Vereinbarung

nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG)

über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens

Ausbildungsmanagement-System (AMS)

Zwischen

der Freien und Hansestadt Hamburg - vertreten durch den Senat -

- Personalamt

einerseits

und

dem dbb hamburg

- beamtenbund und tarifunion -

sowie

dem Deutschen Gewerkschaftsbund

- Bezirk Nord -

als Spitzenorganisationen der Gewerkschaften und Berufsverbände

des öffentlichen Dienstes

andererseits

wird Folgendes vereinbart:

Präambel

Der Senat der Freien und Hansestadt Hamburg (FHH) verfolgt im Rahmen seiner Digitalstrategie für Hamburg u. a. das Ziel der digitalen Verwaltung. Diese umfasst nicht nur die Interaktion mit den Bürgerinnen und Bürgern der FHH, sondern auch die Arbeitserleichterung und Optimierung interner Arbeitsprozesse durch digitale Verfahren in den Behörden und Ämtern.

Mit ihrer gemeinsamen Digitalstrategie unter dem Motto "Wir machen die Personalarbeit der FHH digital" fokussieren sich das Personalamt, der Landesbetrieb (LB) ZAF/AMD und der LB ZPD in diesem Kontext auf die Digitalisierung im Bereich Personal.

Als Organisationseinheit des Personalamtes richtet der LB ZAF/AMD in seiner Rolle als zentraler Dienstleister in der Ausbildung seinen Fokus insbesondere auf Nachwuchskräfte und ihre Ausbildung, zu deren Optimierung und Digitalisierung in den Bereichen Ausbildungsplanung, -organisation und -durchführung es einer einheitlichen IT-Lösung bedarf.

Über das zentrale Ausbildungsmanagement-System (AMS) sollen die vom Personalamt angebotenen Ausbildungen und Berufsvorbereitung gesteuert und ein digitalisierter, standardisierter sowie optimierter Austausch zwischen den Nachwuchskräften und den Ausbildungsbeteiligten ermöglicht werden.

Das AMS unterstützt bei der Organisation und Ablaufplanung der berufspraktischen Ausbildungsphasen und versorgt die an der Ausbildung beteiligten Akteure mit relevanten Informationen.

Nr. 1

Gegenstand der Vereinbarung

Gegenstand der Vereinbarung sind die Einführung, der Betrieb, die Nutzung und die Weiterentwicklung des neuen IT-Verfahrens das Modul Magellan Young Talents des Softwareherstellers GuideCom als Ausbildungsmanagement-System.

Zweck und Ziel des IT-Verfahrens sind in der Anlage 1 - Beschreibung der Verarbeitungstätigkeit - näher beschrieben.

Das AMS bildet die Inhalte, Lernziele, Planung, Organisation und Durchführung der Ausbildung ab.*

Explizit nicht Gegenstand des AMS und dieser Vereinbarung sind die Durchführung von Bewerbungsverfahren, die Personalaktenverwaltung sowie das Urlaubs- und Fehlzeitenmanagement.* Die Funktionalitäten, die im AMS eingesetzt werden, sind in der Anlage 2 - Funktionsübersicht - aufgeführt.*

Die Anlagen sind Bestandteil der vorliegenden Vereinbarung.*

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

Nr. 2

Geltungsbereich

Die Vereinbarung gilt für alle Verwaltungseinheiten der FHH, für die der Senat oberste Dienstbehörde ist und die gleichzeitig an den im AMS verwalteten und vom Personalamt angebotenen Ausbildungen und Berufsvorbereitungen beteiligt sind.

Die konkreten Ausbildungen und Berufsvorbereitungen ergeben sich aus der Anlage 3.

Nr. 3

Ergonomie und Arbeitsplatzgestaltung

Die Gestaltung der ergonomischen Eigenschaften des IT-Verfahrens und der betroffenen Arbeitsplätze richtet sich nach den einschlägigen gesetzlichen Bestimmungen und orientiert sich an den Grundsätzen der DIN EN ISO 9241, insbesondere den Teilen -11 (Anforderung an die Gebrauchstauglichkeit) und -110 (Grundsätze der Dialoggestaltung).

