IDM)

Das Verfahren zum IDM ist in der Regelungsabrede über den Pilotbetrieb eines IDM und der Systembeschreibung, die Vertragsbestandteil sind, näher erläutert. Die Auftragnehmerin verarbeitet im Rahmen ihres Auftrags die dort aufgeführten personenbezogenen Daten.
Die Datenverarbeitung erfolgt ausschließlich zu dem oben angegebenen Zweck.

Die GWDG hält eine aktuelle Dokumentation des Systems zur Einsichtnahme gemäß § 5 Abs. 1 der Regelungsabrede IDM bereit. Die Änderungen dieser Vereinbarungen erfolgen gemäß § 6 der Regelungsabrede IDM.

Die folgenden technischen und organisatorischen Maßnahmen werden verbindlich festgelegt:

1.) Zutrittskontrolle

Die Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet oder genutzt .werden, befinden sich in den. Maschinenräumen der GWDG. Der Zutritt zu den Maschinenräumen erfolgt ausschließlich über ein elektronisches Kontrollsystem (Chipkarten)/ das den Zutritt, automatisch protokolliert. Nur berechtigte Personen erhalten von der GWDG eine personengebundene Chipkarte, die den Zutritt ermöglicht.
Außerhalb der regulären Dienstzeit muss zusätzlich die Alarmanlage der Rechnerräume mit einem Schlüssel ausgeschaltet werden. Der Schlüssel befindet sich außerhalb der Dienstzeit im Gewahrsam der Pforte des MPI für biophysikalische Chemie und wird nur an berechtigte Personen/deren Namen auf einer entsprechenden Liste bei der GWDG erfasst sind, ausgegeben. Der Pförtner prüft Personalausweis, oder Reisepass und lässt sich die Ausgabe der Schlüssel quittieren.

2.) Zugangskontrolle

Die Beschäftigten der GWDG, die mit dem Betrieb der Datenverarbeitungssysteme betraut sind, können ausschließlich mit Ihren persönlichen Benutzerkonten auf diese. Datenverarbeitungssysteme zugreifen. Administrative Tätigkeiten können von Ihnen nur per ssh-Verbindung mit entsprechendem Zertifikat ausgeführt werden. Jeder Zugang wird automatisch protokolliert. Zugangsberechtigte Beschäftigte von Dienstleistern sind in den jeweiligen Verträgen mit den Dienstleistern namentlich aufgeführt. Sie unterliegen den gleichen Regularien wie Beschäftigte der GWDG.

3.) Zugriffskontrolle

Das auf dem Datenverarbeitungssystem eingesetzte Filesystem gewährleistet standardmäßig, dass die zur Benutzung des Datenverarbeitungssystems Berechtigten ausschließlich auf .die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Ebenso gewährleistet das eingesetzte Filesystem standardmäßig, dass die personenbezogenen Daten bei der

Verarbeitung und Nutzung sowie nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Jeder berechtigte Beschäftigte der Universitätseinrichtung erhält ein persönliches Benutzerkonto, unter dem er auf seine Daten zugreifen kann. Mit diesem Benutzerkonto kann der Berechtigte, die Standards verändern, Ist aber für jede Veränderung, selbst verantwortlich.

Der Zugriff auf die Daten erfolgt nur nach erfolgreicher Authentisierung des Benutzers. Die GWDG stellt ein Identitymanagementsystem zur Verwaltung der Benutzerberechtigungen zur Verfügung. Die Benutzerverwaltung. erfolgt durch die Universitätseinrichtung. Die Systeme der *Universitäts-Einrichtung,* sind durch ein Firewallsystem der GWDG geschützt. Die Freischaltung des-Zugriffes auf die Systeme der Universitätseinrichtung erfolgt in Abstimmung mit der Universitätseinrichtung.

Insbesondere ist der Zugriff auf die Systeme des Auftraggebers zu. Zwecken der Fernwartung nur über eine dem Stand .der Technik entsprechende verschlüsselte Verbindung zulässig. Ausnahmen bedürfen der schriftlichen Zustimmung des Auftraggebers.

4.) Weitergabekontrolle

Personenbezogene Daten werden von den berechtigen Nutzern *der* Universitätseinrichtung unter Ihren persönlichen Benutzerkonten weitergegeben. Sie sind für die Weitergabekontrolle verantwortlich.

Muss die GWDG aufgrund gesetzlicher oder behördlicher Vorgaben personenbezogene Daten weitergeben; so Ist *die* Universitätseinrichtung hierüber unverzüglich zu Informieren.

5.) Eingabekontrolle

Personenbezogene Daten werden ausschließlich unter Verwendung individueller Benutzerkonten von den Beschäftigten *der* Universitätseinrichtung in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt.

Die Beschäftigten sind für die Eingabekontrolle verantwortlich. .Insbesondere gilt § 7 der Rahmenvereinbarung über Auftragsdatenverarbeitung personenbezogener Daten

6.) Auftragskontrolle

Die Universitätseinrichtung hat das Recht, die getroffenen technischen und organisatorischen Maßnahmen Im erforderlichen Umfang zu kontrollieren. Die Auftragnehmerin hat die Kontrollen in zumutbarem Umfang zu unterstützen. Im Übrigen gilt § 5 der Rahmenvereinbarung über Auftragsdatenverarbeitung personenbezogener Daten. Die Beauftragung von Unterauf-

tragnehmern bedarf der vorherigen Zustimmung der Universitätseinrichtung.

7.) Verfügbarkeitskontrolle

Die GWDG betreibt ein SAN, über das die Daten der Universitätseinrichtung in RAID-Systemen gespeichert werden. Alle neuen und geänderten Dateien werden einmal täglich In das Backup-. System der GWDG kopiert und dort mindestens drei Monate aufbewahrt. Dadurch werden sie gegen zufällige Zerstörung oder Verlust geschützt.

8.) Trennungsgebot

Es wird auf §4 Abs. 3 der Rahmenvereinbarung über Auftragsdatenverarbeitung personenbezogener Daten Bezug genommen. Die dortigen Regelungen finden auf diese Vereinbarung Anwendung.

Schlussbestimmungen

Änderungen und Ergänzungen dieses Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für die Abänderung dieses Schriftformerfordernisses.

Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, wird die Gültigkeit dieses Vertrages im Übrigen dadurch nicht berührt. Die Vertragsparteien werden in diesem Falle die unwirksame Bestimmung durch eine Regelung ergänzen, die der ausdrücklichen oder stillschweigenden Absicht der Vertragsparteien so nahe wie möglich kommt. Dasselbe gilt im Falle einer Vertragslücke.

Göttingen, den _____

Für die UMG

_____

Prof. Dr. Heyo K. Kroemer

Vorstand Forschung und Lehre

Göttingen, den _____

Für die GWDG

_____

Prof. Dr. Ramin Yahyapour

Geschäftsführer

_____

Dr. Sebastian Freytag

Vorstand Wirtschaftsführung und Administration

Anlage 3 – Tabelle der zu übernehmenden Attribute aus SAP ERP HCM

Die folgende Tabelle enthält alle Attribute, die vom SAP-ERP HCM zum IDM übertragen werden.

Feldname	For-mat	Inhalt	Bemerkung
Persnr	C 8	Personalnummer IT0001-PERSNR	Dient zur Identifikation der jeweiligen Person (Bei Änderung in der Namensgebung)
Werks	C 4	Personalbereich IT0001-WERKS	Dient zur Unterscheidung der Personen aus den verschiedenen Organisationseinrichtungen (z. B. UMG, UNI)
Persg	C 1	Mitarbeitergruppe IT0001-PERSG	Dient zur Identifikation der aktiven Mitarbeiter bzw. emeritierten Profs.
Persk	C 2	Mitarbeiterkreis IT0001-PERSK	Dient zur Einschränkung der Personalstammdaten die an das IDM weitergeleitet werden (z.B. werden Sterbegeldempfänger im IDM nicht angelegt)
Nachn	C 40	Nachname IT0002-NACHN	Basisinformationen
Vorna	C 40	Vorname IT0002-VORNA	Basisinformationen
Namzu	C 15	Namenszusatz IT0002-NAMZU	Basisinformationen
Vorsw	C 15	Namensvorsatz IT0002-VORSW	Basisinformationen
Titel	C 15	Akad. Titel IT0002-TITEL	Basisinformationen
Geschlecht	C 1	Geschlecht IT0002-GESCH	Basisinformationen
Telnr	C 30	Telefonnummer IT0105-USRID, Subtyp 9200	Nur die dienstliche Telefonnummer - dient der Qualitätssteigerung in den verschiedenen Zielsystemen.
Matrikelnr	C 30	Matrikelnummer IT0105-USRID, Subtyp 8000	Dient der Identifikation einer bereits im IDM vorhanden Person um sicherzustellen, dass jede Person nur eine Identität im IDM erhält. Dabei kann die Identität mehrere Accounts haben (z. B. Abgleich Studierender). Dieses Matching kann jedoch nicht das Matching über Name, Geburtsdatum und Geburtsort ersetzten, da keine vollständige Datenhaltung im SAP existiert.
SUB_Barcode	C 8	Barcodenummer für Zutritt SUB IT0050-ZAUSW	Basisinformation für SUB-Dienste und -systeme.
Kostenstelle	C 12	Kostenstelle IT0001-KOSTL	Die primäre Kostenstelle, die zur Person in SAP ERP HCM zugeordnet wurde. Für die Benutzerverwaltung in den SAP-Systemen relevant.

