B. Bekanntmachungen nach § 78 Abs. 2 NPersVG

Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform DIP mit den daran angeschlossenen Quell- und Zielsystemen an der Gottfried Wilhelm Leibniz Universität Hannover zwischen der Leibniz Universität Hannover und dem Personalrat der Leibniz Universität Hannover in der Fassung vom 21.02.2020

Inhaltsverzeichnis

1. Präambel

Die Leibniz Universität Hannover führt die Anwendung Data Integration Platform (DIP) ein. Zur Regelung der Mitbestimmung beim Einsatz und Weiterentwicklung der DIP schließen die Leibniz Universität und der Personalrat nachstehende Dienstvereinbarung.

Die DIP wird durch die Zentrale Einrichtung der Leibniz Universität IT Services (LUIS) eingeführt und betrieben. Aufgrund der verarbeiteten Daten steht sie in unmittelbarem Zusammenhang zum Campus-Management-System SAP-SLcM (Student Lifecycle Management) und dem zukünftig in SAP-SLcM (gespeist aus SAP Mini-HCM Human Ressource Management) realisierten elektronischen Personen- und Einrichtungsverzeichnis (EPV) sowie dem Identitätsmanagement (IDM) zum Verwalten von Zugängen zu IT-Services der LUH.

2. Gegenstand

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

Sie definiert die Grundsätze für die Einführung und den Betrieb der Anwendung DIP, mittels derer relevante Daten aus unterschiedlichen Quellen an zentraler Stelle zusammengeführt und dedupliziert werden. Die angeschlossenen, in dieser Dienstvereinbarung fest definierten Systeme erhalten von der DIP die für ihren Betrieb erforderlichen Daten. Bei der DIP handelt es sich also um die technische Implementierung von Schnittstellen zwischen fest definierten Quellsystemen und entsprechenden, ebenfalls fest definierten Zielsystemen.

Diese Dienstvereinbarung definiert ebenfalls Grundsätze für die Beschäftigtendaten, die in die DIP eingespeist werden (Quellen) und Grundsätze für die Einführung und den Betrieb der Zielsysteme, die über die DIP Beschäftigtendaten erhalten. Diese Zielsysteme haben eigene Begründungen und Grundlagen für ihren Betrieb. Im Rahmen dieser Dienstvereinbarung werden auch Regelungen über eine Dokumentationspflicht aller angeschlossenen Systeme und der Datenweitergabe getroffen.

3. Geltungsbereich

Diese Dienstvereinbarung gilt für alle Beschäftigten der Leibniz Universität Hannover. Diese werden in geeigneter Form über diese Dienstvereinbarung informiert.

4. Systembeschreibung, Leistungsumfang

Die DIP der Leibniz Universität versorgt über ihre zentrale technische Plattform die Schnittstellen definierter Zielsysteme mit definierten Daten. Die DIP dient damit der Vermeidung von separater Datenhaltung pro Schnittstelle. Sie hält an einer Stelle ausschließlich die Daten vor, die aus definierten Quellsystemen für die definierten Zielsysteme benötigt werden.
Die detaillierte Beschreibung der DIP, ihrer Quellen und der zu beliefernden Zielsysteme und deren Verankerung innerhalb der Systemarchitektur der Universität ergibt sich aus ihrem Fachkonzept **Anlage 1** inkl. Beschreibung von Aufbau, Funktionen und der grundsätzlichen Arbeitsweise.

Abbildung 1: Integration der DIP in die CMSAP-Systemlandschaft (Stand 20170811)

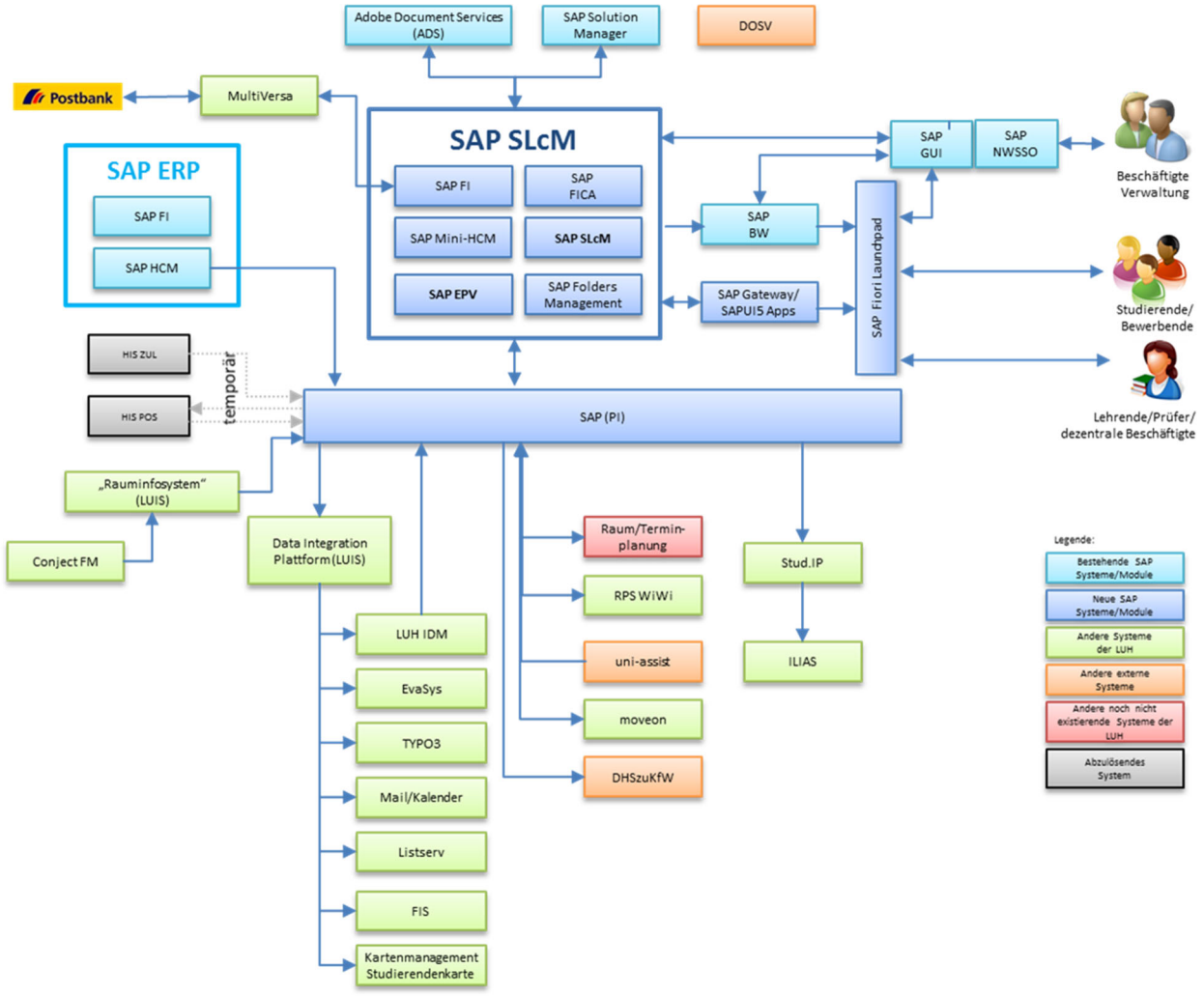
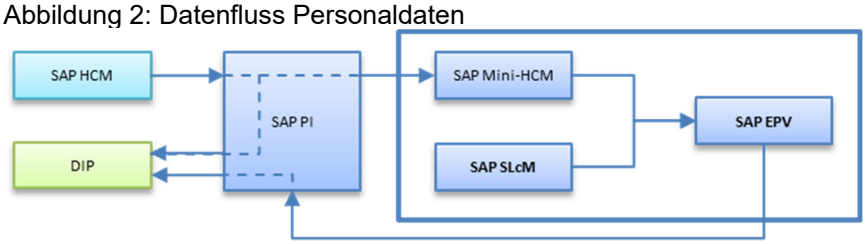


Abbildung 2: Datenfluss Personaldaten



4.1 Bei den Quellsystemen handelt es sich um:

- SAP SLcM (Student Lifecycle Management)
- SAP HCM (Human Capital Management)
- SAP EPV (Einrichtungs- und Personenverzeichnis)

4.2 Bei den Zielsystemen handelt es sich um:

- Identitätsmanagementsystem (IdM)
- TYPO3 Websites der LUH
- Mail / Kalender (Horde, Exchange, SoGo)
- Verteilerlisten zum Versand von E-Mails (Listserv)
- Forschungsinformationssystem (FIS)
- Chipkartenmanagementsystem für die LeibnizCard
- SAP HCM und SAP SLcM

5. Ziel und Zweckbestimmung der DIP

Die Leibniz Universität und der Personalrat stimmen darin überein, dass der Einsatz der DIP folgenden Zielen und Zwecken dient:

- Automatische Übernahme von definierten Daten aus definierten Quellsystemen für definierte Zwecke in den Zielsystemen (Zielen)
- Aufbereitung, Integration und Umschlüsselung von Daten aus den Quellsystemen um die Anforderungen der Zielsysteme abzubilden
- Bereitstellung der aufbereiteten Daten für die Zielsysteme
- Datensparsamkeit: die Daten der Quellsysteme werden nur einmal an einer Stelle aufbereitet und vorgehalten
- Datenqualität: Jedes Zielsystem erhält nur solche Daten, die wirklich benötigt und entsprechend aufbereitetet sind zum erforderlichen Zeitpunkt
- regelmäßige Aktualisierung in den angeschlossenen Anwendungen
- Erhöhung der Sicherheit durch personenbezogene Nutzungsrechte und eindeutige Identitäten
- Zentrale Bereitstellung der Daten für die Zielsysteme durch die DIP verringert die Fehleranfälligkeit und den administrativen Aufwand

6. Schutz der Persönlichkeitsrechte, Datenschutz

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

Die zum Erreichen der Zweckbestimmung dieser Dienstvereinbarung erforderlichen Personendaten die in der DIP erhoben, verarbeitet, genutzt und weitergegeben werden, sind in den **Anlagen 2.1 bis 3.7** mit ihrer Zweckbestimmung abschließend aufgeführt und dokumentiert (Datenkatalog).

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

Das Datenschutzkonzept mit Beschreibung der Mechanismen, die die DIP vor unberechtigten Zugriffen schützen, das Lösch- bzw. Archivierungskonzept, werden mit dem Datenschutzbeauftragten abgestimmt und ergeben sich zusammen mit der Darstellung der Verarbeitungstätigkeit nach Art. 30 DSGVO zur DIP aus **Anlage 4.**

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

7. Leistungs- und Verhaltenskontrolle

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

Wird eine missbräuchliche Nutzung festgestellt, ist die Leibniz Universität Hannover verpflichtet, die Ursachen dafür unverzüglich abzustellen.
Die Leibniz Universität stellt sicher, dass die Administratoren der DIP auf die Einhaltung dieser Dienstvereinbarung verpflichtet werden.

8. Berechtigungskonzept - Zugriffsbestimmungen

Nur die für den Betrieb des DIP zuständigen Administratoren (Fachteam IdM des LUIS) haben zur Entwicklung, Wartung und Fehleranalyse Zugriff auf den DIP-Server und auf die DIP-Datenbank. Sowohl der Server als auch die Datenbank der DIP sind durch gesonderte Authentifizierungen vor unberechtigten Zugriffen geschützt.