Die schutzwürdigen Belange besonderer Beschäftigtengruppen (z.B. Menschen mit Behinderung) werden bei der Arbeitsplatzgestaltung berücksichtigt (z.B. Einrichtung mit Zusatzsoftware wie Bildschirmausleseprogramm, -vergrößerungsprogramm o.ä.), so dass ein barrierefreies Arbeiten möglich ist.

Dataport wurde mit der Prüfung und Ausstellung eines entsprechenden Testats der Barrierefreiheit auf Basis der Barrierefreie-Informationstechnik-Verordnung (BITV 2.0) mit der Europäischen Norm (EN) 301 549 – Version 3.2.1 (2021-03) sowie der Prüfung der Softwareergonomie beauftragt. Die sich aus den Prüfberichten ergebenden Änderungs-/Anpassungsbedarfe wurden mit dem Hersteller besprochen. Die Planung zur Umsetzung dieser Bedarfe ist in Anlage 7 - Umsetzungsplanung - aufgeführt.

Die betroffenen Arbeitsplätze sind mit Endgeräten ausgestattet, die der Fachaufgabe angemessen sind und dem Stand der Technik entsprechen.

Soweit sich aus einer Anwendung neue technische Anforderungen ergeben, wird eine Anpassung vorgenommen. Die Freie und Hansestadt Hamburg als Arbeitgeberin, vertreten durch die jeweils zuständige Behörde bzw. Dienststelle, wird dabei die sich aus den §§ 3-14 Arbeitsschutzgesetz und Anlage 6 der Verordnung über Arbeitsstätten ergebenden Pflichten erfüllen[1].

[1] Näheres regelt die Vereinbarung zu der Vereinbarung nach § 94 HmbPersVG zur betrieblichen Gesundheitsförderung in der hamburgischen Verwaltung hier: Regelung zur Gefährdungsbeurteilung der physischen und psychischen Belastungen am Arbeitsplatz.

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

Nr. 4

Arbeitsplatz- und Einkommenssicherung

Die Einführung und der laufende Betrieb des neuen IT-Verfahrens werden nicht zu Kündigung oder Änderungskündigung von Arbeitsverhältnissen mit dem Ziel der tariflichen Herabgruppierung führen. Bei notwendigen Versetzungen oder Umsetzungen werden vorrangig gleichwertige Arbeitsplätze bzw. Dienstposten angeboten, sofern im bisherigen Tätigkeitsbereich eine gleichwertige Tätigkeit nicht weiter möglich ist.

Bei Versetzungen oder Umsetzungen werden alle Umstände angemessen berücksichtigt, die sich aus der Vor- und Ausbildung, der seitherigen Beschäftigung und persönlicher und sozialer Verhältnisse der bzw. des Betroffenen ergeben.

Gleiches gilt, wenn notwendige personelle Maßnahmen im Einzelfall unvermeidlich sein sollten, weil Beschäftigte auch nach den erforderlichen Fortbildungs- oder Schulungsmaßnahmen den sich aus dem neuen Verfahren ergebenden Anforderungen nicht entsprechen. Auch in diesen Fällen finden betriebsbedingte Kündigungen oder Änderungskündigungen mit dem Ziel der tariflichen Herabgruppierung nicht statt.

Die Arbeitsplatz- und Einkommenssicherung für die Tarifbeschäftigten richtet sich ferner nach dem Tarifvertrag über den Rationalisierungsschutz für Angestellte vom 09.01.1987.

Soweit sich aus dem Beamtenrecht nichts anderes ergibt, gilt die Vereinbarung nach § 94 HmbPersVG über den Rationalisierungsschutz für Beamte vom 09.05.1989.

Auf die Belange der Kolleginnen und Kollegen mit Behinderung wird besonders Rücksicht genommen.

Nr. 5*

Datenschutz Nachwuchskräfte, Ausbilderinnen und Ausbilder

Das AMS unterstützt bei der Planung, Organisation, Durchführung und Steuerung der berufspraktischen Ausbildungsphasen. Bestandteil hiervon ist die Personal(einsatz)planung i.S.d. §§ 85ff. HmbBG i.V.m. § 10 HmbDSG während der Ausbildung. Dabei werden zu den Ausbildungsabschnitten Daten der Nachwuchskräfte sowie der Ausbilderinnen und Ausbilder erhoben, die in ihrer Gesamtheit zugleich den Verlauf der Ausbildung dokumentieren.