Feldname	Format	Inhalt	Bemerkung
SAP_Kennung	C 30	SAP Kennung IT0105-USRID, Subtyp 0001	Dient zur Identifikation im IDM von existierenden SAP ERP HCM-Accounts. Diese Information wird nur bei einigen Personen (die bereits einen SAP-Account haben) übertragen.
NHG	C 1	Gruppe NHG IT9000-WAHL_NHG	Dieses Attribut ermöglicht die Identifikation von Hochschullehrern/ Hochschullehrerinnen, von wissenschaftlichen Beschäftigten und von MTV-Beschäftigten. Es gibt unterschiedliche Nutzungsszenarien bzgl. der Accounts bei Beendigung des Arbeitsverhältnisses.
Orgeh_sh	C 12	Kürzel Organisationseinheit IT1000-SHORT	Beinhaltet auf Universitätsseite die Kostenstelle bzw. die Innenauftragsnummer der jeweiligen Einrichtung
Inst_sh	C 12	Kürzel Institut IT1000-SHORT (Für die Uni: in der OM-Hierarchie das erste O-Objekt mit dem Feld IT1000-SHORT mit einem '-' an der vierten Stelle)	Beinhaltet auf Universitätsseite die Kostenstellengruppe der jeweiligen Einrichtung. Dient bei UniVZ der automatischen Zuordnung von Personen zu Einrichtungen.
Fak_sh	C 12	Kürzel Fakultät IT1000-SHORT (Für die Uni: in der OM-Hierarchie das erste O-Objekt mit dem Feld IT1000-SHORT mit einem '-' an der dritten Stelle)	Basisinformation.
Maßnahme	C 2	Eintritte, Austritte sowie Organisationswechsel	Dient der automatischen Weiterleitung für Deaktivierungen von Accounts an die Zielsysteme (Sperrung von Zugriffen nach Austritt von MA)
IDM-Status	C 2	Statusfeld für Schnittstelle HR2IDM	Attribut zur Steuerung der Übertragung von Daten an das IDM (z. B. können Accounts in Ausnahmefällen von der Personalabteilung gesperrt werden oder die Übertragung von Stammdaten bestimmter Personen ausgesetzt werden).
Personen-ID	C 8	Eindeutiger Schlüssel zur Identifikation von Personen im HR	Dient der Sicherstellung der Zusammenführung von verschiedenen Personalnummern pro Person. Dieses Attribut wird voraussichtlich im Jahr 2015 eingeführt.

Die folgende Tabelle enthält alle Attribute, die im IDM gespeichert sowie teilweise in einige Zielverzeichnissen übertragen werden.

Beschreibung	Attribut im IdM	Attribut in den Zielverzeichnissen
Vorname	Vorname	Vorname
Nachname	Nachname	Nachname
Personalnummer	Personalnummer	Personalnummer
Titel	Titel	Titel
Geschlecht	-	-
Telefonnummer	Telefonnummer	Telefonnummer
Org.Schlüssel/Org.Einheit	Org.Schlüssel/Org.Einheit	Org.Schlüssel/Org.Einheit/[indirekt durch OU]
Kostenstelle	Kostenstelle	Kostenstelle /[indirekt durch OU]
Unterscheidung: Professoren/Wissenschaftl. Mitarbeiter/Mitarbeiter	NHG	NHG
Personalbereich (UNI/UMG)	Werks	Mandant
E-Mail-Adresse(n)	eMail	eMail
User-ID	uid	UID
Beschäftigungsstatus	userStatus	userStatus
Eintrittsdatum	Eintrittsdatum	Eintrittsdatum
Austrittsdatum	Austrittsdatum	Austrittsdatum

Verfahrensbeschreibung gem. § 8 des Nds. Datenschutzgesetzes (NDSG)

☒ **Einzelbeschreibung der Daten verarbeitenden Stelle**

☐ **Sammelbeschreibung der Daten verarbeitenden Stelle zu gleichartigen Verfahren**

Anzahl der Verfahren

☐ **Sammelbeschreibung durch Auftragnehmer (Daten verarbeitende Stelle siehe beiliegende Liste)**

☒ Ersterfassung ☐ Änderung/Ergänzung

Verfahrensbeschreibungen über automatisierte Verfahren zur Erfüllung der Aufgaben nach dem NVerfSchG oder nach dem Nds. SOG sind in Kopie an den Landesbeauftragten für den Datenschutz Niedersachsen zu senden.

1. Anzeigende Stelle

Verfahrensbeschre bung erstellt von (Adresse, Geschäftszeichen)	Telefon:	Ort, Datum:
Universität Göttingen, Goßlerstr. 5/7, 37073 Göttingen, Herr Hochdorfer/ UMG Dr. T. Langbein	0551/39-7942 0551/ 39 22762	11.11.2014, Göttingen, für UMG angepasst 10.3.2016
Name der oder des Datenschutzbeauftragten /Telefon Prof. Dr. Dr. h.c. Werner Heun 0551 / 39-4693 (Universität) Dr. Thomas Langbein 0551 39 22762 (UMG) Referat/Dezernat/Amt/Abteilung	**Unterschrift** (Erstellerin/Ersteller der Verfahrensbeschreibung)	angeordnet durch Leiterin/Leiter Herrn Remmers

2. Bezeichnung des Verfahrens

Bezeichnung des Verfahrens Identity-Management-System	
Eingesetze Programme NetIQ Identity Manager, IDM-Portal (Eigenentwicklung GWDG), Benutzerportal (Eigenentwicklung GWDG)	
☒ Verknüpfungen zu anderen Verfahren oder Dateien bestehen	Bezeichnung dieser anderen Verfahren oder Dateien SAP HR, MS Active Directory, OpenLDAP, SAP-Systeme (KIS, BW, EBP), UniVZ

3. Bezeichnung der Daten verarbeitenden Stelle/ Angaben zur Auftragsdatenverarbeitung

Bezeichnung der Daten verarbeitenden Stelle (bei Sammelbeschre bung durch Auftragnehmer siehe beiliegende Liste)
Georg-August-Universität Göttingen und die Universitätsmedizin Göttingen

Ort, Datum Göttingen 11.11.2014; angepasst 10.3.2016

☐ Die gesamte Datenverarbeitung wird bei der Daten verarbeitenden Stelle se bst durchgeführt.

☒ Teile der Datenverarbeitung werden bei einem Auftragnehmer durchgeführt. Das Auftragsverhältnis ist schriftlich geregelt, § 6 NDSG wird beachtet.

Name und Anschrift der Auftragnehmer sowie Art der Datenverarbeitung (z.B. Erfassung, Mikroverfilmung, Vernichtung)
Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen mbH
Am Faßberg 11
37077 Göttingen

Art der Datenverarbeitung: Konfiguration und Betrieb im Rahmen der Auftragsdatenverarbeitung

4. Zweckbestimmung des Verfahrens

- Einheitliche Verwaltung von Benutzer-Accounts für alle Nutzergruppen und Dienste am Wissenschaftsstandort Göttingen,
- Unterstützung eines Zugriffsmanagements auf IT-Systeme von der Ausstatung der Nutzer mit den notwendigen Accountdaten bei der Einstellung bis hin zur Abgrenzung des Zugriffes bei Vertragsende,
- Erfüllung wichtiger Compliance-Forderungen bezüglich der Ausstattung von Mitarbeiter(innen) mit persönlichen Accounts,

5. Rechtsgrundlage der Verarbeitung

Rechtsgrundlage für den Betrieb des Identity-Management-Systems sind die einschlägigen Rechtsgrundlagen für die Datenverarbeitung an der Universität Göttingen. Die Datenverarbeitung an der Universität Göttingen beruht auf einer Reihe unterschiedlicher Rechtsgrundlagen, die damit auch die rechtliche Basis des Identity Management darstellen. Einschlägig sind vor allem § 17 NHG, § 9, 10 NDSG und ergänzend § 88 I NBG sowie für die Universitätsklinik auch § 4 in Verbindung mit § 12 ff. BDSG und die Dienstvereinbarungen zum Betrieb des Identity-Managment-Systems zwischen dem Personalrat der Universität Göttingen und dem Präsidium der Georg-August-Universität, sowie zwischen dem Personalrat der UMG und dem Vorstand der UMG.

6. Kreis der Betroffenen

Mitglieder, Angehörige und Gäste der Universität Göttingen (ausgenommen Studierende, es sei den, dass sie Arbeitnehmer an der Universität Göttingen oder an der UMG sind).