9. Auswertungen und Protokolle

Alle in der DIP anfallenden Auswertungen und Protokolldaten, die im Sinne dieser Vereinbarung personenbezogene Beschäftigtendaten enthalten, dienen ausschließlich der Administration der DIP zu Zwecken der Gewährleistung der Systemsicherheit und der Analyse und Korrektur technischer Fehler. Andere Auswertungen sind unzulässig. Diese Daten unterliegen der strikten Zweckbindung gem. § 10 Abs. 4 NDSG.

Die Löschung erfolgt entsprechend der **Anlage 4** und nach den gesetzlichen Fristen.

10. Schnittstellen

Schnittstellen im Sinne dieser Dienstvereinbarung sind technische Übergabepunkte und Verfahren, durch die Daten der DIP an die Zielsysteme übergeben werden, oder durch die Daten aus Quellsystemen auf die hier geregelte DIP gelangen.

Quellsysteme der DIP sind Systeme oder Verzeichnisse, die die DIP mit Daten speisen. Die Speicherung von Daten muss soweit erfolgen, dass eine Identität eindeutig erkannt, zugeordnet und alle Zielsysteme von der DIP zentral mit den für sie jeweils notwendigen Daten versorgt werden können. Die zu erfassenden Daten werden jeweils pro Quellsystem ermittelt und dem zuvor genannten Zweck angepasst. In der **Anlagen 2** sind die aus den jeweiligen Quellsystemen übernommenen Datenfelder abschließend aufgeführt.

Zielsysteme der DIP sind Systeme, die die DIP zur Bereitstellung, Integration und Aufbereitung nutzen. Es werden nur diejenigen Daten übergeben, die für die Zweckbestimmung des Zielsystems erforderlich und im Rahmen dieser Dienstvereinbarung für das Zielsystem geregelt sind. Die an die jeweiligen Zielsysteme zu übergebenden Daten und Datenfelder sind in der **Anlage 3** abschließend aufgeführt.

Jedes angeschlossene Quell- und Zielsystem wird in Form eines Steckbriefes, innerhalb der **Anlagen 2 und 3** dokumentiert. Diese Dokumentation muss folgende Informationen enthalten:

a) eine Aufstellung der aus den Quellen an die DIP zu leitenden Datenfelder
b) eine Aufstellung der von der DIP an die Zielsysteme weiterzugebenden Datenfelder,
c) eine grundsätzliche Beschreibung des Systems,
d) eine Darlegung der Ziele, die mit dem System verfolgt werden,
e) eine Beschreibung, wie das System administriert wird,
f) eine Beschreibung, wie in dem System Datenschutz gewährleistet wird,
g) eine Beschreibung und Begründung der Regeln, die der Weitergabe der Daten zugrunde liegen. Insbesondere ist darzulegen, ob die Regeln grundsätzlich auf einem Automatismus basieren oder durch einen zusätzlichen Administrationsvorgang beeinflusst werden.

Für Systeme, die per Dienstvereinbarungen geregelt sind, reicht bzgl. der Punkte c) bis g) der Verweis auf die entsprechende Vereinbarung aus.

Für jedes neu an die DIP anzuschließende System werden die **Anlagen 2 und 3** durch einen entsprechenden Steckbrief ergänzt. Diese Ergänzung unterliegt der Mitbestimmung des Personalrats, welcher das Recht hat, die Vorlage ergänzender Informationen zu verlangen. Die Mitbestimmung für das anzuschließende System selbst ist dadurch nicht verbraucht.

11. Rechte der Beschäftigten, Qualifizierung

Alle Beschäftigten erhalten auf Anfrage Auskunft über alle zu ihrer Person gespeicherten Daten.

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

Alle Administratoren der DIP werden rechtzeitig und in geeigneter Art und Weise über die Einführung und Funktionsweise des Systems sowie den Inhalt dieser Dienstvereinbarung informiert.

12. Rechte der Personalvertretungen

Entsprechend § 59 Nr. 2 NPersVG hat der Personalrat die Pflicht und das Recht, die Einhaltung aller einschlägigen Gesetze und Normen zu überwachen. Jede zukünftige Änderung und Erweiterung des in den **Anlagen 1 - 4** dokumentierten Systems unterliegt der Mitbestimmung und Kontrolle des Personalrats. Insbesondere werden keine Funktionen aktiviert, die nicht in den Anlagen dokumentiert sind.

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

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

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

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

13. Schlussbestimmungen, Inkrafttreten, Kündigung

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

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

Diese Dienstvereinbarung mit Anlagen tritt mit der Bekanntgabe im Verkündungsblatt in Kraft. Sie kann einseitig unter Einhaltung einer Kündigungsfrist von vier Monaten, frühestens jedoch zum 31.12.2021 gekündigt werden. Sollten einzelne Bestimmungen dieser Vereinbarung insbesondere wegen Verstoßes gegen § 82 NPersVG, nichtig sein oder werden, so berührt dies nicht die Gültigkeit der übrigen Bestimmungen. Anstelle der unwirksamen Bestimmungen, oder zur Ausfüllung eventueller Lücken der Vereinbarung soll eine angemessene Regelung treten, die dem am Nächsten kommt, was die Parteien nach ihrer Zwecksetzung gewollt

haben. Die einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform. Im Übrigen gilt § 78 Abs. 4 NPersVG.

Nach Beendigung der Dienstvereinbarung ist der änderungslose Weiterbetrieb der DIP unter den hier vereinbarten Bedingungen möglich. Die Dienststelle und der Personalrat verpflichten sich, im Falle der Kündigung unverzüglich Verhandlungen über eine Nachfolgeregelung aufzunehmen.

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

Hannover, den

Leibniz Universität Hannover
Der Präsident

_____

Hannover, den

Leibniz Universität Hannover
Personalrat

_____

Anlagenübersicht, Vers. 1.0 vom 16.12.19

Anlage 1	Fachkonzept DIP	
Anlage 2 2.1 2.2 2.3	Quellsysteme: Steckbrief SAP SLcM Steckbrief SAP HCM Steckbrief SAP EPV	
Anlage 3 3.1 3.2 3.3 3.4 3.5 3.6 3.7	Zielsysteme: Steckbrief LUH IDM Steckbrief TYPO3 Steckbrief Mail/Kalender Steckbrief Listserv Steckbrief FIS Steckbrief Chipkartenmanagementsystem Steckbrief SAP HCM und SAP SLcM	
Anlage 4	Datenschutzkonzept, Lösch- und Archivierungskonzept, Bestätigung des Datenschutzbeauftragten (incl. Löschen/Archivierung) und Darstellung der Verarbeitungstätigkeit nach Art. 30 DSGVO DIP	

Anlage 1

zur Dienstvereinbarung über die Einführung und Anwendung der Data Integration Platform an der Gottfried Wilhelm Leibniz Universität Hannover zwischen der Leibniz Universität Hannover unddem Personalrat der Leibniz Universität Hannover

Fachkonzept

Dokumenteninformation

1. Beschreibung der Systemlandschaft

1.1 Bezug der Daten aus den Quellsystemen

Kernstück der Data Integration Platform (DIP) ist eine Datenbank, die alle notwendigen Daten zum Betrieb der angebundenen Zielsysteme enthält. Die Datenbank muss zu Beginn des regulären Betriebes einmalig alle für den Betrieb der Zielsysteme notwendigen Daten aus den Quellsystemen erhalten. Die angebundenen Quellsysteme sind SAP-HCM, SAP-SlcM und das SAP-EPV.

Werden im SAP Datensätze aktualisiert, prüft die Process Integration Schnittstelle (SAP-PI), ob diese Datensätze die Data Integration Platform benötigt, und übermittelt im Falle einer Abgabeberechtigung die geänderten Datensätze via XML-Message an die Data Integration Platform. Die Datenübertragung erfolgt verschlüsselt.

1.2 Aufbereitung der Daten

Die Data Integration Platform nimmt die XML-Message der Quellsysteme entgegen, bereitet die im XML enthaltenen Datensätze auf, so dass sie in die Datenbank gespeichert werden können und der Datenbestand aktualisiert werden kann.

Datenbestände mit unterschiedlicher Prägung (z.B. Personendaten) sollen von der Data Integration Platform unter einer einheitlichen Identifikationsnummer (LUH-ID) zusammengefasst werden. Liegen Identitäten einer Person (z.B. Student und Doktorand) aus unterschiedlichen Datenbeständen der Hochschule vor, müssen sie aufgrund der Anforderungen der Zielsysteme ebenfalls unter einer einheitlichen Identifikationsnummer (LUH-ID) zusammengefügt werden.

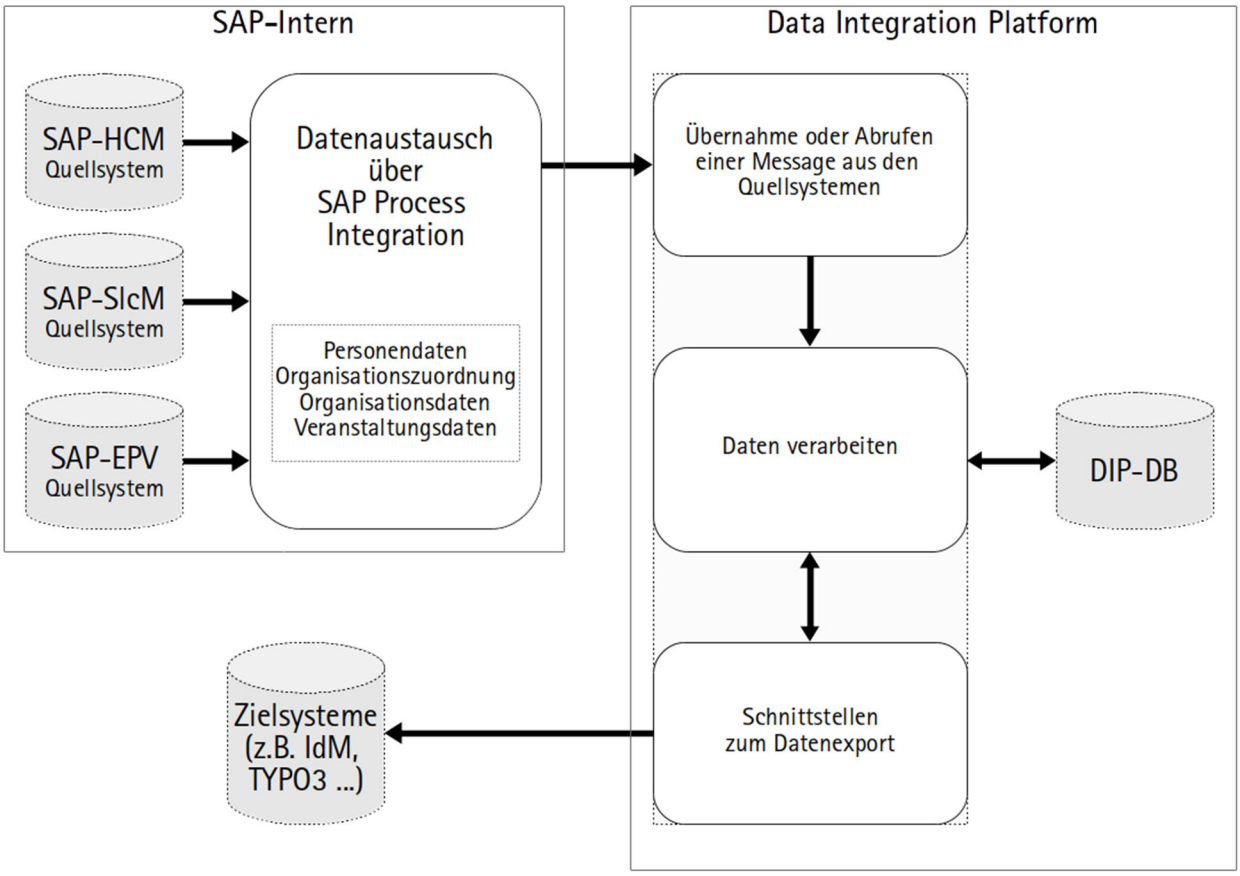
1.3 Ausgabe der Daten an die angeschlossenen Zielsysteme

Die Data Integration Platform enthält für jedes aangeschlossene Zielsystem eine eigene Schnittstelle, die die notwendigen Daten aus der DIP-Datenbank aufnimmt und den jeweiligen Zielsystemen zur Verfügung stellt. Je nach Anforderung des Zielsystems werden die für den Betrieb des Zielsystems benötigten Daten als kompletter Dump ausgegeben oder das Zielsystem fordert nur einen Teil der festgelegten Datenfelder an. Die technische Ausprägung der Schnittstelle gibt das Zielsystem vor. Jedes Zielsystem muss sich systemindividuell authentifizieren. Es erhält nur die in Anlage 3 der Dienstvereinbarung zur Data Integration Platform festgelegt Daten.