Die Rechte der Nachwuchskräfte sowie der Ausbilderinnen und Ausbilder in Bezug auf die Personalaktendaten und die Grundsätze der Personalaktenführung bleiben durch die Einführung des AMS unberührt. Die Grundsätze der Transparenz, der Richtigkeit, der Zulässigkeit und der Vertraulichkeit werden gewährleistet. Die Daten der Nachwuchskräfte sowie der Ausbilderinnen und Ausbilder sind datenschutzkonform zu verarbeiten und vor unzulässigen Verhaltens- und Leistungskontrollen zu schützen. Der Schutz der Daten der Nachwuchskräfte sowie der Ausbilderinnen und Ausbilder vor unbefugter Einsichtnahme, vor Löschung und vor Veränderung ist durch technische Maßnahmen entsprechend dem jeweiligen Stand der Technik zu gewährleisten.

Eine abschließende Liste der verarbeiteten Datenfelder ergibt sich aus der Anlage 1 Ziffer 3.2.

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

Nr. 6*

Schutz der Anwenderinnen und Anwender vor Leistungs- und Verhaltenskontrolle*

Anwenderinnen und Anwender in Bezug auf das AMS sind folgende Personen- bzw. Funktionsgruppen in Bezug auf die vom Personalamt angebotene Ausbildung:*

- Nachwuchskräfte
- Ausbilderinnen und Ausbilder sowie Koordinatoren
- Je nach Berufsbild zuständige Ausbildungsleitungen
- Beschäftigte, die Aufgaben in der Personalbetreuung übernehmen
- Beschäftigte, die Aufgaben in der Ausbildungssteuerung übernehmen
- Beschäftigte im Praxisbüro (Fachrichtung Soziale Arbeit)
- Beschäftigte der Fachlichen Leitstelle

Hinsichtlich der Daten der Anwenderinnen und Anwender gilt das Folgende:

- Es werden nur diejenigen personenbezogenen Daten verarbeitet (hierunter fallen auch Auswertungen, vgl. Artikel 4, Ziffer 1 und 2 Verordnung (EU) 2016/679, DSGVO), die für die Erledigung der Fachaufgabe erforderlich sind. Diese Daten sind in der Anlage 1 Ziffer 3.2 aufgeführt.
- Im Rahmen des Ausbildungsmanagements werden vorhandene Daten, wie z.B. Beurteilungen, auch dazu genutzt, die Anwendung von Beurteilungsmaßstäben zu vergleichen und zu thematisieren. Zudem werden im Rahmen der Ausbildungsziele Daten der Nachwuchskräfte zur Leistungsdokumentation verarbeitet. Die personenbezogenen Daten werden gemäß der Vereinbarung nach § 94 HmbPersVG über den Prozess zur Einführung und Nutzung allgemeiner automatisierter Bürofunktionen und multimedialer Technik und zur Entwicklung von E-Government vom 10.09.2001 nicht zu einer darüber hinausgehenden Leistungs- und Verhaltenskontrolle der Anwenderinnen und Anwender genutzt. Dies gilt sowohl unmittelbar über das IT-Verfahren als auch mittelbar über andere IT-Verfahren.
- Die im Zusammenhang mit diesem Verfahren verarbeiteten personenbezogenen Daten der Anwenderinnen und Anwender dürfen grundsätzlich nicht zur Begründung dienst- und/oder arbeitsrechtlicher Maßnahmen verwendet werden. Ausnahmsweise ist dies bei einem (auch zufällig entstandenen) konkreten Verdacht zur Aufklärung von Missbrauchstatbeständen (Dienstvergehen, Verletzung arbeitsvertraglicher Pflichten oder strafbare Handlungen) zulässig. Der auslösende Sachverhalt ist zu dokumentieren. Der zuständige Personalrat ist möglichst[2] vorher zu unterrichten. Die bzw. der betroffene Beschäftigte ist zu unterrichten, sobald dies ohne Gefährdung des Aufklärungsziels möglich ist. Daten, die ausschließlich zum Zwecke der Aufklärung erhoben wurden, sind zu löschen, sobald der Verdacht ausgeräumt ist oder sie für Zwecke der Rechtsverfolgung nicht mehr benötigt werden.
- Die Erteilung von Berechtigungen erfolgt auf der Grundlage eines Berechtigungs- und Rollenkonzepts, in dem die für die verschiedenen Funktionen/Mitarbeitergruppen erforderliche

[2] Von der vorherigen Information des Personalrats darf nur abgewichen werden, wenn andernfalls das Ziel der Auswertung nicht erreicht werden kann. Gründe dafür können sich im Einzelfall ergeben, z.B. bei Gefahr im Verzuge oder einer Gefährdung des Ermittlungszwecks. Erfolgt die Unterrichtung des Personalrats erst nachträglich, sind ihm die dafür maßgeblichen Gründe zu benennen.