Ungefähre Anzahl der Betroffenen 17000

7. Fristen für die Sperrung und Löschung der Daten

Professorinnen/Professoren: Lebenslang
Professorinnen/Professoren bei Wechsel der Hochschule oder bei Wechsel zu einem anderen Arbeitgeber : 1 Jahr
Wissenschaftliche Mitarbeiter/innen: 6 Monate
Mitarbeiter/innen: Deaktivierung mit Vertragsende

8. Gespeicherte Daten

8.1 Art der gespeicherten Daten Jeder Betroffenenkreis ist einzeln aufzuführen; siehe auch Ausfüllhinweise	**8.2 Herkunft oder Empfänger bei regelmäßiger Übermittlung** Es ist anzukreuzen, ob es sich um eine übermittelnde (Ü) oder empfangende (E) Stelle handelt.			
			Ü	E
	a	NeitQ Identity Manamgement System	☒	☒
	b	SAP HR (Personalverwaltung)	☒	☒
	c	MS Active Directory	☒	☒
	d	OpenLDAP	☐	☒
	e	SAP KIS, BW, EBP	☐	☒
	f	UniVZ	☐	☒
	g		☐	☐

	a	**b**	**c**	**d**	**e**	**f**	**g**
Personalnummer	☒	☒	☐	☐	☒	☒	☐
Personalbereich	☒	☒	☒	☐	☒	☒	☐
Mitarbeitergruppe	☒	☒	☐	☐	☐	☒	☐
Mitarbeiterkreis	☒	☒	☐	☐	☐	☒	☐
Nachname	☒	☒	☒	☒	☒	☒	☐
Vorname	☒	☒	☒	☒	☒	☒	☐
Namenszusatz	☒	☒	☒	☒	☒	☒	☐
Namensvorsatz	☒	☒	☒	☒	☒	☒	☐
Akad. Titel	☒	☒	☒	☒	☒	☒	☐
Geschlecht	☒	☒	☒	☐	☒	☒	☐
Dienstliche Telefonnummer	☒	☒	☒	☐	☒	☒	☐
Matrikelnummer	☒	☒	☐	☐	☐	☒	☐
SUB-Barcode	☒	☒	☐	☐	☐	☐	☐
Kostenstellennummer	☒	☒	☒	☐	☒	☒	☐
Gruppe NHG	☒	☒	☐	☐	☐	☒	☐
Organisationseinheit/Organisationsschlüssel	☒	☒	☒	☒	☒	☒	☐
Institut	☒	☒	☐	☐	☐	☒	☐
Fakultät	☒	☒	☐	☐	☐	☒	☐
Massnahme (Eintritt, Austritt, Wechsel)	☒	☒	☒	☐	☒	☒	☐
IDM-Status aus SAP-HR	☒	☒	☐	☐	☐	☐	☐
Personen-ID aus SAP-HR	☒	☒	☐	☐	☐	☒	☐
Accountname	☒	☒	☒	☒	☒	☐	☐
Passwort	☒	☒	☒	☒	☒	☐	☐
Beginndatum des Zugangs	☒	☒	☒	☐	☒	☐	☐
Endedatum des Zugangs	☒	☒	☒	☐	☒	☐	☐

Primäre E-Mail Adresse	☒	☒	☒	☒	☒	☒	☐
	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐
Bitte hier doppelklicken um eine neue Zeile einzufügen							

☐ Es findet keine regelmäßige Übermittlung statt

8.3 Beabsichtigte Übermittlung von Daten in Staaten nach § 14 NDSG

Rechtsgrundlage für die Übermittlung
keine

Zweck der Übermittlung
entfällt

Behördeninterner Teil der Verfahrensbeschreibung

9. Angaben zu dem Verfahren nach Nr. 2

Bezeichnung des Verfahrens
Identity-Management-System

Eingesetze Programme
NetIQ Identity Manager, IDM-Portal (Eigenentwicklung GWDG), Benutzerportal (Eigenentwicklung GWDG)

☐ Verknüpfungen zu anderen Verfahren oder Dateien bestehen	Bezeichnung dieser anderen Verfahren oder Dateien SAP HR, MS Active Directory, SAP-Systeme (KIS, BW, EBP), UniVZ

10. Betriebsart des Verfahrens

☒ Stapel- (Batch-) Betrieb ☒ Dialogbetrieb	Bitte zusätzlich angeben ☒ Datenbank ☐ Tabellenkalkulation ☐ Textverarbeitung ☒ Manuell ☐ Sonstiges:

11. Art der Geräte

(Betriebssystemangaben ohne exakte Versionsnummern)

☐ Großrechner der Firma	Betriebssystem
☒ Rechner mittlerer Größe	Betriebssystem Linux, FreeBSD
☒ Vernetzte Arbeitsplatzcomputer	Betriebssystem Windows, Linux
☐ Alleinstehende PC	Betriebssystem

☐ Sonstiges:

☐ Datenfernübertragung	☐ Standleitung (”DDV” oder ”HfD”)	☐ Wählleitung mit Modem
☒ Sonstige Datenfernübertragung		

12. Übermittlungsverfahren

☐ COM-Mikrofiche-austausch	☐ Datenträger-austausch	☐ Dateitransfer mittels Datenfernübertragung	☒ Automatisiertes Abrufverfahren

13. Verfahren zur Sperrung, Löschung, Auskunftserteilung

☒ Manuelle Sperrung	☒ Automatische Sperrung	☐ Manuelle Löschung	☐ Automatische Löschung

Verfahren der Auskunftserteilung:

☒ Schriftliche Mitteilung	☐ Einsichtnahme vor Ort	☐ Sonstiges:

14. Technische und organisatorische Angaben nach § 7 NDSG

14.1 Bauliche Maßnahmen

☐ Grundsätzlich kein Publikumsverkehr in Räumen mit Arbeitsplatzcomputern (APC) oder Terminals.
☐ Alle Räume mit APC sind bei Abwesenheit der Bediensteten mit Sicherheitsschlössern verschlossen.
☐ Es werden nur APC eingesetzt (keine Zentralrechner wie Großrechner, Server, Mehrplatzsysteme).
☒ Alle Zentralrechner sind in einer Sicherheitszone mit zusätzlicher Zugangskontrolle untergebracht.
☐ Sicherung wichtiger mobiler Datenträger in separatem, gesicherten Archivraum oder Tresor.

14.2 Technische Maßnahmen

☒ Sicherung aller Rechner durch	☒ Passwort	☐ Magnetstreifenkarte/Chipkarte

☒ Die Begrenzung der Zugriffsrechte auf die zuständigen Bediensteten ist technisch gesichert.
☒ Verschlüsselung bei der Speicherung und ggf. bei der Datenfernübertragung.
☒ Protokollierung von Systemaktivitäten (z.B. Benutzer-Login).
☒ Protokollierung des Zugriffs auf einzelne Datensätze.
☐ Regelmäßige Auswertung der Protokolle.

14.3 Organisatorische Maßnahmen

Die Zugriffsberechtigungen sind auf folgende Personen beschränkt:

Administratoren der GWDG mit vollständigem Zugriff auf alle Daten.
Enduser besitzen ausschliesslich Zugriff auf einige Attribute der eigenen Person.
IT Institutsadministratoren haben Zugriff auf die Daten aller diesem Institut zugeordneten Personen. Die Liste der IT Institutsadministratoren wird von der GWDG verwaltet.

☐ Eine Dienstanweisung zum Datenschutz ist vorhanden.

Sonstiges:

14.4 Weitere wichtige technisch-organisatorische Maßnahmen

Anlage 5 – Datenschutzvorabkontrolle

1. Systembeschreibung

Beim Novell „Identity Management“ (IDM) handelt es sich um eine Lösung zur zentralen Verwaltung von Identitäten. Das System bietet umfangreiche Synchronisationsfunktionen für z. B. verschiedene Verzeichnisdienste, Datenbanken, Betriebs- und HR-Systeme. Das IDM strebt eine Senkung des administrativen Aufwands zur Verwaltung von Identitäten und die Verwendung einheitlicher Nutzer-Accounts an. Dabei können ausgehend von den im IDM zentral gespeicherten Daten (Identitäten) alle benötigten Informationen an verschiedene angeschlossene Systeme und Applikationen verteilt werden. Andererseits ist es ebenso möglich, bestimmte Informationen aus den angeschlossenen Systemen und Applikationen an das IDM zu übertragen bzw. diese zu synchronisieren. Die an das IDM angeschlossenen bzw. anzuschließenden Systeme und Applikationen sind in der nachfolgenden Abbildung dargestellt. Weiterhin ist zu erkennen, welche Systeme lediglich als Zielsysteme verwendet werden und welche Systeme auch Daten liefern.

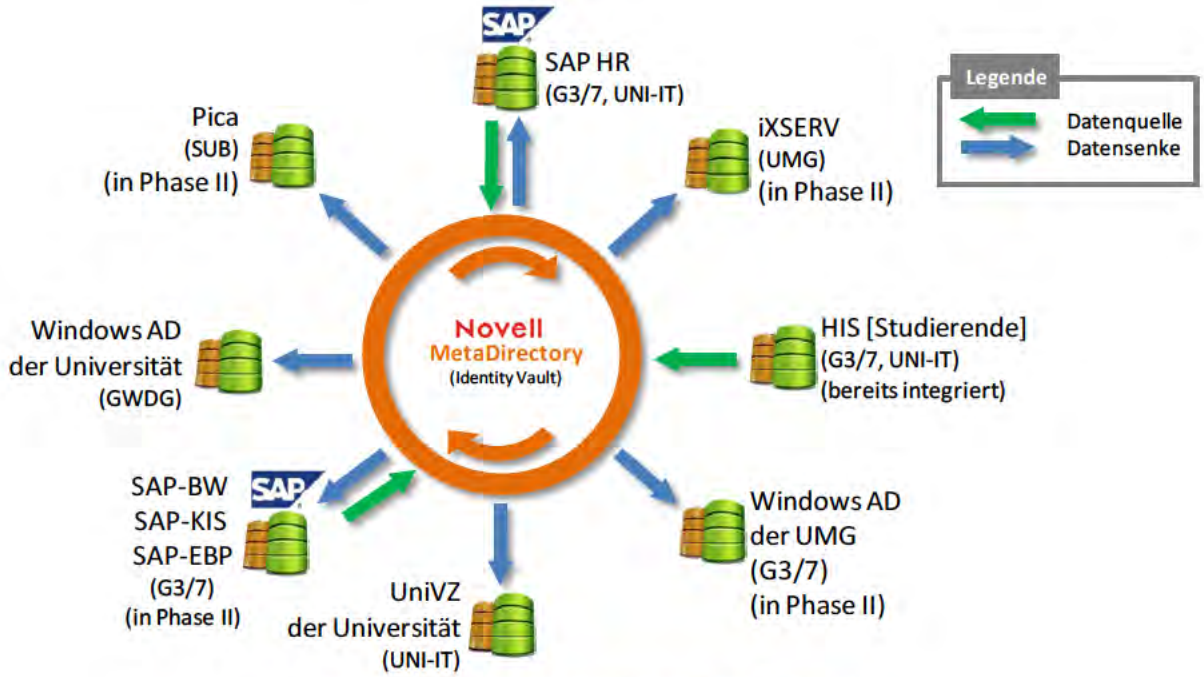


Abbildung 1: Datenquellen und -Senken

Der Zugriff auf das IDM erfolgt browserbasiert über ein IDM-Portal (https://idm.gwdg.de/). In diesem können die Nutzer sog. Selbstbedienungsfunktionen in Anspruch nehmen (z. B. Passwortänderung, Pflege persönlicher Daten wie Telefonnummer, Raumnummer, usw.). Auch die administrative Pflege erfolgt über dieses Portal. Administratoren haben hierzu umfassendere Berechtigungen. Genauere Ausführungen hierzu sind im Abschnitt 5 zu finden. Weitere Softwareanforderungen sind aus Nutzersicht nicht vorhanden, da das IDM lediglich die Daten verwaltet. Es dient nicht zur operativen Arbeit. Diese erfolgt weiterhin in den bisher genutzten Systemen.