1.4 Graphische Darstellung der Systemlandschaft

Die folgende Graphik zeigt schematisch den Datenfluss zwischen den Datenbanken der Quell- und Zielsysteme und der Data Integration Platform.

Abbildung 1: Integration der Data Integration Platform in die IT-Struktur der LUH



Die Data Integration Platform soll keine speziellen Funktionalitäten (GUI, Weboberfläche) zur Verwaltung der personenbezogenen Daten besitzen. Die DIP soll weitgehend ohne fremden Eingriff automatisiert betrieben werden. Die Kommunikationswege sind auf die Verbindungen zu Quell- und Zielsystemen für die Datenübermittlung beschränkt, daneben wird das System nur zu Zwecken der Systemadministration und des Backups angesprochen.

1.5 Technische Realisierung

Die DIP ist eine Individualsoftware, die im LUIS entwickelt wurde um die Schnittstellen zwischen Quell- und Zielsystemen mit ähnlichen Daten effizient und datensparsam abzuwickeln. Technisch besteht die DIP aus einer Datenbank (PostgreSQL), einem Message Broker zum Abholen und Versenden der Nachrichten (RabbitMQ) sowie Anwendungen zur Aufbereitung und Bereitstellung der Daten (Individualentwicklung in Python und Java). Die DIP wird in einer virtualisierten Umgebung im LUIS auf Basis von Linux betrieben.

2. Quellsysteme
Die Quellsysteme werden in Anlage 2 der Dienstvereinbarung Data Integration Platform beschrieben.

3. Zielsysteme
Die Zielsysteme werden in Anlage 3 der Dienstvereinbarung Data Integration Platform beschrieben.

Anlage 2

Übersicht angeschlossene Quellsysteme

2.1. SAP SlcM

Grunddaten des Quellsystems:

Name	Campusmanagement auf Basis SAP SLcM (Student Lifecycle Management)
Betreiber	Niedersächsisches Hochschulkompetenzzentrum für SAP (CCC)
Zweck	Verwaltung der Studierendendaten

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus dem Quellsystem:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 100. bis 199. sind weitere Attribute aus dem Bereich Studierendendaten. Die Attribute mit den Nummer 400. bis 499. sind weitere Attribute aus dem Bereich Veranstaltungsdaten.

Nr.	Quelle	Daten	zur Nr.	Zweck in der DIP
1.	SAP SLcM	Nachname		siehe Anlage 3
2.	SAP SLcM	Vorname(n)		siehe Anlage 3
3.	SAP SLcM	Geburtsname		siehe Anlage 3
4.	SAP SLcM	Geburtsdatum/-ort		siehe Anlage 3
5.	SAP SLcM	Anrede/Geschlecht		siehe Anlage 3
6.	SAP SLcM	Namenszusätze		siehe Anlage 3
7.	SAP SLcM	akad. Titel		siehe Anlage 3
10.	SAP SLcM	Matrikelnummer		siehe Anlage 3
11.	SAP SLcM	Studiengang (Studiengangs-ID), angestrebter Abschluss, Immatrikulationsstatus		siehe Anlage 3
12.	SAP SLcM	LUH-ID		siehe Anlage 3
13.	SAP SLcM	Nutzerstatus (z.B. beurlaubt)		siehe Anlage 3
14.	SAP SLcM	E-Mail-Adresse		siehe Anlage 3
15.	SAP SLcM	Anschrift		siehe Anlage 3
16.	SAP SLcM	Telefonnummer		siehe Anlage 3
17.	SAP SLcM	Organisationszugehörigkeit(en)		siehe Anlage 3
21.	SAP SLcM	Start-/Endedatum der Universitätszugehörigkeit		siehe Anlage 3
100.	SAP SLcM	interne ID der Person im CMS		siehe Anlage 3
101.	SAP SLcM	Statuswerte Einschreibung		siehe Anlage 3
102.	SAP SLcM	Statuswerte Hörerstatus		siehe Anlage 3
103.	SAP SLcM	Vorsatzwort (von und zu)	6.	siehe Anlage 3

104.	SAP SLcM	Zusatzwort (Freiherr)	6.	siehe Anlage 3
105.	SAP SLcM	c/o (Zustellanweisung)	15.	siehe Anlage 3
106.	SAP SLcM	Straße	15.	siehe Anlage 3
107.	SAP SLcM	Hausnummer	15.	siehe Anlage 3
108.	SAP SLcM	Land (zur Adresse)	15.	siehe Anlage 3
109.	SAP SLcM	Postleitzahl	15.	siehe Anlage 3
110.	SAP SLcM	Ort	15.	siehe Anlage 3
111.	SAP SLcM	Postfach	15.	siehe Anlage 3
113.	SAP SLcM	Nationalität		siehe Anlage 3
114.	SAP SLcM	Titel/Grad, Ehrentitel	6.	siehe Anlage 3
115.	SAP SLcM	Exma-Grund.	11.	siehe Anlage 3
116.	SAP SLcM	Studiengänge (Studiengangs-ID)	11.	siehe Anlage 3
117.	SAP SLcM	Studiengänge (Kürzel)	11.	siehe Anlage 3
118.	SAP SLcM	ÖPNV-Semesterticket		siehe Anlage 3
119.	SAP-SlCM	Studierendenkategorie (z.B. Promotionsstudierende)		siehe Anlage 3
400.	SAP SLcM	ID		siehe Anlage 3
401.	SAP SLcM	Name		siehe Anlage 3
402.	SAP SLcM	Kennung		siehe Anlage 3
403.	SAP SLcM	Freigabestatus		siehe Anlage 3
404.	SAP SLcM	Akademisches Jahr		siehe Anlage 3
405.	SAP SLcM	Akademische Periode		siehe Anlage 3
406.	SAP SLcM	Art		siehe Anlage 3
407.	SAP SLcM	Inhaltl. Beschreibung		siehe Anlage 3
408.	SAP SLcM	Sichtbar im Webauftritt?		siehe Anlage 3
409.	SAP SLcM	Zuordnung zu OE		siehe Anlage 3
411.	SAP SLcM	Zuordnung in VVZ-Struktur		siehe Anlage 3
412.	SAP SLcM	Zuordnung zu anderen Veranstaltungen		siehe Anlage 3
413.	SAP SLcM	Zuordnung zu Studiengängen		siehe Anlage 3
414.	SAP SLcM	Termine		siehe Anlage 3
415.	SAP SLcM	URL zu SLcM		siehe Anlage 3
416.	SAP SLcM	Dozenten		siehe Anlage 3

Die Schnittstelle zu SAP SLcM befindet sich noch in Entwicklung. Zur Übertragung der notwendigen Attribute wird neben der speziell für Phase 1 entwickelten Schnittstelle noch die Standardnachricht für Studierende aus dem it.education-System übertragen. Die Attribute sind in der Datei: 20171129-SIIA_DIP_StudentStudyMaintain.wsdl spezifiziert.

b) Datenfelder, die von der Data Integration Platform (DIP) an die Zielsysteme übergeben werden:

Siehe Anlage 3 zur Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform (DIP).

c) Beschreibung:

SAP SlcM (SAP Student Lifecycle Management) ist ein Softwareprodukt zur Verwaltung der Studierendendaten. SAP SlcM soll an der Leibniz Universität Hannover als Campusmanagement System, die Studierenden von der Bewerbung, Einschreibung bis zum Abschluss des Studiums begleiten. Das Campusmanagement System soll im wesentlichen folgende Aufgaben erfüllen:

- Alumnimanagement
- Akademische Struktur und Organisationsstruktur
- Bewerber-, Zulassungs- und Studierendenmanagement
- Gebührenmanagement
- Lehrveranstaltungs- und Raumvergabemanagement
- Prüfungsmanagement
- Studiengangsmanagement

d) Ziel und Zweck:

Das Campusmanagement System auf Basis SAP SLcM (Student Lifecycle Management) hat zum Ziel, die Verwaltungsprozesse des Studienzyklus der Studierenden von der Bewerbung um einen Studienplatz bis zur Zeugnisausgabe effektiv und effizient zu unterstützen.

e) Administration des Zielsystems:

Das Modul SAP SLcM (Student Lifecycle Management) wird durch das Niedersächsische Hochschulkompetenzzentrum für SAP und dem Fachteam SAP-Basis des LUIS administriert.

f) Regeln des Datenschutzes:

Siehe Projekt CMSAP.

g) Regeln zur Datenweitergabe:

Nur die in dieser Anlage festgelegten Datenfelder werden von SAP SLcM zur DIP übertragen. Die Übertragung erfolgt automatisiert und verschlüsselt. Die DIP speichert die Daten in eine Datenbank, dedupliziert die Daten gegebenenfalls und gibt sie an die Zielsysteme in der benötigten Form weiter. Die an jedes Zielsystem übergebenen Datenfelder sind in der Anlage 3 zur Dienstvereinbarung Data Integration Platform (DIP) festgelegt. Mit Beginn des regulären Betriebes der DIP, sollen die definierten Datenfelder einmal initial per full-load übertragen werden. Werden im anschließenden laufenden Betrieb die Datenfelder im SAP SlcM geändert, sorgt die SAP interne Process Integration Schnittstelle (SAP PI) per HTTPS-Adapter (Message Queuing) für den Datenaustausch zur DIP. Die Weitergabe der definierten Datenfelder an die Zielsysteme wird zu festgelegten Zeitpunkten (z.B. sofort nach Nachrichteneingang, zu definierten Zeiten) ausgeführt. Zur Herstellung konsistenter Daten z.B. im Fehlerfalle kann im SAP SLcM ein erneuter full-load ausgelöst werden.

2.2. SAP HCM

Grunddaten des Quellsystems:

Name	SAP HCM (Human Capital Management)
Betreiber	Niedersächsisches Hochschulkompetenzzentrum für SAP (CCC)
Zweck	Verwaltung der Beschäftigtendaten

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus dem Quellsystem:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 100. bis 199. sind Attribute aus dem Bereich Studierendendaten. Die Attribute mit den Nummer 200. bis 299. sind weitere Attribute aus dem Bereich Beschäftigtendaten.