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

Berechtigungen festgelegt werden um mandantenspezifische (d. h. separat für jede Organisationsstruktur geltende) Berechtigungsstrukturen abzubilden. Das Rechte- und Rollenkonzept wird in der Anlage 4 näher beschrieben.

- Die Sicherstellung einer revisionssicheren Protokollierung wird im Protokollierungskonzept - Anlage 5 - näher beschrieben. Zudem wird die bei Dataport genutzte Infrastruktur beschrieben.*

Nr. 7*

Qualifizierung der Anwenderinnen und Anwender

Mit der Einführung dieses Verfahrens ändern sich die Arbeitsbedingungen der Anwenderinnen und Anwender, die dafür erforderlichen Qualifizierungsmaßnahmen verfolgen das Ziel, die Anwenderinnen und Anwender entsprechend ihrer Rolle zu einer selbstständigen und sicheren Erledigung ihrer fachlichen neuen Aufgaben zu befähigen. Diese Qualifizierungsmaßnahme soll zeitnah und vor Einführung des IT-Verfahrens erfolgen. Nach ca. 4 – 6 Monaten Arbeit mit dem IT-Verfahren wird den Anwenderinnen und Anwendern Gelegenheit gegeben, durch eine Ergänzungsqualifizierung selbst empfundene Defizite aufzuarbeiten. Für die Qualifizierungsmaßnahmen trägt die zuständige Behörde oder Dienststelle in Verbindung mit der fachlich zuständigen Stelle die Verantwortung.

Bei der Entwicklung des Qualifizierungskonzepts wird geprüft, ob bei mittelbar von dem IT-Verfahren betroffenen Beschäftigten ein Qualifizierungsbedarf besteht. Die Einzelheiten werden in einem - Qualifizierungskonzept - dargestellt, das als Anlage 6 beigefügt ist.

Den Anwenderinnen und Anwendern werden Hilfen zum Umgang mit dem IT-Verfahren bereitgestellt, die sich über das IT-Verfahren selbst und an zentraler Stelle (z.B. im FHHportal) aufrufen lassen. Es wird außerdem gewährleistet, dass für alle Anwenderinnen und Anwender im Falle auftretender Probleme eine versierte Ansprechstelle zur Verfügung steht.

Es wird gewährleistet, dass auch Menschen mit Behinderung qualifiziert werden können, ggf. werden individuell angepasste Qualifizierungsmaßnahmen entwickelt.

Die Spitzenorganisationen und die Personalräte erhalten Gelegenheit an den Qualifizierungsmaßnahmen teilzunehmen.

Nr. 8

Organisation und Ablauf

Die Einführung des neuen IT-Verfahrens bedeutet für die Anwenderinnen und Anwender, dass die bisherigen Arbeitsweisen sich verändern. Sie setzt daher sorgfältig organisierte und durchgeführte Einführungsprozesse voraus. Die Einführung des IT-Verfahrens in den Behörden und/oder Dienststellen wird in zeitlicher und organisatorischer Hinsicht als Meilenstein- oder Roll-Out-Planung beschrieben. Sie erfolgt grundsätzlich im Rahmen der bestehenden Organisation der Dienststelle. Bei Bedarf können auch andere Umsetzungsstrukturen gewählt werden.

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

Auf dieser Basis sollen repräsentative Anwenderinnen und Anwender sowie die örtlichen Personalräte und die Spitzenorganisationen der Gewerkschaften und Berufsverbände die Möglichkeit erhalten, das zukünftige IT-Verfahren frühzeitig kennen zu lernen und in Bezug auf zentrale funktionelle Anforderungen qualitätssichernde Hinweise zu geben.

Den örtlichen Personalräten wird Gelegenheit gegeben, an der Umsetzung teilzunehmen.