Hardwareseitig existieren im operativen Betrieb drei IDM-Server (zwei physikalische, ein virtueller) bei der GWDG. Von diesen Servern ausgehend, übernehmen ca. 40 Treiber das Schreiben und Lesen der Informationen von und zu den angeschlossenen Systemen und Applikationen. Die Übertragung der Informationen geschieht über eine gesicherte Verbindung (VPN-Tunnel). Weitere Ausführungen sind Abschnitt 4 zu entnehmen.

Im System selbst werden keine Daten verdichtet bzw. neue generiert. Eine Ausnahme bildet hier lediglich das Einmal/Start-Passwort bei der Generierung des Accounts. Dieses wird für die neuen Nutzer zu Beginn gesetzt und muss anschließend durch die Nutzer geändert werden.

Die Ziel-Struktur im IDM besitzt folgenden Aufbau:

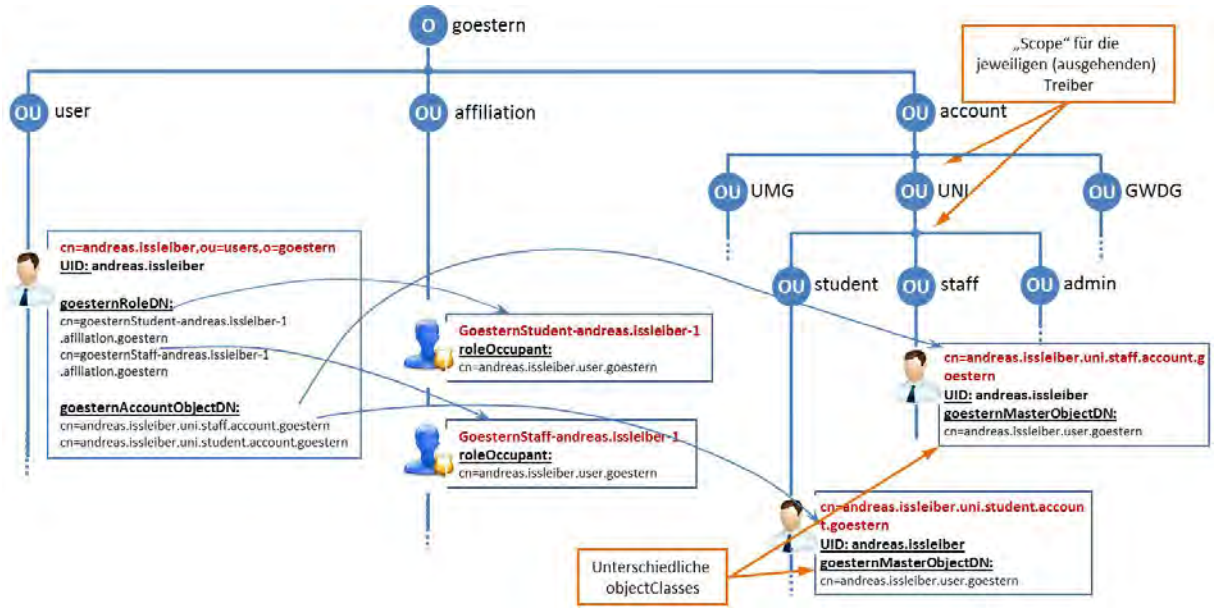


Abbildung 2: Zielstruktur IDM, Benutzerobjekte und Affiliations

Das User-Object *(o=goestern, ou=user)* beinhaltet alle relevanten Attribute und wird durch das GWDG-Endnutzerportal bearbeitet. Die Attribute enthalten ebenfalls die jeweiligen Rollen des Nutzers (*goesternRoleDN*), die auf Basis der Affiliation zugeordnet worden sind. Außerdem wird ebenfalls eine Accountzuordnung in die jeweiligen Bereiche der Universität vorgenommen (*unterschiedliche ObjectClasses*). Im Beispiel in Abbildung 2 handelt es sich also um einen Nutzer, der die Rollen *goesternStudent* und *goesternStaff* zugeordnet bekommen hat und somit als Mitarbeiter und als Studierender in die jeweiligen Bereiche der Universität *(o=goestern, ou=account, ou=uni)* eingeordnet wird.

Der grundsätzliche Ablauf der Datenverarbeitung im IDM ist der nachfolgenden Prozessdarstellung zu entnehmen:

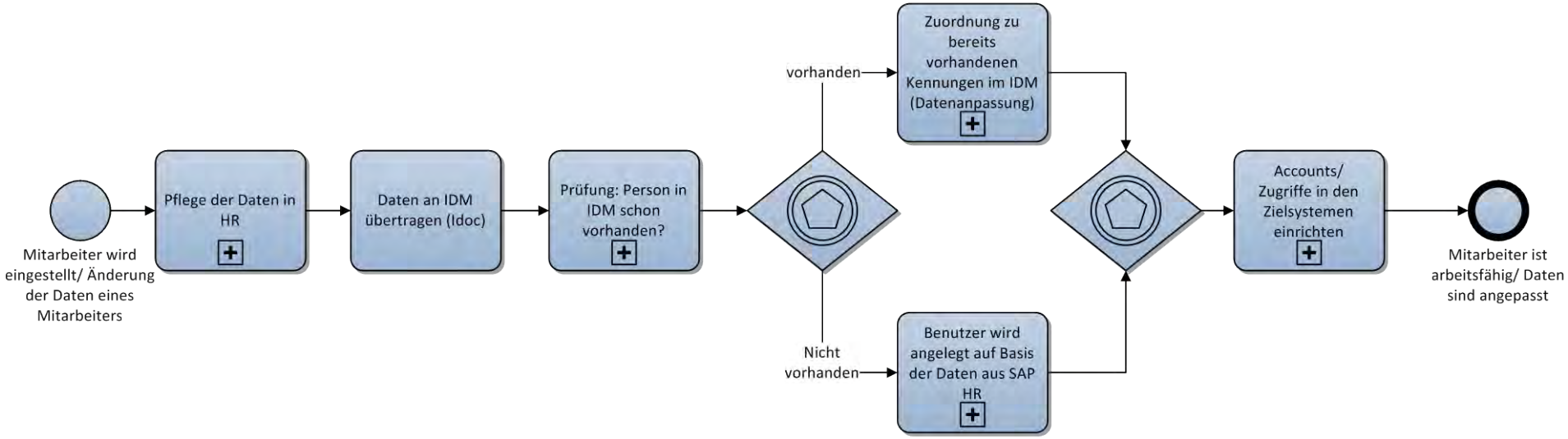


Abbildung 3: Grundsätzlicher Ablauf der Datenverarbeitung vom IDM

Wenn ein Mitarbeiter eingestellt wird oder an seinen Daten eine Veränderung an den Personaldaten vorgenommen werden muss (z. B. Namenänderung durch Heirat, Vertragsverlängerung), erfolgt dies über die Personalabteilungen. Diese pflegen die Daten in das System ein. Aus SAP ERP HCM wird anschließend ein IDoc erzeugt (dieses enthält Datensätze von neuen oder geänderten „Personen“). Im IDM wird geprüft, ob diese Person bereits vorhanden ist. Ist dies der Fall, werden die Daten im IDM angepasst (z. B. der Account aufgrund des längeren Vertrages verlängert). Ist dies nicht der Fall, wird für die neu eingestellte Person ein neuer Account generiert. Anschließend erfolgt die Provisionierung der Informationen zu den o. g. Zielsystemen und der Prozess ist abgeschlossen.