Nr.	Quelle	Daten	zur Nr.	Zweck in der DIP
1	HCM	Nachname		siehe Anlage 3
2	HCM	Vorname(n)		siehe Anlage 3
3	HCM	Geburtsname		siehe Anlage 3
4	HCM	Geburtsdatum/-ort		siehe Anlage 3
5	HCM	Anrede/Geschlecht		siehe Anlage 3
6	HCM	Namenszusätze		siehe Anlage 3
7	HCM	akad. Titel		siehe Anlage 3
8	HCM	Personalnummer		siehe Anlage 3
9	HCM	Art des Beschäftigungsverhältnisses		siehe Anlage 3
12	HCM	LUH-ID		siehe Anlage 3
13	HCM	Nutzerstatus		siehe Anlage 3
17	HCM	Organisationszugehörigkeit(en)		siehe Anlage 3
21	HCM	Start-/Enddatum der Universitätszugehörigkeit		siehe Anlage 3
100	HCM	interne ID der Person im CMS		siehe Anlage 3
103	HCM	Vorsatzwort	6	siehe Anlage 3
104	HCM	Zusatzwort	6	siehe Anlage 3
113	HCM	Nationalität		siehe Anlage 3
114	HCM	Titel/Grad, Ehrentitel	6	siehe Anlage 3
200	HCM	Aktiv/Inaktiv	13	siehe Anlage 3
201	HCM	CP Pers.Nr.	8	siehe Anlage 3
202	HCM	Akademischer Grad (vorgestellt)	7	siehe Anlage 3
203	HCM	Akademischer Grad (nachgestellt)	7	siehe Anlage 3
204	HCM	Hauspostkennzeichen	15	siehe Anlage 3
205	HCM	Beschäftigtengruppe NHG	9	siehe Anlage 3
206	HCM	Kennzeichen: Sichtbarkeit		siehe Anlage 3
211	HCM	Eintrittdatum	21	siehe Anlage 3
212	HCM	Austrittdatum	21	siehe Anlage 3
213	HCM	LUH-OE-ID	17	siehe Anlage 3
320	HCM	Fächergruppen, Lehr- und Forschungsbereiche und Fachgebiete (Destatis)		siehe Anlage 3

b) Datenfelder, die von der Data Integration Platform (DIP) an die Zielsysteme übergeben werden:

Die Punkte c) bis f) sind in der Dienstvereinbarung SAP-HR beschrieben. Siehe: **https://www.personalrat.uni-hannover.de/fileadmin/institut/pdf/Dienstvereinbarungen/dv_sap-erp-hr_vkb2011-08.pdf**

g) Regeln zur Datenweitergabe:

Nur die in dieser Anlage festgelegten Datenfelder werden von SAP HCM zur DIP übertragen. Die Übertragung erfolgt automatisiert und verschlüsselt. Die DIP speichert die Daten in eine Datenbank, dedupliziert die Daten gegebenenfalls und gibt sie an die Zielsysteme in der benötigten Form weiter. Die an jedes Zielsystem übergebenen Datenfelder sind in der Anlage 3 zur Dienstvereinbarung Data Integration Platform (DIP) festgelegt. Mit Beginn des regulären Betriebes der DIP, sollen die definierten Datenfelder einmal initial per full-load übertragen werden. Werden im anschließenden laufenden Betrieb die Datenfelder im SAP HCM geändert, sorgt die SAP interne Process Integration Schnittstelle (SAP PI) per HTTPS-Adapter (Message Queuing) für den Datenaustausch zur DIP. Die Weitergabe der definierten Datenfelder an die Zielsysteme wird zu festgelegten Zeitpunkten (z.B. sofort nach Nachrichteneingang, zu definierten Zeiten) ausgeführt. Zur Herstellung konsistenter Daten z.B. im Fehlerfalle kann im SAP HCM ein erneuter full-load ausgelöst werden.

2.3. SAP EPV

Grunddaten des Quellsystems:

Name	SAP EPV (Einrichtungs- und Personenverzeichnis)
Betreiber	Niedersächsisches Hochschulkompetenzzentrum für SAP (CCC)
Zweck	Verwaltung des Einrichtungs- und Personenverzeichnisses

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus dem Quellsystem:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 200. bis 299. sind Attribute aus dem Bereich Beschäftigtendaten. Die Attribute mit den Nummer 300. bis 399. sind weitere Attribute aus dem Bereich Organisationsdaten.

Nr.	Quelle	Daten	zur Nr.	Zweck in der DIP
12	EPV	LUH-ID		siehe Anlage 3
14	EPV	E-Mail-Adresse (Dienstlich)		siehe Anlage 3
16	EPV	Telefonnummer (Dienstlich)		siehe Anlage 3
15	EVP	Anschrift (Dienstlich)		siehe Anlage 3
17	EPV	Organisationszugehörigkeit(en)		siehe Anlage 3
18	EPV	Gebäude/Raum		siehe Anlage 3
207	EPV	Funktion		siehe Anlage 3
208	EPV	Sprechzeiten		siehe Anlage 3
209	EPV	URL zu pers. Seite		siehe Anlage 3
210	EPV	URL zu SLcM		siehe Anlage 3
213	EPV	LUH-OE-ID	17	siehe Anlage 3
214	EPV	Sortierkennzeichen zur Anzeige wie im EPV		siehe Anlage 3
215	EPV	Diensttelefonnummer	16	siehe Anlage 3
306	EPV	Adresse – Straße der Organisationseinheit	15	siehe Anlage 3

307	EPV	Adresse – Hausnummer der Organisations-einheit	15	siehe Anlage 3
308	EPV	Adresse – Ort der Organisationseinheit	15	siehe Anlage 3
309	EPV	Adresse – Postleitzahl der Organisations-einheit	15	siehe Anlage 3
310	EPV	Adresse – Land der Organisationseinheit	15	siehe Anlage 3
311	EPV	URL zu SlcM		siehe Anlage 3
312	EPV	URL zu Webauftritt		siehe Anlage 3
316	EPV	Telefonnummern, Zentrale der Organisati-onseinheit,		siehe Anlage 3
317	EPV	E-Mail-Adressen, Funktionsmailadressen der Organisationseinheit		siehe Anlage 3
300	EPV	interne ID der Organization im CMS		siehe Anlage 3
301	EPV	Name der Organisationseinheit		siehe Anlage 3
302	EPV	Organisations-Typ		siehe Anlage 3
303	EPV	Startdatum		siehe Anlage 3
304	EPV	Endedatum		siehe Anlage 3
305	EPV	Übergeordnete OE		siehe Anlage 3
314	EPV	Objektkürzel – Ort der Organisationseinheit		siehe Anlage 3
315	EPV	Kurzname der Organisationseinheit		siehe Anlage 3
318	EPV	Vollständiger Name der Organisationsein-heit		siehe Anlage 3
319	EPV	SAP-Kürzel, Kürzel der Organisationsein-heit in SAP		siehe Anlage 3
321	EPV	name of the organizational unit		siehe Anlage 3
322	EPV	short name of the organizational unit		siehe Anlage 3
323	EPV	full name of the organizational unit		siehe Anlage 3

b) Datenfelder, die von der Data Integration Platform (DIP) an die Zielsysteme übergeben werden:

Siehe Anlage 3 zur Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform (DIP).

c) Beschreibung:

Im SAP EPV werden die Organisationsdaten aus SAP HCM um Daten des Einrichtungs- und Personenverzeichnisses (z.B. Funktionen, Adressdaten) ergänzt.

d) Ziel und Zweck:

Zuordnung der Beschäftigtendaten zu Organisationseinheiten über Funktionen zur Realisierung des Einrichtungs- und Personenverzeichnisses der LUH.

e) Administration des Zielsystems:

SAP HCM und SAP EPV werden durch das Niedersächsische Hochschulkompetenzzentrum für SAP und dem Fachteam SAP-Basis des LUIS administriert.

f) Regeln des Datenschutzes:
siehe Projekt CMSAP (EPV)

g) Regeln zur Datenweitergabe:

Nur die in dieser Anlage festgelegten Datenfelder werden von SAP EPV zur DIP übertragen. Die Übertragung erfolgt automatisiert und verschlüsselt. Die DIP speichert die Daten in eine Datenbank, dedupliziert die Daten gegebenenfalls und gibt sie an die Zielsysteme in der geforderten Form weiter. Die an jedes Zielsystem übergebenen Datenfelder sind in der Anlage 3 zur Dienstvereinbarung Data Integration Platform (DIP) festgelegt. Mit Beginn des regulären Betriebes der DIP, sollen die definierten Datenfelder einmal initial per full-load übertragen werden. Werden im anschließenden laufenden Betrieb die Datenfelder im SAP EPV geändert, sorgt die SAP interne Process Integration Schnittstelle (SAP PI) per HTTPS-Adapter (Message Queuing) für den Datenaustausch zur DIP. Die Weitergabe der definierten Datenfelder an die Zielsysteme wird zu festgelegten Zeitpunkten (z.B. sofort nach Nachrichteneingang, zu definierten Zeiten) ausgeführt. Zur Herstellung konsistenter Daten z.B. im Fehlerfalle kann im SAP EPV ein erneuter full-load ausgelöst werden.

Anlage 3

Übersicht angeschlossene Zielsysteme

3.1. Identitätsmanagementsystem (IdM)

3.2. TYPO3 Websites der LUH

3.3. Mail/Kalender (Horde, Exchange, SoGo)

3.4. Verteilerlisten zum Versand von E-Mails (Listserv)

3.5. Forschungsinformationssystem (FIS)

3.6. Chipkartenmanagementsystem für die LeibnizCard

3.7. SAP HCM und SAP SLcM

3.1. Identitätsmanagementsystem (IdM)

Grunddaten des Zielsystems:

Name	Identitätsmanagementsystem
Betreiber	Leibniz Universität IT Services
Zweck	Bereitstellung und Verwaltung von Nutzerzugängen zu EDV-Ressourcen

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus den Quellsystemen:

Siehe Anlage 2 zu der Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform (DIP)

b) Datenfelder, die von der Data Integration Platform (DIP) an das Zielsystem Identitätsmangementsysten (IdM) weitergegeben werden:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 100. bis 199. sind weitere Attribute aus dem Bereich Studierendendaten. Die Attribute mit den Nummer 200. bis 299. sind weitere Attribute aus dem Bereich Beschäftigtendaten. Die Attribute mit den Nummer 300. bis 399. sind weitere Attribute aus dem Bereich Organisationsdaten. Die Attribute mit den Nummer 400. bis 499. sind weitere Attribute aus dem Bereich Veranstaltungsdaten.