Folgende Attribute werden aus SAP ERP HCM an das IDM übertragen:

Attribute aus SAP-HR		
Persnr	C 8	Personalnummer IT0001-PERSNR
Werks	C 4	Personalbereich IT0001-WERKS
Persg	C 1	Mitarbeitergruppe IT0001-PERSG
Persk	C 2	Mitarbeiterkreis IT0001-PERSK
Nachn	C 40	Nachname IT0002-NACHN
Vorna	C 40	Vorname IT0002-VORNA
Namzu	C 15	Namenszusatz IT0002-NAMZU
Vorsw	C 15	Namensvorsatz IT0002-VORSW
Titel	C 15	Akad. Titel IT0002-TITEL
Gebdat	Datum	Geburtsdatum IT0002-GBDAT
Gebort	C 40	Geburtsort IT0002-GBORT
Geschlecht	C 1	Geschlecht IT0002-GESCH
Telnr	C 30	Telefonnummer IT0105-USRID, Subtyp 9200
Matrikelnr	C 30	Matrikelnummer IT0105-USRID, Subtyp 8000
SUB_Barcode	C 8	Barcodenummer für Zutritt SUB IT0050-ZAUSW
SAP_Kennung	C 30	SAP Kennung IT0105-USRID, Subtyp 0001
Grnhg	C 1	Gruppe NHG IT9000-WAHL_NHG
Orgeh_sh	C 12	Kürzel Organisationseinheit IT1000-SHORT
Inst_sh	C 12	Kürzel Institut IT1000-SHORT (Für die Uni: in der OM-Hierarchie das erste O-Objekt mit dem Feld IT1000-SHORT mit einem '-' an der vierten Stelle)
Fak_sh	C 12	Kürzel Fakultät IT1000-SHORT (Für die Uni: in der OM-Hierarchie das erste O-Objekt mit dem Feld IT1000-SHORT mit einem '-' an der dritten Stelle)
Beurlaubung	C 1	Beurlaubung – das Feld muss noch definiert und automatisch gefüllt werden

Abbildung 4: Übertragene Attribute

2. Rechtsgrundlage der Datenverarbeitung

Die Datenverarbeitung an der Universität und an der Universitätsmedizin Göttingen beruht auf einer Reihe unterschiedlicher Rechtsgrundlagen, die damit auch die rechtliche Basis des Identity Management darstellen. Einschlägig sind vor allem § 17 NHG, § 9, 10 NDSG und ergänzend § 88 I NBG sowie für die Universitätsklinik auch § 4 in Verbindung mit § 12 ff. BDSG.

3. Gefahrenanalyse

Bewertungsmerkmale: niedrig, mittel, hoch

Bedrohungs-objektgruppen	Potenzielle Gefahren	Eintritts-wahrschein-lichkeit
Infrastruktur, Hardware	Hohe Belastung der Netzwerkverbindung → Eingeschränkte Verfügbarkeit der abgebildeten Prozesse	Mittel
	Ausfall der für den IDM-Dienst/ SAP-Server relevanten Netzwerk-komponenten (partieller Netzwerkausfall) → Arbeitsfähigkeit grundlegend vorhanden (z. B. Anmeldung am PC), Änderungen im IDM werden erst nach der Fehlerbeseitigung übernommen (z. B. Passwortänderung) → dennoch keinen Datenverlust	Niedrig
	Totalausfall zentraler Netzwerkkomponenten → Eine Arbeitsfähigkeit der Mitarbeiter in der Universität ist nicht mehr gegeben (dieses Szenario ist ebenso ohne IDM möglich). → dennoch keinen Datenverlust	(Sehr) niedrig
Software, Anwendungsdaten	Softwarefehler → Eingeschränkte Verfügbarkeit der Dienste, Datenverlust: Die Software wird umfassend getestet. Eine 3-stufige Systemlandschaft für Tests vor der Produktivsetzung ist vorhanden.	Niedrig
	Gefährdung der Vertraulichkeit der Daten: Umfassende Sicherheitsmechanismen (z. B. Verschlüsselte Verbindung, asymmetrische Verschlüsselung) sind implementiert.	Niedrig
Personen	Gefährdung der Vertraulichkeit der Daten: Systembetreuer unterliegen einer Verschwiegenheitserklärung und handeln daher gemäß der Datenschutz-Richtlinien.	Niedrig

Abbildung 5: Gefahrenanalyse

4. Risikoanalyse

Wahrscheinlichkeit des Schadeneintritts:

Schadeneintrittskriterium	Bewertung
Missbrauchsinteresse	Niedrig
Aufwand (um Schaden herbeizuführen)	Sehr hoch
Risiko (entdeckt zu werden)	Sehr hoch
Verarbeitungshäufigkeit (Anzahl der Angriffspunkte)	Mittel

Abbildung 6: Risikoanalyse

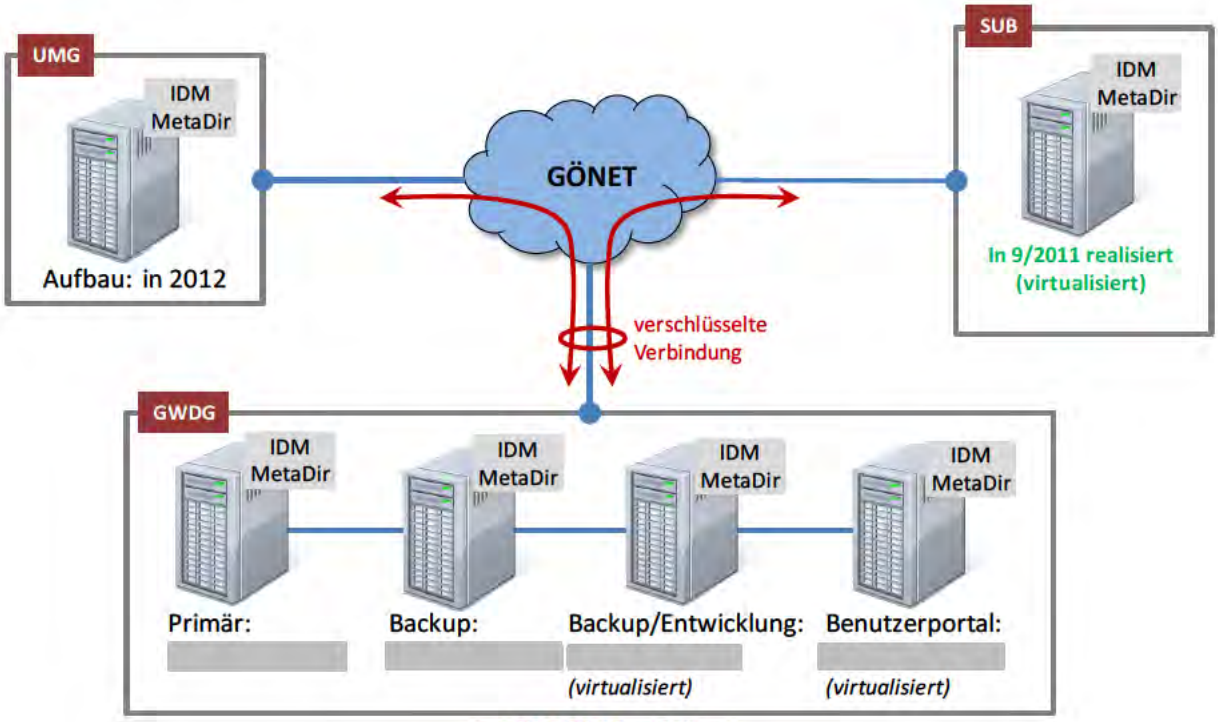
Das IDM selbst speichert lediglich die Informationen über die Mitarbeiter/innen und verwaltet deren Identitäten. IDM selbst ist nach außen nicht sichtbar. Vom IDM werden Informationen an die Zielsysteme verteilt und aktualisiert. Dort erfolgt die Bereitstellung (z. B. UniVz: Eintrag anlegen und Kontaktdaten bereitstellen).[1] Die im IDM gespeicherten Informationen sind i. d. R. in die LfD-Stufe A einzuordnen, da diese bisher auch frei zugänglich sind (z. B. Kontaktinformationen und Institutszugehörigkeit in UniVz). Andere Informationen (z. B. Personalnummer) könnten berechtigtes Interesse der Einsicht nehmenden erwecken (LfD-Stufe B). Es ist jedoch nicht möglich, hiermit einen Schaden anzurichten. Außerdem werden diese Informationen auch nur für die Kommunikation zwischen SAP ERP HCM und IDM benötigt. In anderen Systemen werden diese Daten nicht verarbeitet.
Das nach dem LfD-Schutzstufenkonzept am höchsten einzustufende Attribut ist das Passwort des Nutzers/der Nutzerin. Wenn jemand Kenntnis über das Passwort eines Nutzers/ einer Nutzerin hat, kann der Nutzer/ die Nutzerin in seiner/ihrer gesellschaftlichen Stellung oder in seinen/ ihren wirtschaftlichen Verhältnissen beeinträchtigt werden („Ansehen"). Dementsprechend ist das Passwort in die LfD-Stufe C einzuordnen. Dieses Bedarf folglich eines besonderen Schutzes. Hierauf wird im Abschnitt Datensicherungskonzept nochmals eingegangen.