Nr.	**Quelle**			**Daten**	**zur Nr.**	**Zweck**
	SLcM	**HCM**	**EPV**			
1	SlcM	HCM		Nachname		Weitergabe IdM
2	SlcM	HCM		Vorname(n)		Weitergabe IdM
3	SlcM	HCM		Geburtsname		Weitergabe IdM
4	SlcM	HCM		Geburtsdatum/-ort		Weitergabe IdM
5	SlcM	HCM		Anrede/Geschlecht		Weitergabe IdM
6	SlcM	HCM		Namenszusätze		Weitergabe IdM
7	SlcM	HCM		akad. Titel		Weitergabe IdM

8		HCM		Personalnummer		Weitergabe IdM
9	SlcM	HCM		Art des Beschäftigungsverhältnisses		Weitergabe IdM
10	SlcM			Matrikelnummer		Weitergabe IdM
11	SlcM			Studiengang (Studiengangs-ID), angestrebter Abschluss, Immatrikulationsstatus		Weitergabe IdM
12	SlcM	HCM	EPV	LUH-ID		Weitergabe IdM
13	SlcM	HCM		Nutzerstatus		Weitergabe IdM
14	SlcM		EPV	E-Mail-Adresse		Weitergabe IdM
15	SlcM		EPV	Anschrift		Weitergabe IdM
16	SlcM		EPV	Telefonnummer		Weitergabe IdM
17	SlcM	HCM	EPV	Organisationszugehörigkeit(en)		Weitergabe IdM
19	SlcM			Benutzergruppen		Weitergabe IdM
20	SlcM			Primäre Benutzergruppe		Weitergabe IdM
21	SlcM	HCM		Start-/Endedatum der Universitätszugehörigkeit		Weitergabe IdM
100	SlcM	HCM		interne ID der Person im CMS		Weitergabe IdM
103	SlcM	HCM		Vorsatzwort	6	Weitergabe IdM
104	SlcM	HCM		Zusatzwort	6	Weitergabe IdM
105	SlcM			c/o	15	Weitergabe IdM
106	SlcM			Straße	15	Weitergabe IdM
107	SlcM			Hausnummer	15	Weitergabe IdM
108	SlcM			Land	15	Weitergabe IdM
109	SlcM			Postleitzahl	15	Weitergabe IdM
110	SlcM			Ort	15	Weitergabe IdM
111	SlcM			Postfach	15	Weitergabe IdM
114	SlcM	HCM		Titel/Grad, Ehrentitel	6	Weitergabe IdM
115	SlcM			Exma-Grund	11	Weitergabe IdM
116	SlcM			Studiengänge (Studiengangs-ID)	11	Weitergabe IdM
117	SlcM			Studiengänge (Kürzel)	11	Weitergabe IdM
118	SlcM			ÖPNV-Semesterticket		Weitergabe IdM
200		HCM		Aktiv/Inaktiv	13	Weitergabe IdM
201		HCM		CP Pers.Nr.	8	Weitergabe IdM
202		HCM		Akademischer Grad (vorgestellt)	7	Weitergabe IdM
203		HCM		Akademischer Grad (nachgestellt)	7	Weitergabe IdM
204		HCM		Hauspostkennzeichen	15	Weitergabe IdM
205		HCM		Beschäft.gruppe NHG	9	Weitergabe IdM
207			EPV	Funktion		Weitergabe IdM
211		HCM		Eintrittdatum	21	Weitergabe IdM
212		HCM		Austrittdatum	21	Weitergabe IdM
213		HCM	EPV	LUH-OE-ID	17	Weitergabe IdM

215			EPV	Diensttelefonnummer	16	Weitergabe IdM
300			EPV	interne ID der Organisation im CMS		Weitergabe IdM
301			EPV	Name		Weitergabe IdM
302			EPV	Organisations-Typ		Weitergabe IdM
303			EPV	Startdatum		Weitergabe IdM
304			EPV	Endedatum		Weitergabe IdM
305			EPV	Übergeordnete OE		Weitergabe IdM
311			EPV	URL zu SlcM		Weitergabe IdM

c) Die Anlagen c) bis f) sind in der Dienstvereinbarung Identitätsmanagementsystem (IdM) beschrieben.

https://www.personalrat.uni-hannover.de/fileadmin/institut/pdf/Dienstvereinbarungen/dv_idm_vkb2017_05.pdf

g) Regeln zur Datenweitergabe:

Nur die in dieser Anlage festgelegten Datenfelder werden von der Data Integration Platform (DIP) zum IdM übertragen. Die Übertragung erfolgt automatisiert und verschlüsselt. Die Übernahme der fest definierten Datenfelder aus der DIP erfolgt zeitnah.

3.2. TYPO3 Websites der LUH

Grunddaten des Zielsystems:

Name	TYPO3 Websites der LUH
Betreiber	Leibniz Universität IT Services
Zweck	Bereitstellung der Webauftritts der LUH

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus den Quellsystemen:

Siehe Anlage 2 zu der Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform (DIP)

b) Datenfelder, die von der Data Integration Platform (DIP) an das Zielsystem TYPO3 Websites der LUH weitergegeben werden:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 100. bis 199. sind weitere Attribute aus dem Bereich Studierendendaten. Die Attribute mit den Nummer 200. bis 299. sind weitere Attribute aus dem Bereich Beschäftigtendaten. Die Attribute mit den Nummer 300. bis 399. sind weitere Attribute aus dem Bereich Organisationsdaten. Die Attribute mit den Nummer 400. bis 499. sind weitere Attribute aus dem Bereich Veranstaltungsdaten.

Nr.	Quelle			Daten	zur Nr.	Zweck
	SLcM	HCM	EPV			
1	SlcM	HCM		Nachname		Publikation EPV/Impressum/ Nutzerverwaltung
2	SlcM	HCM		Vorname(n)		Publikation EPV/Impressum/ Nutzerverwaltung
5	SlcM	HCM		Anrede/Geschlecht		Publikation EPV/Impressum/ Nutzerverwaltung
6	SlcM	HCM		Namenszusätze		Publikation EPV/Impressum/ Nutzerverwaltung
7	SlcM	HCM		akad. Titel		Publikation EPV/Impressum/ Nutzerverwaltung
12	SlcM	HCM	EPV	LUH-ID		Nutzerverwaltung
14	SlcM		EPV	E-Mail-Adresse		Publikation EPV/Impressum/ Nutzerverwaltung
15	SlcM		EPV	Anschrift		Publikation EPV/Impressum/ Nutzerverwaltung
16	SlcM		EPV	Telefonnummer		Publikation EPV/Impressum/ Nutzerverwaltung
17	SlcM	HCM	EPV	Organisationszugehörigkeit(en)		Publikation EPV/Impressum/ Nutzerverwaltung
18	SlcM		EPV	Gebäude/Raum		Publikation EPV/Impressum/ Nutzerverwaltung
100	SlcM	HCM		interne ID der Person im CMS		Nutzerverwaltung
106	SlcM			Straße	15	Publikation EPV/Impressum/ Nutzerverwaltung
107	SlcM			Hausnummer	15	Publikation EPV/Impressum/ Nutzerverwaltung
109	SlcM			Postleitzahl	15	Publikation EPV/Impressum/ Nutzerverwaltung
110	SlcM			Ort	15	Publikation EPV/Impressum/ Nutzerverwaltung
204		HCM		Hauspostkennzeichen	15	Publikation EPV/Impressum/ Nutzerverwaltung

206		HCM		Kennzeichen: Sichtbarkeit		Publikation EPV/Impressum/ Nutzerverwaltung
207			EPV	Funktion		Publikation EPV/Impressum/ Nutzerverwaltung
208			EPV	Sprechzeiten		Publikation EPV/Impressum/ Nutzerverwaltung
209			EPV	URL zu pers. Seite		Publikation EPV/Impressum/ Nutzerverwaltung
213		HCM	EPV	LUH-OE-ID	17	Publikation EPV/Impressum/ Nutzerverwaltung
214			EPV	Sortierkennzeichen zur Anzeige wie im EPV		Publikation EPV/Impressum
215			EPV	Diensttelefonnummer	16	Publikation EPV/Impressum/ Nutzerverwaltung
216				Mobile	16	Publikation EPV/Impressum/ Nutzerverwaltung
217				Fax	16	Publikation EPV/Impressum/ Nutzerverwaltung
218				Funktionskurzname (shortName)		Publikation EPV/Impressum/ Nutzerverwaltung
300			EPV	interne ID der Organization im CMS		Publikation EPV/Impressum/ Nutzerverwaltung
301			EPV	Name der Organisationseinheit		Publikation EPV/Impressum/ Nutzerverwaltung
306			EPV	Adresse – Straße der Organisationseinheit	15	Publikation EPV/Impressum/ Nutzerverwaltung
307			EPV	Adresse – Hausnummer der Organisationseinheit	15	Publikation EPV/Impressum/ Nutzerverwaltung
308			EPV	Adresse – Ort der Organisationseinheit	15	Publikation EPV/Impressum/ Nutzerverwaltung
309			EPV	Adresse – Postleitzahl der Organisationseinheit	15	Publikation EPV/Impressum/ Nutzerverwaltung
315			EPV	Kurzname der Organisationseinheit		Publikation EPV/Impressum/ Nutzerverwaltung
318			EPV	Vollständiger Name der Organisationseinheit		Publikation EPV/Impressum/ Nutzerverwaltung

c) Beschreibung:

Die Einrichtung Leibniz Universität IT Services bietet einen Dienst zur Erstellung und Pflege der Webauftritte an der Leibniz Universität Hannover an. Die Webauftritte werden mit dem Content-Management-System TYPO3 betrieben. Die Einrichtungen und Institute erhalten auf Anforderung eine Webinstallation mit vorgegeben Layout-Templates zur Darstellung ihrer Webauftritte nach den Corporate-Design Vorgaben der LUH. Die Nutzung des TYPO3-Webservices mit dem LUH-Template-Vorgaben ist für alle dienstlichen Webauftritte mit Außenwirkung verbindlich. Die Ausgestaltung und Pflege der einzelnen Webseiteninhalte liegt im Verantwortungsbereich der Einrichtungen und Institute der LUH. Zur Verwaltung der eigenen Webseiten sind persönliche Nutzerzugänge (Redakteur) erforderlich. Der Webdienst umfasst Schulungen und Support für die Redakteure.

d) Ziel und Zweck:

Bereitstellung eines umfassenden Webdienstes für die Webpräzenz der Leibniz Universität Hannover.

e) Administration des Zielsystems:

Das Content-Management-System TYPO3 wird durch das Fachteam Webservice der Einrichtung Leibniz Universität IT Services administriert. Es haben nur die mit der Administration beauftragten Personen Zugriff auf die Server und die Logdateien. Die Server werden im internen Netz der LUH betrieben und sind von außen (abgesehen von der Webpräsenz) nicht erreichbar. Für die Inhalte der Webseiten sind die einzelnen Einrichtungen und Institute der Leibniz Universität Hannover verantwortlich.

f) Regeln des Datenschutzes:

Die Meldung einer Verarbeitungstätigkeit gem. Art. 30 Datenschutzgrundverordnung (DSGVO) ist erfolgt. Bezeichnung des bestehenden Verfahrens: Webservice LUIS.

g) Regeln zur Datenweitergabe:

Nur die in dieser Anlage festgelegten Datenfelder werden von der Data Integration Platform (DIP) zum Dienst „TYPO3 Websites der LUH“ übertragen. Die Übertragung erfolgt automatisiert und verschlüsselt. Die Übernahme der fest definierten Datenfelder aus der DIP erfolgt zeitnah.

3.3. Mail/Kalender (Horde, Exchange, SoGo)

Grunddaten des Zielsystems:

Name	Mail / Kalender (Horde, Exchange, SoGo)
Betreiber	Leibniz Universität IT Services
Zweck	Bereitstellung Mailservice/Kalender

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus den Quellsystemen:

Siehe Anlage 2 zu der Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform (DIP)

b) Datenfelder, die von der Data Integration Platform (DIP) an das Zielsystem Mail/Kalender (Horde, Exchange, SoGo) weitergegeben werden:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 100. bis 199. sind weitere Attribute aus dem Bereich Studierendendaten. Die Attribute mit den Nummer 200. bis 299. sind weitere Attribute aus dem Bereich Beschäftigtendaten. Die Attribute mit den Nummer 300. bis 399. sind weitere Attribute aus dem Bereich Organisationsdaten. Die Attribute mit den Nummer 400. bis 499. sind weitere Attribute aus dem Bereich Veranstaltungsdaten.