5. Datensicherungskonzept

Aufgrund der redundanten Auslegung der IdM-Server in Form eines Serverclusters, sind die zentralen Daten auf drei IdM-Server synchron verteilt. Bei Ausfall eines Servers, bleibt der IdM-Dienst weiterhin funktionsfähig. Überdies sind aufgrund der Servervirtualisierung bei der GWDG auch die physischen Standorte der IdM-Server auf drei zentrale Punkte verteilt (GWDG, SUB, FMZ).
Dennoch erfolgt zusätzlich eine tägliche Datensicherung aller IdM-Server zu dem zentralen Backupsystem der GWDG (TSM, Tivoli). Neben den Daten wird auch das Betriebssystem der IdM-Server gesichert. Die Sicherungsdaten befinden sich in, nur durch autorisiertes Personal zugänglichen, Räumen der GWDG sowie der Fernmeldezentrale der Universität (FMZ).
Durch den zusätzlichen Aufbau eines zweiten IdM-Cluster, welcher im Normalbetrieb zu Entwicklungszwecken genutzt wird, besteht in Ausnahmesituation die Möglichkeit, den IdM-Dienst auf

[1] Für diese Systeme existieren bereits Dienstvereinbarungen

diesen Entwicklungscluster innerhalb von wenigen Stunden zu aktivieren. Durch tägliche Synchronisation des Produktiv-Cluster mit dem Entwicklungscluster sind auch die Daten relativ aktuell und bilden die Basis für die Aufrechterhaltung des IdM-Dienstes in extremen Ausnahmesituationen (Disaster Recovery).



ca. 90.000 Identitäten

Abbildung 7: IDM-Systemstandorte

6. Berechtigungskonzept

Funktionale Einschränkungen erfolgen bezüglich verschiedener Bearbeitungsaktivitäten. So können bspw. bestimmte Personengruppen (angepasst an den jeweiligen Aufgabenbereich) Attributen und weiteren Inhalten ändern oder nur anzeigen. Hierbei können drei verschiedene Rollen unterschieden werden:

Administrator-Rolle (GWDG) (bisher 3 Personen)	Lokale Admin	Normaler Nutzer (alle anderen Mitarbeiter)
- Administration und Pflege des IDMs - Zugriff auf alle hinterlegten Informationen - Möglichkeit des Auslesens des Passwortes - Zurücksetzen bzw. neuvergeben des PWs möglich	- Für eigene Institute/ Abteilungen eine Auswahl von vordefinierten Attributen ändern (über Portal, kein direkter Zugriff auf das IDM) - Zurücksetzen bzw. neuvergeben des PWs möglich (eigenes Institut)	- Kann vordefinierte eigenen Daten anzeigen und ändern (über Portal, keine direkter Zugriff auf das IDM). - z. B. Passwort, Telefonnummer

Abbildung 8: Rollen im IDM

7. Schutz des Passwortes

Wie bereits in

Abbildung 8 dargelegt, haben die Administratoren der GWDG die Möglichkeit, das Passwort eines Nutzers auszulesen. Es ist technisch notwendig, dass das Passwort verfügbar ist, da sonst keine Synchronisation des Passwortes mit anderen Systemen erfolgen kann (diese verwenden andere Verschlüsselungsalgorithmen). Außerdem stellt das Auslesen des Passwortes einen erheblichen Aufwand dar (Skript-Erstellung). Aufgrund des geringen Missbrauchsinteresses der Administratoren und des hohen Risikos von den anderen Administratoren entdeckt zu werden, ist das Passwort sicher aufbewahrt. Alle anderen Nutzer haben keine Möglichkeit an das Passwort zu gelangen.

Anlage 6 – Berechtigungskonzept

Diese Anlage stellt das Berechtigungskonzept für die folgenden Komponenten dar:

- Identity-Management-System (IDM), Metadirectory von NetIQ bei der GWDG,
- IDM-Portal bei der GWDG sowie
- Endnutzer-Portal bei der GWDG.

Für die Komponenten des IDM sowie die daran angeschlossenen Portale existieren drei grundlegende Rollen:

1.) **IDM-Administrator:** besitzt uneingeschränkten Zugriff auf alle Bereiche mit allen Attributen des IDM.

2.) **Institutsadmin:** sind Administratoren der jeweiligen Instituts- sowie Abteilungs- und Stabsstellenbereiche. Diese Personen bekommen lesenden Zugriff auf alle in dem Institut oder der Abteilung oder Stabsstelle zugehörigen Daten der Institutsadministrator hat aber nur für ein Teil der Daten schreibrechte (z.B. Initialisierung eines neuen Kennwortes).

3.) **Endnutzer:** sind die Mitarbeiterinnen und Mitarbeiter, welche im Rahmen der Selbstbedienungsfunktion einige der zur eigenen Person gehörenden Attribute (Datenfelder einer Identität) ändern können. Dieses sind insbesondere die Adresse, Telefonnummern sowie das/die Passwörter. Änderungen an Vor- sowie Nachname, UserID, primärer eMail-Adresse des Benutzers sind weder durch den Benutzer noch durch den Administrator oder den zuständigen Institutsadministrator möglich.

Berechtigungskonzept IDM (MetaDirectory)

Identity-Management (IDM, MetaDirectory)					
Personen	**Institution**	**Rolle**	**Anzahl der Personen**	**Zugewiesene Rechte**	**Zielbereich**
IDM-Administratoren	GWDG	Administrator	3	• Lesen • Schreiben • Ändern • Löschen	Alle Objekte / alle Attribute im gesamten IDM
IT-Administratoren UMG	UMG	IT-Administratoren	35; 12 IT-Service, 13 IT-Rufbereitschaft, 10 SAP IT-Admins	• Lesen • Schreiben • Ändern • Einfügen von Identitäten	Nur Objekte der UMG
Administratoren der einzelnen Institute und Abteilungen der Universität	UNI	Institutsadministrator	186, für die jeweiligen 186 Institutsbereiche	• Lesen • Schreiben • Ändern • Einfügen von Identitäten	Nur Objekte des jeweiligen Institutsbereiches

Berechtigungskonzept IDM-Portal

IDM-Portal (http://idm.gwdg.de)					
Personen	**Institution**	**Rolle**	**Anzahl der Personen**	**Zugewiesene Rechte**	**Zielbereich**
IDM-Administratoren	GWDG	Administrator	3	• Lesen • Schreiben • Ändern • Löschen	Alle Objekte / alle Attribute im gesamten IDM
IT-Administratoren UMG	UMG	IT-Administratoren	35; 12 IT-Service, 13 IT-Rufbereitschaft, 10 SAP IT-Admins	• Lesen • Schreiben • Ändern • Einfügen von Identitäten	Nur Objekte der UMG
Administratoren der einzelnen Institute und Abteilungen der Universität	UNI	Instituts-admin	186, für die jeweiligen 186 Institutsbereiche	• Lesen • Schreiben • Ändern • Einfügen von Identitäten	Nur Objekte des jeweiligen Institutsbereiches

Berechtigungskonzept Benutzerportal

Endnutzerportal (http://portal.gwdg.de)					
Personen	**Institution**	**Rolle**	**Anzahl der Personen**	**Zugewiesene Rechte**	**Zielbereich**
IDM-Administratoren	GWDG	Administrator	3	• Lesen • Schreiben • Ändern • Löschen	Alle Objekte / alle Attribute im gesamten IDM
Endnutzer	UMG/ UNI	Endnutzer	Alle Personen von UMG/ UNI / GWDG	• Lesen • Schreiben • Ändern	Nur Attribute des eigenen Benutzerobjektes. Geändert werden können hierbei nur die Attribute: • Passwort • Passwort-Vergessen-Funktion • zusätzliche eMail-Adressen • zusätzliche Adressen • zusätzliche Telefonnummern

Anlage 7 – Übersicht der Zielsysteme

Diese Anlage listet die Zielsysteme auf, die zur Anbindung an das Identity-Management-System genutzt werden.

Auflistung der anzubindenden Zielsysteme		
Name des Systems	**Kurzname**	**Verantwortlicher für Zielsystem**
SAP-Personaladministration und Organisationsmanagement der UNI	SAP ERP HCM	Herr Hochdorfer (UNI) Herr Wiebersiek (UMG)
SAP-Rechnungswesen	SAP KIS	Herr Hochdorfer (UNI) Herr Wiebersiek (UMG) Herr Bartussek (UMG)
Active Directory der Universitätsmedizin	AD UMG	Herr Huchthausen (UMG) Frau Nolte (UMG)
Active Directory der Universität	AD UNI	Herr Ißleiber (GWDG)
HIS-Universitätsverzeichnisse	UniVZ	Herr Lambertz (UNI)

Anlage 8a – Zielsystem AD der UNI

Kurzbeschreibung der Anbindung des AD der UNI an das IDM
Erstellung im Rahmen des Gö*-Teilprojektes IDM

Beschreibung des anzubindenden Systems			
Bearbeiter / Datum	Hochdorfer (UNI IT) / 07.09.2013 Martina Willmann (GWDG) Andreas Ißleiber (GWDG)		
Name des Systems (z.B. Windows AD, LDAP)	Active Directory der Universität		
Funktion als Ziel- und / oder Quell-System	Zielsystem als Empfänger der Benutzerdaten (Accounts)		
Kurzbeschreibung des Verzeichnisdienstes / der Datenbank - Version - Ggf. Servicepacks	Active Directory mit der Funktionsebene Windows Server 2003 Aktuell 6 Domain Controller (5x Windows Server 2003, 1x Windows Server 2008 R2)		
Format der Daten (UID, etwaige Sonderattribute, Flags)			
Credentials für den Zugang zum System *(relevant für die Anbindung an das MetaDir)*	**Username/DN**	**Rechte (read/write)**	**Beschreibung**
	[redacted]		Schreibrecht in das AD

Beschreibung des anzubindenden Systems			
Angabe der für die Anbindung relevanten **Attribute** sowie deren mögliche Inhalte (Länge, Zeichensatz), die vom/zum MetaDir übertragen werden	**Attributname**	**Format**	**Bedeutung/Beschreibung**
	Accountname	C 20	Accountname
	Name	C 40	Nachname
	Vorname	C 40	Vorname
	Titel	C 15	Titel
	Namzu	C15	Namenszusatz
	Vorsw	C15	Vorsatzwort
	Geschlecht	C1	Geschlecht
	Abteilung	C 40	Abteilung/Institut/…
	E-Mail	C 240	E-Mail Adresse
	Telefon	C 30	Telefonnummer
	Passwort	C 20	Passwort (verschlüsselt)
	Sperre	C1	Account soll gesperrt werden
	Beginn	Datum	Gültigkeitsbeginn des Accounts
	Ende	Datum	Gültigkeitsende des Accounts
	Personalnummer	C8	Personalnummer als eindeutiges Merkmal der Mitarbeiter
Angabe möglicher Zielsysteme, die über das MetaDir versorgt werden			

<table>
<tr><th colspan="4">Beschreibung des anzubindenden Systems</th></tr>
<tr><td rowspan="2">Abhängigkeiten zu anderen Systemen</td><td colspan="2">System</td><td>Abhängigkeit</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td rowspan="3">Ansprechpartner für das System</td><td>Name</td><td>Telefon</td><td>eMail</td></tr>
<tr><td>GWDG, AD-Team</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td rowspan="2">Umfang Anzahl der existierenden bzw. zu erwartenden Accounts/Objekte</td><td colspan="2">Anzahl der Objekte
Stand: 07.09.2013</td><td>Mögliche zukünftige Anzahl
Stand: 07.09.2013</td></tr>
<tr><td colspan="2">ca. 15.000</td><td>Mit keinen gravierenden Fluktuationen zu rechen</td></tr>
<tr><td>Datenschutz/Sicherheits-relevanz. Bsp.:
- Daten dürfen nicht den Bereich verlassen</td><td colspan="3"></td></tr>
<tr><td>Passwort Policy
(wenn vorhanden)
- Länge des Passwortes
- Sonderzeichen
- Groß/Kleinschreibung</td><td colspan="3">Wird durch das Benutzerportal definiert. Im AD selbst existieren keine Passwordpolicies, da ausschließlich Passwörter durch das Portal geändert werden können.</td></tr>
<tr><td>Etwaige redundante Systeme (z. B. Windows AD-Cluster)</td><td colspan="3">6 Domain Controller</td></tr>
<tr><td>IP-Adresse(n) des/der Systems/Systeme</td><td colspan="3"></td></tr>
</table>

Anlage 8b – Zielsystem SAP HR

Kurzbeschreibung der Anbindung von SAP ERP HCM an das IDM
Erstellung im Rahmen des Gö*-Teilprojektes IDM

Beschreibung des anzubindenden Systems			
Bearbeiter / Datum	Wiebersiek, Hochdorfer / 25.06.2011 - aktualisiert 25.02.2016		
Name des System (z.B. Windows AD, LDAP)	SAP HR Hier werden ausschließlich die Module Personaladministration und Organisationsmanagement betrieben. Ein Mandant 010 für alle Personalbereiche (Universitätsmedizin, Universität, Studentenwerk, Akademie der Wissenschaften, XLAB, GBV, UMG Gastronomie)		
Funktion als Ziel- und / oder Quell-System	Zielsystem als Empfänger der Benutzerdaten (Accounts)		
Kurzbeschreibung des Verzeichnisdienstes / der Datenbank - Version - Ggf. Servicepacks	SAP Release Enterprise ECC 6.0 /EHP 6 Support Package HR 96/EAHR 58 (wird kontinuierlich aktualisiert) Oracle-Datenbank Version 11.2.0.4.0		
Format der Daten (UID, etwaige Sonderattribute, Flags)			
Credentials für den Zugang zum System *(relevant für die Anbindung an das MetaDir)*	**Username/DN**	**Rechte (read/write)**	**Beschreibung**

Beschreibung des anzubindenden Systems			
Angabe der für die Anbindung relevanten **Attribute** sowie deren möglichen Inhalte (Länge, Zeichensatz), die vom/zum MetaDir übertragen werden	**Attributname**	**Format**	**Bedeutung / Beschreibung**
	Accountname	C 12	Accountname
	Name	C 40	Nachname
	Vorname	C 40	Vorname
	Titel	C 15	Titel
	Namzu	C15	Namenszusatz
	Vorsw	C15	Vorsatzwort
	Geschlecht	C1	Geschlecht
	Abteilung	C 40	Abteilung/Institut/…
	E-Mail	C 240	E-Mail Adresse
	Telefon	C 30	Telefonnummer
	Persnr	C 8	Personalnummer
	Kostenstelle	C 8	Kostenstelle / Für die Uni analog zum Feld Kürzel der Organisationseinheit
	Passwort	C 20	Passwort (verschlüsselt)
	Sperre	C 1	Sperre des Accounts
	Beginn	Datum	Gültigkeitsbeginn des Accounts
	Ende	Datum	Gültigkeitsende des Accounts
Angabe möglicher Zielsysteme, die über das MetaDir versorgt werden			

<table>
<tr><th colspan="5">Beschreibung des anzubindenden Systems</th></tr>
<tr><td rowspan="2">Abhängigkeiten zu anderen Systemen</td><td>System</td><td colspan="3">Abhängigkeit</td></tr>
<tr><td>SAP HR</td><td colspan="3">3-System-Landschaft bestehend aus Produktions-, Konsolidierungs- und Entwicklungssystem.

Das jeweilige HR-System stellt auch die Benutzer-Accounts für die ESS-Portallandschaft zur Verfügung.</td></tr>
<tr><td rowspan="4">Ansprechpartner für das System</td><td>Name</td><td colspan="2">Telefon</td><td>eMail</td></tr>
<tr><td>U. Flachs Nobrega, Bereichsleitung</td><td colspan="2">0551/3919629</td><td>Udo.flachs-nobrega@med.uni-goettingen.de</td></tr>
<tr><td>K.-H. Wiebersiek</td><td colspan="2">0551/3933447</td><td>wiebersiek@med.uni-goettingen.de</td></tr>
<tr><td>Z. Hochdorfer</td><td colspan="2">0551/397942</td><td>Zsolt.hochdorfer@zvw.uni-goettingen.de</td></tr>
<tr><td rowspan="2">Umfang Anzahl der existierenden bzw. zu erwartenden Accounts/Objekte</td><td colspan="2">Anzahl der Objekte
Stand: 25.02.2016</td><td colspan="2">Mögliche zukünftige Anzahl
Stand: 25.02.2016</td></tr>
<tr><td colspan="2">> 5000</td><td colspan="2">Es ist mit einem leichten Anstieg der Nutzerzahlen zu rechnen</td></tr>
<tr><td>Datenschutz/Sicherheits-relevanz. Bsp.:
- Daten dürfen nicht den Bereich verlassen</td><td colspan="4"></td></tr>
<tr><td>Passwort Policy
(wenn vorhanden)
- Länge des Passwortes
- Sonderzeichen
- Groß/Kleinschreibung</td><td colspan="4">Anmerkung:
Gesonderte Beschreibung (auf dem IDM SharePoint-Server hinterlegt).</td></tr>
<tr><td>Etwaige redundante Systeme (z. B. Windows AD-Cluster)</td><td colspan="4">keine</td></tr>
<tr><td>IP-Adresse(n) des/der Systems/Systeme</td><td colspan="4">Produktion GAUSSP01: [redacted] (Patlan)
Entwicklung: GAUSST01: [redacted] (Patlan)</td></tr>
</table>

Anlage 8c – Zielsystem SAP KIS

Kurzbeschreibung der Anbindung von SAP KIS an das IDM
Erstellung im Rahmen des Gö*-Teilprojektes IDM

Beschreibung des anzubindenden Systems			
Bearbeiter / Datum	Wiebersiek, Hochdorfer / 26.06.2011 - aktualisiert 25.02.2016		
Name des System (z.B. Windows AD, LDAP)	SAP KIS Hier werden die Module Patientenverwaltung, Rechnungswesen, Materialmanagement, Instandhaltung etc. betrieben. Mandant 010 für die Universitätsmedizin und Mandant 020 für die Universität.		
Funktion als Ziel- und / oder Quell-System	Zielsystem als Empfänger der Benutzerdaten (Accounts)		
Kurzbeschreibung des Verzeichnisdienstes / der Datenbank - Version - Ggf. Servicepacks	SAP Release Enterprise ECC 6.0 Support Package (wird kontinuierlich aktualisiert) Oracle-Datenbank Version 11.2.0.4.0		
Format der Daten (UID, etwaige Sonderattribute, Flags)			
Credentials für den Zugang zum System *(relevant für die Anbindung an das MetaDir)*	**Username/DN**	**Rechte (read/write)**	**Beschreibung**

Beschreibung des anzubindenden Systems			
Angabe der für die Anbindung relevanten **Attribute** sowie deren möglichen Inhalte (Länge, Zeichensatz), die vom/zum MetaDir übertragen werden	**Attributname**	**Format**	**Bedeutung/Beschreibung**
	Accountname	C 12	Accountname
	Name	C 40	Nachname
	Vorname	C 40	Vorname
	Titel	C 15	Titel
	Namzu	C15	Namenszusatz
	Vorsw	C15	Vorsatzwort
	Geschlecht	C1	Geschlecht
	Abteilung	C 40	Abteilung/Institut/…
	E-Mail	C 240	E-Mail Adresse
	Telefon	C 30	Telefonnummer
	Persnr	C 8	Personalnummer
	Kostenstelle	C 8	Kostenstelle / für die Uni analog zum Feld Kürzel der Organisationseinheit
	Passwort	C 20	Passwort (verschlüsselt)
	Sperre	C 1	Sperre des Accounts
	Beginn	Datum	Gültigkeitsbeginn des Accounts
	Ende	Datum	Gültigkeitsende des Accounts
Angabe möglicher Zielsysteme, die über das MetaDir versorgt werden			