Nr.	**Quelle**			**Daten**	**zur Nr.**	**Zweck**
	SLcM	**HCM**	**EPV**			
1	SlcM	HCM		Nachname		Nutzerverwaltung
2	SlcM	HCM		Vorname(n)		Nutzerverwaltung

12	SlcM	HCM	EPV	LUH-ID		Nutzerverwaltung
14	SlcM		EPV	E-Mail-Adresse		Nutzerverwaltung

c) Beschreibung:

Die Einrichtung Leibniz Universität IT Services bietet für alle Mitarbeiterinnen, Mitarbeiter und Studierende der Leibniz Universität Hannover den Dienst Mail und Kalender an. Der Dienst Mail stellt eine Mailadresse und eine kennwortgeschütze Mailbox zum Senden, Empfangen und Speichern von Nachrichten zur Verfügung. Der Dienst Kalender verfügt über eine kennwortgeschütze Weboberfläche und Client Zugänge zur Verwaltung von Terminen. Es können Termine erstellt und alle an diesen Dienst teilnehmenden Personen dazu eingeladen werden. Die Weboberfläche ermöglicht die Einsicht der eigenen Termine und die Einsicht der Termine der Mitbenutzerinnen und Mitbenutzer.

d) Ziel und Zweck:

Mail: Bereitstellung eines Informations- und Kommunikationsdienstes für alle Mitglieder und Angehörigen der Leibniz Universität Hannover.

Kalender: Bereitstellung eines Terminplaners mit Visualisierung der Termine für alle Beschäftigten der Leibniz Universität Hannover. Voraussetzung für den Dienst Kalender ist eine Mailadresse der LUH.

e) Administration des Zielsystems:

Der Dienst „Mail/Kalender“ wird durch das Fachteam Mail der Einrichtung Leibniz Universität IT Services administriert. Es haben nur die mit der Administration beauftragten Personen Zugriff auf die Server und die Logdateien. Die Server werden im internen Netz der LUH betrieben und sind von außen nur über die Webmail-Oberfläche und Mail- bzw. Kalender-Protokolle erreichbar.

f) Regeln des Datenschutzes:

Die Meldung einer Verarbeitungstätigkeit gem. Art. 30 Datenschutzgrundverordnung (DSGVO) ist erfolgt. Bezeichnung des bestehenden Verfahrens: Zentraler E-Mail und Kalender-Dienst der LUH

g) Regeln zur Datenweitergabe:

Nur die in dieser Anlage festgelegten Datenfelder werden von der Data Integration Platform (DIP) zum Dienst „Mail/Kalender (Horde, Exchange, SoGo)“ übertragen. Die Übertragung erfolgt automatisiert und verschlüsselt. Die Übernahme der fest definierten Datenfelder aus der DIP erfolgt zeitnah.

3.4. Verteilerlisten zum Versand von E-Mails (Listserv)

Grunddaten des Zielsystems:

Name	Verteilerlisten zum Versand von E-Mails (Listserv)
Betreiber	Leibniz Universität IT Services
Zweck	Verteilerlisten zum Versand von E-Mails an ausgewähle Personen

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus den Quellsystemen:

Siehe Anlage 2 zu der Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform (DIP)

b) Datenfelder, die von der Data Integration Platform (DIP) an das Zielsystem Verteilerlisten zum Versand von E-Mails (Listserv) weitergegeben werden:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 100. bis 199. sind weitere Attribute aus dem Bereich Studierendendaten. Die Attribute mit den Nummer 200. bis 299. sind weitere Attribute aus dem Bereich Beschäftigtendaten. Die Attribute mit den Nummer 300. bis 399. sind weitere Attribute aus dem Bereich Organisationsdaten. Die Attribute mit den Nummer 400. bis 499. sind weitere Attribute aus dem Bereich Veranstaltungsdaten.

Nr.	Quelle			Daten	zur Nr.	Zweck
	SLcM	HCM	EPV			
1	SlcM	HCM		Nachname		versenden von E-Mails
2	SlcM	HCM		Vorname(n)		versenden von E-Mails
14	SlcM		EPV	E-Mail-Adresse		versenden von E-Mails
207			EPV	Funktion		versenden von E-Mails

c) Beschreibung:

Der Dienst „Verteilerlisten zum Versand von E-Mails (Listserv)“ stellt den universitären Einrichtungen ein Mailinglisten-Management System zur Verfügung. Über eine Weboberfläche können berechtigte Personen Mailinglisten (Listen von E-Mailadressen) zur Kommunikation mit Einrichtungen der LUH, Interessengemeinschaften und universitätsübergreifenden Arbeitsgruppen festlegen. Der Zugang zu den Mailinglisten ist kennwortgeschützt.

d) Ziel und Zweck:

Über Listen von E-Mailadressen soll ein Kommunikationsmittel für einen ausgewählten Personenkreis zur Verfügung stehen.

e) Administration des Zielsystems:

Der Dienst „Verteilerlisten zum Versand von E-Mails (Listserv)“ wird durch das Fachteam Mail der Einrichtung Leibniz Universität IT Services administriert. Es haben nur die mit der Administration beauftragten Personen Zugriff auf die Server und die Logdateien. Die Server werden im internen Netz der LUH betrieben und sind von außen nur über die Weboberfläche des Mailinglisten-Management Systems erreichbar. Die Inhalte der Mailinglisten werden von den Personen mit Zugriffsberechtigungen auf die Liste administriert.

f) Regeln des Datenschutzes:

Die Meldung einer Verarbeitungstätigkeit gem. Art. 30 Datenschutzgrundverordnung (DSGVO) ist erfolgt. Bezeichnung des bestehenden Verfahrens: Listserv: Zentraler E-Mail-Verteiler-Dienst

g) Regeln zur Datenweitergabe:

Für die Aufnahme von E-Mailadressen in die Mailinglisten sind ausschließlich die Listeneigentümer zuständig. Die Daten werden zum Teil von Hand eingegeben oder automatisiert eingelesen.

3.5. Forschungsinformationssystem (FIS)

Grunddaten des Zielsystems:

Name	Forschungsinformationssystem
Betreiber	Dezernat 4 – Forschung und EU-Hochschulbüro, Technologietransfer
Zweck	Verwaltung von wissenschaftlichen Publikationen

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus den Quellsystemen:

Siehe Anlage 2 zu der Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform (DIP)

b) Datenfelder, die von der Data Integration Platform (DIP) an das Zielsystem Forschungsinformationssystem (FIS) weitergegeben werden:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 100. bis 199. sind weitere Attribute aus dem Bereich Studierendendaten. Die Attribute mit den Nummer 200. bis 299. sind weitere Attribute aus dem Bereich Beschäftigtendaten. Die Attribute mit den Nummer 300. bis 399. sind weitere Attribute aus dem Bereich Organisationsdaten. Die Attribute mit den Nummer 400. bis 499. sind weitere Attribute aus dem Bereich Veranstaltungsdaten.

Nr.	**Quelle**			**Daten**	**zur Nr.**	**Zweck**
	SLcM	**HCM**	**EPV**			
1	SlcM	HCM		Nachname		Nutzerverwaltung Publikation
2	SlcM	HCM		Vorname(n)		Nutzerverwaltung Publikation
4	SlcM	HCM		Geburtsdatum/-ort		Nutzerverwaltung Publikation
5	SlcM	HCM		Anrede/Geschlecht		Nutzerverwaltung Publikation
6	SlcM	HCM		Namenszusätze		Nutzerverwaltung Publikation
7	SlcM	HCM		akad. Titel		Nutzerverwaltung Publikation
9	SlcM	HCM		Art des Beschäftigungsverhältnisses		Nutzerverwaltung Publikation
11	SlcM			Studiengang (Studiengangs-ID), angestrebter Abschluss, Immatrikulationsstatus		Nutzerverwaltung Publikation
12	SlcM	HCM	EPV	LUH-ID		Nutzerverwaltung
14	SlcM		EPV	E-Mail-Adresse		Nutzerverwaltung Publikation
17	SlcM	HCM	EPV	Organisationszugehörigkeit(en)		Nutzerverwaltung Publikation
19	SlcM			Benutzergruppen		Nutzerverwaltung Publikation
21	SlcM	HCM		Start-/Endedatum der Universitätszugehörigkeit		Nutzerverwaltung

103	SlcM	HCM		Vorsatzwort	6	Nutzerverwaltung Publikation
104	SlcM	HCM		Zusatzwort	6	Nutzerverwaltung Publikation
113	SlcM	HCM		Nationalität		Nutzerverwaltung Publikation
114	SlcM	HCM		Titel/Grad, Ehrentitel	6	Nutzerverwaltung Publikation
119	SlCM			Studierendenkategorie (z.B. Promotionsstudierende)	11	Nutzerverwaltung Publikation
202		HCM		Akademischer Grad (vorgestellt)	7	Nutzerverwaltung Publikation
203		HCM		Akademischer Grad (nachgestellt)	7	Nutzerverwaltung Publikation
204		HCM		Hauspostkennzeichen	15	Nutzerverwaltung Publikation
205		HCM		Beschäftigtengruppe NHG	9	Nutzerverwaltung
207			EPV	Funktion		Nutzerverwaltung Publikation
209			EPV	URL zu pers. Seite		Nutzerverwaltung Publikation
212		HCM		Austrittdatum	21	Nutzerverwaltung
213		HCM	EPV	LUH-OE-ID	17	Nutzerverwaltung Publikation
215			EPV	Diensttelefonnummer		Nutzerverwaltung Publikation
301			EPV	Name		Nutzerverwaltung Publikation
302			EPV	Organisations-Typ		Nutzerverwaltung Publikation
303			EPV	Startdatum		Nutzerverwaltung Publikation
304			EPV	Endedatum		Nutzerverwaltung Publikation
305			EPV	Übergeordnete OE		Nutzerverwaltung Publikation
306			EPV	Adresse – Straße		Nutzerverwaltung Publikation
307			EPV	Adresse – Hausnummer		Nutzerverwaltung Publikation
308			EPV	Adresse – Ort		Nutzerverwaltung Publikation
309			EPV	Adresse – Postleitzahl		Nutzerverwaltung Publikation
310			EPV	Adresse – Land		Nutzerverwaltung Publikation
312			EPV	URL zu Webauftritt		Nutzerverwaltung Publikation

315			EPV	Kurzname		Nutzerverwaltung Publikation
316			EPV	Telefonnummern		Nutzerverwaltung Publikation
317			EPV	E-Mail-Adressen		Nutzerverwaltung Publikation
318			EPV	Vollständiger Name		Nutzerverwaltung Publikation
319			EPV	SAP-Kürzel		Nutzerverwaltung Publikation
320		HCM		Fächergruppen, Lehr- und Forschungsbereiche und Fachgebiete (Destatis)		Nutzerverwaltung Publikation

c) Beschreibung:

Kernstück des Forschungsinformationssystems ist eine Datenbank mit Forschungsinformationen, die mit Personendaten und Daten der Forschungseinrichtung verknüpft ist. Die Forschungsinformationen selbst, können untereinander verknüpft werden und es besteht die Möglichkeit Daten manuell einzugeben, oder automatisiert aus anderen Datenbanken zu übernehmen. Eine Webschnittstelle bietet den Nutzerinnen und Nutzern des Forschungsinformationssystems einen bequemen Zugang zu den Informationen in der Datenbank.

d) Ziel und Zweck:

Bereitstellungen von Publikationen und Projekten der Leibniz Universität Hannover aus dem Bereich Forschung. Das Forschungsinformationssystem soll Mitarbeiterinnen und Mitarbeiter in die Lage versetzen Forschungsergebnisse leichter zu erreichen.

e) Administration des Zielsystems:

Das Forschungsinformationssystem wird durch das Dezernat 4 – Forschung und EU-Hochschulbüro, Technologietransfer und dem LUIS administriert.

f) Regeln des Datenschutzes:

Die Meldung einer Verarbeitungstätigkeit gem. Art. 30 Datenschutzgrundverordnung (DSGVO) ist erfolgt. Bezeichnung des bestehenden Verfahrens: Testphase des zukünftigen Forschungsinformationssystems der Universität Hannover.

g) Regeln zur Datenweitergabe:

Nur die in dieser Anlage festgelegten Datenfelder werden von der Data Integration Platform (DIP) zum Forschungsinformationssystems übertragen. Die Übertragung erfolgt automatisiert und verschlüsselt. Die Übernahme der fest definierten Datenfelder aus der DIP erfolgt zeitnah.

3.6. Chipkartenmanagementsystem für die LeibnizCard

Grunddaten des Zielsystems:

Name	LeibnizCard für Studierende und Beschäftigte
Betreiber	Leibniz Universität IT Services
Zweck	Einheitlicher Digitaler Ausweis mit Zugangs- und Geldbörsenfunktion

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus den Quellsystemen:

Siehe Anlage 2 zu der Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform (DIP)

b) Datenfelder, die von der Data Integration Platform (DIP) an das Zielsystem Chipkartenmanagementsystem für die LeibnizCard weitergegeben werden:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 100. bis 199. sind weitere Attribute aus dem Bereich Studierendendaten. Die Attribute mit den Nummer 200. bis 299. sind weitere Attribute aus dem Bereich Beschäftigtendaten. Die Attribute mit den Nummer 300. bis 399. sind weitere Attribute aus dem Bereich Organisationsdaten. Die Attribute mit den Nummer 400. bis 499. sind weitere Attribute aus dem Bereich Veranstaltungsdaten.

Nr.	Quelle			Daten	zur Nr.	Zweck
	SLcM	HCM	EPV			
1	SlcM	HCM		Nachname		Nachweis der Zugehörigkeit
2	SlcM	HCM		Vorname(n)		Nachweis der Zugehörigkeit
5	SlcM	HCM		Anrede/Geschlecht		Nachweis der Zugehörigkeit
6	SlcM	HCM		Namenszusätze		Nachweis der Zugehörigkeit
7	SlcM	HCM		akad. Titel		Nachweis der Zugehörigkeit
10	SlcM			Matrikelnummer		Nachweis der Zugehörigkeit
12	SlcM	HCM	EPV	LUH-ID		Nachweis der Zugehörigkeit
13	SlcM	HCM		Nutzerstatus (z.B. beurlaubt bei Studierenden)		Nachweis der Zugehörigkeit
15	SlcM			Anschrift		Nachweis der Zugehörigkeit
21	SlcM	HCM		Start-/Endedatum der Universitätszugehörigkeit		
25				Initialpasswort (in DIP/IDM generiert)		Nachweis der Zugehörigkeit
101	SlcM			Statuswerte Einschreibung		Nachweis der Zugehörigkeit
118	SlcM			ÖPNV-Semesterticket		Nachweis der Zugehörigkeit
204		HCM		Hauspostkennzeichen	15	Nachweis der Zugehörigkeit

c) Beschreibung:

Mit der LeibnizCard für Studierende und Beschäftigte soll die Identitätsprüfung, die Bezahlfunktion und die Schließfunktion (Zugangskontrolle) rund um das Campusleben der Studierenden und Be-

schäftigten auf einer Karte zusammengefügt werden. Die Karte dient als Studierendenausweis, Beschäftigtenausweis, Semesterticket, Bibliotheksausweis, Mensakarte und als CampusCard für den Hochschulsport, zur Zeiterfassung und zum Zugang zu den SAP Systemen (Zertifikatsfunktion).

d) Ziel und Zweck:

Es sollen die verschiedenen Einzelausweise für die Einrichtungen der Leibniz Universität Hannover zu einem Multifunktionalen Ausweis mit Bezahlfunktion wie z.B. Mensakarte zusammengeführt werden.

e) Administration des Zielsystems:

Das Chipkartenmanagementsystem wird durch das LUIS administriert.

f) Regeln des Datenschutzes:

Die Meldung einer Verarbeitungstätigkeit gem. Art. 30 Datenschutzgrundverordnung (DSGVO) ist erfolgt. Bezeichnung des bestehenden Verfahrens: LeibnizCard

g) Regeln zur Datenweitergabe:

Nur die in dieser Anlage festgelegten Datenfelder werden von der Data Integration Platform (DIP) zum Chipkartenmanagementsystem übertragen. Die Übertragung erfolgt automatisiert und verschlüsselt. Die Übernahme der fest definierten Datenfelder aus der DIP erfolgt zeitnah.

3.7. SAP HCM und SAP SLcM

Grunddaten des Zielsystems:

Name	SAP HCM (Human Capital Management), Campusmanagement auf Basis SAP SLcM (Student Lifecycle Management)
Betreiber	Niedersächsisches Hochschulkompetenzzentrum für SAP (CCC)
Zweck	Verwaltung der Beschäftigtendaten, Verwaltung der Studierendendaten

a) Folgende Datenfelder erhält die Data Integration Platform (DIP) aus den Quellsystemen:

Siehe Anlage 2 zu der Dienstvereinbarung über die Einführung und Anwendung der Anwendung Data Integration Platform (DIP)

b) Datenfelder, die von der Data Integration Platform (DIP) an das Zielsystem SAP HCM und SAP SLcM für weitergegeben werden:

Die Attribute mit den Nummern 1. bis 27. sind in der Anlage 2 (Datenkatalog) der Dienstvereinbarung Identitätsmanagementsystem vergeben und belegt. Die Nummern 28. bis 99. sind für Änderungen der Dienstvereinbarung Identitätsmanagementsystem reserviert. Die Attribute mit den Nummer 100. bis 199. sind weitere Attribute aus dem Bereich Studierendendaten. Die Attribute mit den Nummer 200. bis 299. sind weitere Attribute aus dem Bereich Beschäftigtendaten. Die Attribute mit den Nummer 300. bis 399. sind weitere Attribute aus dem Bereich Organisationsdaten. Die Attribute mit den Nummer 400. bis 499. sind weitere Attribute aus dem Bereich Veranstaltungsdaten.

Nr.	Quelle				Daten	zur Nr.	Zweck
	SLcM	HCM	EPV	DIP/IdM			
8		HCM			Personalnummer		Übermittlung der Zugangsdaten IdM

12	SlcM	HCM	EP V	DIP/IdM	LUH-ID		Übermittlung der Zugangs-daten IdM
14	SlcM		EP V	DIP/IdM	E-Mail-Adresse		Übermittlung der Zugangs-daten IdM
25				DIP/IdM	Initialpasswort		Übermittlung der Zugangs-daten IdM
201		HCM			CP Pers.Nr.	8	Übermittlung der Zugangs-daten IdM

Anmerkung zu Nummer 14: Die E-Mailadresse ist die Kontaktemailadresse und sie muss im IdM durch die nutzenden Personen bestätigt werden. Sie kann im IdM geändert werden. Dies hat zur Folge, dass sie nach der Bestätigung durch die nutzenden Personen zu den Quellsystemen zurück übertragen werden muss.

Anmerkung zu Nummer 25: Das Initialpasswort für die Erstanmeldung am IdM wird ebenfalls im IdM/DIP generiert und muss für den Ausdruck der Zugangsdaten für neue Beschäftigte wieder an die Quellsysteme übermittelt werden. Hat die berechtigte Person das Initialpasswort auf ein persönliches Passwort geändert, erhalten die Quellsysteme für das Attribut Initialpasswort den Textinhalt „Wurde bereits von Ihnen geändert“. Das persönliche Passwort für das IdM kann auf das Initialpasswort zurückgesetzt werden, so dass ein neues persönliches Passwort vergeben werden kann.

c) Beschreibung:

Siehe Anlage 2.2 und Anlage 2.1 zur Dienstvereinbarung Data Integration Platform (DIP) unter Punkt c) Beschreibung.

d) Ziel und Zweck:

Siehe Anlage 2.2 und Anlage 2.1 zur Dienstvereinbarung Data Integration Platform (DIP) unter Punkt d) Ziel und Zweck.

e) Administration des Zielsystems:

Das Modul SAP HCM (Human Capital Management) und das Modul SAP SLcM (Student Lifecycle Management) wird durch das Niedersächsische Hochschulkompetenzzentrum für SAP und dem Fachteam SAP-Basis des LUIS administriert.

f) Regeln des Datenschutzes:

Siehe Projekt CMSAP.

g) Regeln zur Datenweitergabe:

Nur die in dieser Anlage festgelegten Datenfelder werden von der Data Integration Platform (DIP) zu SAP HCM und zu SAP SLcM übertragen. Die Übertragung erfolgt automatisiert und verschlüsselt. Die Übernahme der fest definierten Datenfelder aus der DIP erfolgt zeitnah.

Anlage 4

Datenschutzkonzept

4. Sicherheitskonzept und Administration

4.1 Schutzbedarfsfeststellung

In der DIP werden zu den Personendaten weitere Attribute wie Studiengangsinformationen, Kontaktdaten und Daten der Organisationseinheiten der LUH vorgehalten (vgl. Anlage 2). Diese Daten sind im datenschutzrechtlichen Sinne der Schutzstufe B zuzuordnen und insbesondere vor nicht-autorisiertem Zugriff zu schützen (Vertraulichkeit). Die Integrität ist für die Stammdaten durch den nächtlichen Import und einem Message Broker zum Abholen und Versenden der Nachrichten, automatisch nach spätestens einem Tag gegeben. Die DIP dient zum Empfangen der Daten aus definierten Quellsystemen (vgl. Anlage 2) mit anschließender Aufbereitung und Weitergabe der Daten an die in der Anlage 3 aufgeführten Zielsysteme. Daher ist der Schutzbedarf bzgl. Informationssicherheit angelehnt an den BSI-Grundschutz-Standard 100-2 der DIP bzgl. der Integrität als hoch zu bewerten. Je nach Zielsystem muss die Aktualität der Daten unmittelbar nach der Änderung im SAP vorhanden sein. Angelehnt an den BSI-Grundschutz ist der Schutzbedarf der DIP bzgl. Informationssicherheit (über das Maximum) insgesamt als hoch zu bewerten.

4.3 Einbindung in die IT-Systemlandschaft

Der Server mit der Data Integration Platform ist über ein dediziertes Netzwerksegment mit dem LUH-Netz verbunden. Es ist nur eine unidirektionale Verbindung von SAP-PI zur Data Integration Platform und unidirektionale Verbindungen von der Data Integration Platform zu den Zielsystemen zugelassen. Das Netzwerksegment ist vom LUH-Netz durch eine Hardware-Firewall, die mit einer Whitelisting-Policy inklusive starker Restriktion ausgehenden Datenverkehrs betrieben wird, abgetrennt. Der Datenbankserver ist von außerhalb dieser Segmente nicht erreichbar. Der Remote-Zugang per SSH auf den Server ist nur mit einem persönlichen Benutzeraccount (kein anonymer root-Zugriff) und nur von berechtigten Systemen aus möglich. Nur die für den Betrieb des DIP zuständigen Administratoren (Fachteam IdM) haben zur Wartung und zur Fehleranalyse Zugriff auf den DIP- Server und auf die DIP-Datenbank. Die Datenbank der Data Integration Platform ist durch einen gesonderten Zugang (Nutzername, Passwort) vor unberechtigten Zugriffen geschützt. Die Betriebssystem-Software der Data Integration Platform erhält zeitnah die bereitgestellten Updates von LUH-internen Servern. Die Funktionsbereitschaft und die Betriebsparameter der zentralen DIP-Dienste werden ständig durch in den LUIS betriebene Monitoring-Dienste überwacht.