Beschreibung des anzubindenden Systems			
Abhängigkeiten zu anderen Systemen	**System**		**Abhängigkeit**
	SAP KIS		3-System-Landschaft bestehend aus Produktions-, Konsolidierungs- und Entwicklungssystem.
Ansprechpartner für das System	**Name**	**Telefon**	**eMail**
	U. Flachs Nobrega, Bereichsleitung	0551/3919629	Udo.flachs-nobrega@med.uni-goettingen.de
Umfang Anzahl der existierenden bzw. zu erwartenden Accounts/Objekte	**Anzahl der Objekte Stand: 25.02.2016**		**Mögliche zukünftige Anzahl Stand: 25.02.2016**
	ca. 3000		Es ist mit keinen gravierenden Anstiegen zu rechnen
Datenschutz/Sicherheits-relevanz. Bsp.: - Daten dürfen nicht den Bereich verlassen			
Passwort Policy (wenn vorhanden) - *Länge des Passwortes* - *Sonderzeichen* - *Groß/Kleinschreibung*	Anmerkung: Gesonderte Beschreibung (auf dem IDM SharePoint-Server hinterlegt).		
Etwaige redundante Systeme (z. B. Windows AD-Cluster)	keine		
IP-Adresse(n) des/der Systems/Systeme	Produktion GAUSSP02: [redacted] (Patlan) Entwicklung: GAUSST02: [redacted] (Patlan)		

Anlage 8d – Zielsystem UniVZ

Kurzbeschreibung der Anbindung von UniVZ an das IDM
Erstellung im Rahmen des Gö*-Teilprojektes IDM

Beschreibung des anzubindenden Systems			
Bearbeiter/in / Datum	Winkler, Hochdorfer / 24.06.2011 Lambertz / 18.07.2011 Lambertz / 07.09.2013		
Name des Systems (z. B. Windows AD, LDAP)	UniVZ (HIS-LSF)		
Funktion als Ziel- und / oder Quell-System	Zielsystem als Empfänger von Mitarbeiterdaten.		
Kurzbeschreibung des Verzeichnisdienstes / der Datenbank	Das System UniVZ (Universitätsverzeichnisse) wird von der Abteilung IT betreut und basiert auf dem LSF Modul der HIS GmbH. Das Modul LSF ist eine Webanwendung für Lehre, Studium und Forschung. Als Datenbank für die Speicherung von Informationen, wie z. B. Lehrveranstaltungen, Personen, wird eine PostgreSQL eingesetzt. Die Anwendung und die Datenbank befinden sich im Netz der Zentralverwaltung.		
- Version - Ggf. Servicepacks	Version HIS-LSF: 14 Version Datenbank: PostgreSQL: 9.x		
Format der Daten (UID, etwaige Sonderattribute, Flags)			
Credentials für den Zugang zum System *(relevant für die Anbindung an das MetaDir)*	**Username/DN**	**Rechte (read/write)**	**Beschreibung**
	Lsf_import_hr	Write	Der User bekommt Schreibrechte auf die Tabelle „tmp_pers“

Beschreibung des anzubindenden Systems			
Angabe der für die Anbindung relevanten **Attribute** sowie deren möglichen Inhalte (Länge, Zeichensatz), die vom/zum MetaDir übertragen werden	**Attributsname**	**Format**	**Bedeutung / Beschreibung**
	EmployeeID	C 12	EmployeeID, aber in SAP-ERP HCM noch nicht gepflegt. Kann für die Zukunft interessant sein.
	Personalnummer	C 8	Personalnummer
	Nachn	C 25	Nachname
	Vorna	C 25	Vorname
	Namzu	C 15	Namenszusatz
	Vorsw	C 15	Vorsatzwort zum Nachnamen
	Titel	C 15	Akad. Titel
	Gesch	C 1	Geschlecht
	Werks	C 4	Personalbereich
	Persk	C 2	Mitarbeiterkreis
	Persg	C 1	Mitarbeitergruppe
	Orgeh_sh	C 12	Kürzel der Organisationseinheit
	Fak_sh	C 12	Kürzel der zugehörigen Fakultät
	Telnr	C 30	Dienstliche Telefonnummer
	Eintritt	Datum	Eintrittsdatum
	Austritt	Datum	Austrittsdatum
	Accountname	C 20	Accountname, aktuell
	NHG	C 1	Gruppe NHG
	Kostenstelle	C 12	Kostenstelle
	E-MAIL	C 240	E-Mail Adresse
Angabe möglicher Zielsysteme, die über das MetaDir versorgt werden	---		

Beschreibung des anzubindenden Systems			
Abhängigkeiten zu anderen Systemen	**System**		**Abhängigkeit**
	StudIP Flexnow		Bekommt Daten aus UniVZ. Liefert Daten in das UniVZ und bekommt Daten aus dem UniVZ.
Ansprechpartner für das System	**Name**	**Telefon**	**eMail**
	Tiberius Winkler	0551/394245	Tiberius.winkler@zvw.uni-goettingen.de
Umfang Anzahl der existierenden bzw. zu erwartenden Accounts/Objekte	**Anzahl der Objekte Stand: 07.09.2013**		**Mögliche zukünftige Anzahl Stand: 07.09.2013**
	ca. 18.800 Objekte		ca. 20.000 Objekte
Datenschutz / Sicherheitsrelevanz. Bsp.: - Daten dürfen nicht den Bereich verlassen	Es handelt sich um personenbezogene Daten.		
Passwort Policy (wenn vorhanden) - *Länge des Passwortes* - *Sonderzeichen* - *Groß/Kleinschreibung*			
Etwaige redundante Systeme (z. B. Windows AD-Cluster)	Die Anwendung ist auf zwei Servern verteilt, die Datenbank läuft auf einem Server.		
IP-Adresse(n) des/der Systems/Systeme	[redacted] (Datenbank)		

Anlage 8e – Zielsystem Active Directory (Verzeichnisdienst) der UMG

Kurzbeschreibung der im Rahmen des Gö*-Teilprojektes anzubindenden Verzeichnisse

Beschreibung des anzubindenden Systems			
Bearbeiter (Name) / Datum	Jens Huchthausen (UMG, G3-76), 14.08.2013 – Aktualisierung 26.02.2016		
Name des System (z.B. Windows AD, LDAP)	UMG ADs (PatLAN und WissLAN); UMGADS für Exchange 2010 der UMG.		
Funktion als Ziel- und/oder Quell-System	Zielsystem als Empfänger der Benutzerdaten (Accounts)		
Kurzbeschreibung des Verzeichnisdienstes/Datenbank - Version - Ggf. Servicepacks	PatLAN UKG-Domäne: Microsoft Active Directory mit der Funktionsebene und Gesamtstrukturebene Windows Server 2003 Aktuell 4 Domain Controller (3x Windows Server 2008 R2) WissLAN UMG-Domäne: Microsoft Active Directory mit der Funktionsebene und Gesamtstrukturebene Windows Server 2003 Aktuell 3 Domain Controller (3x Windows Server 2008 R2)		
Format der Daten (UID, etwaige Sonderattribute, Flags)			
Credentials für den Zugang zum System *(relevant für die Anbindung an das MetaDir)*	**Username/DN**	**Rechte (read/write)**	**Beschreibung**
	[redacted]	Read/write (eingeschränkt)	Anlage von Benutzern aus dem IDM in UMG-AD

			und die Kennwortsynchronisation
Angabe der für die Anbindung	**Attributname**	**Format**	**Bedeutung/Beschreibung**
	Accountname	C 20	Accountname
	Name	C 40	Nachname
	Vorname	C 40	Vorname
	Titel	C 15	Titel
	Aufbereit_Name	C 80	Aufbereiteter Name
	Abteilung	C 40	Abteilung/Institut/...
	E-Mail	C 240	E-Mail Adresse
	Telefon	C 30	Telefonnummer
	Passwort	C 20	Passwort (verschlüsselt)
	Beginn	Datum	
	Ende	Datum	
	Kostenstelle	C20	Kostenstelle des Mitarbeiters
	Funktion	C40	Funktion des Mitarbeiters
	Raum	C40	Raumnummer des Mitarbeiters
	Personalnummer	C20	Personalnummer als eindeutiges Merkmal der Mitarbeiter

<table>
<tr><td>Angabe möglicher Zielsysteme, die über das MetaDir versorgt werden</td><td colspan="3">Active Directories der UMG: UKG UMG, UMGEXC, UMGADS</td></tr>
<tr><td rowspan="3">Ansprechpartner für das System</td><td>Name</td><td>Telefon</td><td>eMail</td></tr>
<tr><td>Jens Huchthausen</td><td>0551-3914451</td><td>huchthausen@med.uni-goettingen.de</td></tr>
<tr><td>Vanessa Nolte</td><td>0551-3913746</td><td>vanessa.nolte@med.uni-goettingen.de</td></tr>
<tr><td></td><td>Torsten Hesse</td><td>0551-3912532</td><td>torsten.hesse@med.uni-goettingen.de</td></tr>
<tr><td rowspan="2">Umfang Anzahl der existierenden bzw. zu erwartenden Accounts/Objekte</td><td colspan="2">Anzahl der Objekte Stand:
Datum: 26.02.2016</td><td>Mögliche zukünftige Anzahl
Stand:
Datum: 26.02.2016</td></tr>
<tr><td colspan="2">>10000</td><td>Keine gravierenden Änderungen.</td></tr>
<tr><td>Datenschutz/Sicherheitsrelevanz. Bsp.:
- Daten dürfen nicht den Bereich verlassen</td><td colspan="3">Verfahren ist enger Abstimmung mit dem Datenschutzbeauftragten der UMG erfolgt. Bei einem etwaigen Ausfall des IDM bleiben die angeschlossenen ADs in ihrer Funktionalität bestehen.</td></tr>
<tr><td>Passwort Policy (wenn vorhanden)
- Länge des Passwortes
- Sonderzeichen
- Groß/Kleinschreibung</td><td colspan="3">Es gelten die Passwortregeln des IDM, die sich an den Passwortregeln des SAP-Systems orientieren.</td></tr>
</table>

Etwaige redundante Systeme (z.B. Windows AD-Cluster)	Derzeit 9 Domaincontroller
IP-Adresse(n) des/der Systems/Systeme	IP-Adressen der Domain Controller der ADs UKG, UMG, UMGADS