4.4 Graphische Darstellung der IT-Systemlandschaft

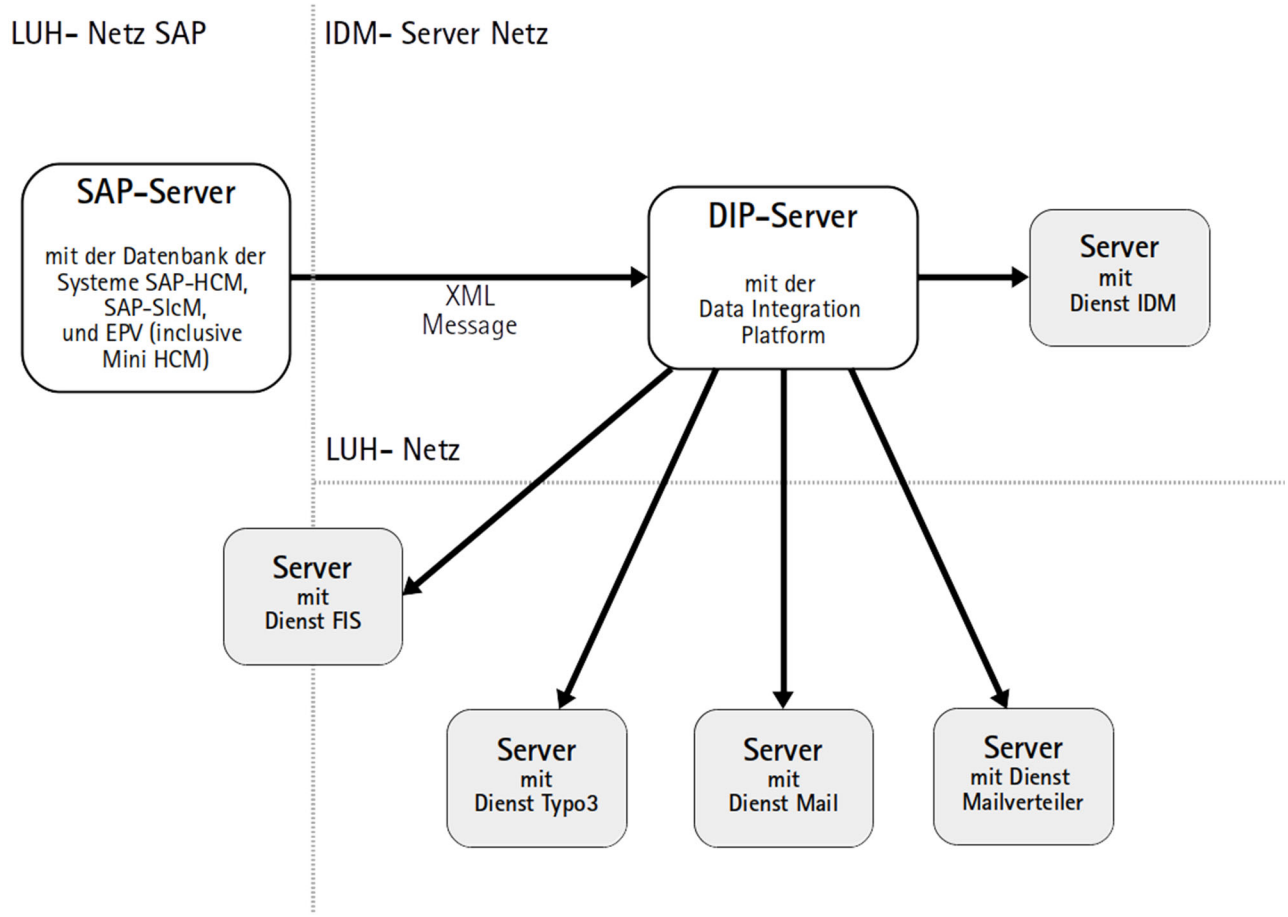


Abbildung 2: Zugriffe auf die Server der Data Integration Platform

4.5 Kommunikation

Die zu importierenden Nutzerdaten werden über einen verschlüsselten Kanal vom SAP-System zur Data Integration Platform übertragen (TLS-Verschlüsselung mit Zertifikatsprüfung) und von der DIP zu den Servern der Zielsysteme ebenfalls verschlüsselt übertragen (TLS-gesichert oder via SSH mit Prüfung des Serverzertifikats bzw. -schlüssels). Die Zugriffe von oder auf die DIP werden soweit technisch möglich mit Client-Zertifikaten oder -Schlüsseln gesichert, mindestens mit einem komplexen Passwort.

4.6 Backup

Es werden nächtlich Backups des gesamten Datenbestands hergestellt und mit Hilfe des zentralen Backup-Dienstes des Rechenzentrums in gestufter Weise aufbewahrt (täglich inkrementell, wöchentliches Vollbackup). Die Vorhaltezeit beträgt mindestens 4 und maximal 8 Wochen.

Zusätzlich werden die gesamten Server-Installationen nächtlich gesichert, dies dient der schnellen Wiederherstellung im Notfall, z.B. bei Hardware-Schäden (Disaster Recovery). **Anlage 4**

4.7 Logging

4.7.1. Systemlogdateien

Die Protokollierung der Aktionen in Logdateien dient der Integrität der Datenverarbeitungssysteme. Sie erleichtert die Suche nach Fehlfunktionen und trägt dazu bei, unberechtigte Zugriffe aufzudecken. Folgende Teilkomponenten der Data Integration Platform erstellen Logdateien:

- Betriebssystem (Linux)
- Webserver (Apache)
- Applikationsserver (Tomcat)
- Anwendungen (Python und Java)

Die Logdateien werden täglich gepackt und nach einer vorgegebenen Zeit automatisch gelöscht. Die Logdateien dienen der Umsetzung technisch-organisatorischer Schutzmaßnahmen nach NDSG §7 und unterliegen insbesondere NDSG §10 Abs.4. Da über die DIP ggf. auch mittelbar Zugriff auf personenbezogene Daten möglich ist und geschützt werden muss, wird eine maximale Speicherdauer von 30 Tagen festgelegt.

4.7.2. Schnittstellenlogdateien

Logdaten der Schnittstellen (von den Quellsystemen und zu den Zielsystemen) werden aus Gründen der Nachweisbarkeit für 90 Tage gespeichert. Fehler in den Quell- oder Zielsystemen fallen evtl. erst spät auf. Die DIP als Schnittstellenplattform muss hier die Möglichkeit aufweisen Fehlkonfigurationen oder falsche Datenlieferungen zu ermitteln und zu belegen.

4.8 Löschfristen

Stammdaten der Personen nach Ausscheiden:

- Reduktion auf ID, Name, Geburtsdatum/-ort nach 1 Jahr
- Komplett-Löschung nach 2 Jahren

Die Löschfristen entsprechen den Fristen im IDM. In der DIP werden die Daten für eine mögliche Deduplikation und Reaktivierung von Identitäten benötigt. Personen, die innerhalb von 2 Jahren wieder zurück an die LUH kommen (z.B. Studienabschluss und spätere Beschäftigung, befristete Arbeitsverträge mit Lücken, Lehrtätigkeiten mit längeren Pausen) sollen die selbe LUH-ID erhalten.

Weiterhin kann es im Fehlerfall passieren, dass eine Nachricht aus den Quellsystemen (z.B. Vertragsverlängerung oder Rückmeldung) nicht in der DIP ankommt. Dies fällt häufig erst sehr spät, z.B. bei der semesterweisen Validierung der LeibnizCard auf. Durch die längere Speicherung der Daten in der DIP kann hier ein schnellerer Support und eine Recherche der Fehlersituation erfolgen.

4.9 Maßnahmen Datenschutz

Zugangskontrolle
Die Datenverarbeitungsanlagen (Server inklusive Storage) stehen im Maschinensaal des Rechenzentrums der Universität. Die Zugänge zu diesem Maschinensaal sind auf Mitarbeiter im Rechenzentrum und temporär auf Wartungspersonal im Bedarfsfall beschränkt. Die Zugänge werden über eine elektronische Schließanlage kontrolliert und sind bei Missbrauch auditierbar[1]. Das Gebäude ist alarmgesichert und rund um die Uhr durch Mitarbeiter bzw. anwesenden Wachschutz überwacht. Ein Zugang zum DIP-System selbst ist zudem durch das Logging des Systems und das Monitoring überwacht.

[1] Geregelt in der Dienstvereinbarung über die Nutzung von elektronischen Schließanlagen und Zugangskontrollsystemen, vgl. Verkündungsblatt der Universität Hannover 2/2001 S.24

Das Backup-System ist analog am zweiten Standort (HLRN-Halle) geschützt.

Datenträgerkontrolle
Im DIP-System und im Backup kommen nur fest verbaute Festplatten zum Einsatz. Die Entsorgung erfolgt nach Löschung oder (bei Defekt) über zertifizierte Entsorger.

Speicherkontrolle
Ein direkter Zugriff auf die Speicher ist nur für Systemadministratoren möglich. Die Systemadministratoren müssen sich aber zuvor am System authentifizieren und ein Zugang ist nur aus dem Mitarbeiternetz des Rechenzentrums bzw. durch direkten Zugang möglich. Die DIP-Systemadministratoren sind wenige Beschäftigte des LUIS und auf den Datenschutz sowie diese Dienstvereinbarung verpflichtet.

Übermittlungskontrolle
Die über Schnittstellen im- und exportierten Daten werden protokolliert.

Eingabekontrolle
Importe, die zu Datenveränderungen führen, werden von der DIP protokolliert. Die Data Integration Platform (DIP) wird automatisiert betrieben.

Verfügbarkeitskontrolle
Die Daten der DIP sind Replikationen der Daten der führenden Systeme und daher jederzeit reproduzierbar. Die Daten der DIP werden für eine schnelle Wiederherstellbarkeit nach einem stufigen Backup-Konzept mit Auslagerung an einen anderen Standort gesichert (vgl. Abschnitt 4.6 oben).

Auftragskontrolle
Eine Datenverarbeitung im Auftrag findet nicht statt.

Transportkontrolle
Alle Datenübertragungen zum und vom DIP-System bzgl. angebundener Quell- und Zielsysteme finden mittels TLS oder SSH verschlüsselt statt. Dabei wird zur Authentifizierung nach Stand der Technik auf Zertifikate bzw. Schlüssel gesetzt, Passwörter kommen nur in technisch bedingten Ausnahmefällen und dann komplex und lang zum Einsatz. Dieses schließt die Kommunikation mit dem Backup-System ein.

Organisationskontrolle
Die Mitarbeiter des Rechenzentrums sind auf den Datenschutz verpflichtet, die DIP-Administratoren zusätzlich auf diese Dienstvereinbarung. Zur DIP existiert eine Verfahrensmeldung. Die Leibniz Universität Hannover hat einen betrieblichen Datenschutzbeauftragten bestellt.

4.10. Auswertungen

4.10.1 Einzelfallbezogene Zugriffe bei Supportanfragen

Bei Supportanfragen findet im Einzelfall ein lesender Zugriff auf die Stammdaten statt, um Fehler in der DIP auszuschließen.

4.10.2 Auswertung zur Sicherstellung des ordnungsgemäßen Betriebes

Grundsätzlich können über die SQL-Kommandos der Datenbank Auswertungen jeglicher Art ausgeführt werden. Die Datenbank ist aber nur für die Administratoren der Data Integration Platform zugänglich und Auswertungen werden nur zur Fehleranalyse und Fehlerkorrektur der DIP-Anwendungen durchgeführt. Die Auswertungen werden nicht gespeichert und nur im Dialogverfahren angezeigt. Nach Beendigung der Sitzung sind die Daten wieder gelöscht. Die Ergebnisse dieser Auswertungen unterliegen einer strengen Zweckbindung gemäß § 6 Abs. 4 NDSG. Andere Auswertungen sind nur nach der Mitbestimmung durch den Personalrat und Prüfung der datenschutzrechtlichen Vorgaben zulässig.