Sollte es bei der Einführung des Verfahrens zu nicht auflösbaren Konflikten in einer Behörde oder Dienststelle kommen, werden sich die Verhandlungspartner dieser Vereinbarung um eine einvernehmliche Lösung bemühen.

Nr. 9

Evaluation des Betriebs unter Beteiligung der Spitzenorganisationen

Drei Jahre nach Inkrafttreten der Vereinbarung wird durch die fachlich zuständige Stelle eine Evaluation durchgeführt.

Die Evaluation umfasst insbesondere die Gestaltung

- der Arbeitsprozesse (z.B. Unterstützung der Aufgabenerledigung durch das Verfahren),
- der Dialogoberfläche (logischer Bildschirmaufbau),
- die Hardware-Ausstattung (z.B. Angemessenheit der Monitorgröße) sowie
- die Realisierung der Umsetzungsplanung (Anlage 7).

Soweit möglich werden bei der Evaluation alle Entwicklungsziele zu fachlichen Belangen, Datenschutz, Anwendungstauglichkeit (Gebrauchstauglichkeit) und Qualifizierungsmaßnahmen berücksichtigt. Die Einzelheiten des Evaluationsverfahrens werden mit den Spitzenorganisationen der Gewerkschaften beraten. Die Anmerkungen werden bei der Durchführung berücksichtigt.

Die Erhebung erfolgt anonymisiert auf elektronischem Wege. Zur Konkretisierung der Ergebnisse können in begrenzter Zahl Gespräche mit Mitarbeiterinnen und Mitarbeitern bzw. Anwender-Workshops stattfinden.

Das Ergebnis wird den Spitzenorganisationen der Gewerkschaften vorgestellt und mit Ihnen erörtert.

Nr. 10

Verfahren bei Änderungen

Das in Nr. 1 beschriebene Verfahren wird bei Bedarf weiterentwickelt.

Vor wesentlichen Änderungen des Verfahrens sowie erforderlicher Anpassungen der Anlagen, z. B. des Berechtigungs-, Rollen und Löschkonzepts, welche einen eigenständigen inhaltlichen Gehalt haben, informiert die für das Fachverfahren verantwortliche Behörde bzw. Dienststelle

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

in Abstimmung mit der für die Verhandlungsführung zuständigen Stelle die Spitzenorganisationen der Gewerkschaften so rechtzeitig, dass sie noch Einfluss auf die Änderungen nehmen können.

Die Spitzenorganisationen der Gewerkschaften erhalten die Gelegenheit, sich binnen 4 Wochen nach Zugang der Information zu der wesentlichen Änderung zu äußern. Wenn sich keine der Spitzenorganisationen der Gewerkschaften zu der Änderung innerhalb dieser Frist äußert, gilt die Zustimmung als erteilt. Andernfalls nehmen die Beteiligten Verhandlungen auf.

Nr. 11

Schlussbestimmungen

Soweit durch die Vereinbarung örtliche Mitbestimmungstatbestände nicht geregelt werden, bleibt die Mitbestimmung der örtlichen Personalvertretung bzw. des Nachwuchspersonalrates unberührt.

Die Vereinbarung tritt mit sofortiger Wirkung in Kraft.

Sie kann mit einer Frist von sechs Monaten zum Ende eines Jahres gekündigt werden. Bei Kündigung wirkt die Vereinbarung bis zum Abschluss einer neuen Vereinbarung nach. In diesem Fall werden die Partner der Vereinbarung unverzüglich Verhandlungen über den Abschluss einer neuen Vereinbarung aufnehmen.

Hamburg, den 06.02.2023

Freie und Hansestadt Hamburg für den Senat gez. Volker Wiedemann

dbb hamburg beamtenbund und tarifunion gez. Rudolf Klüver

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

Deutscher Gewerkschaftsbund

-Bezirk Nord-

gez.

Olaf Schwede

Anlagen:

1. Beschreibung der Verarbeitungstätigkeit
2. Funktionsübersicht AMS
3. Übersicht über die Ausbildungen und Berufsvorbereitungen
4. Berechtigungs-, Rollen- und Löschkonzept
5. Protokollierungs- und Infrastrukturkonzept
6. Qualifizierungskonzept
7. Umsetzungsplanung Barrierefreiheit / Softwareergonomie

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

.

Hamburg

Beschreibung der Verarbeitungstätigkeit

(Bitte an die Verzeichnisführende Stelle absenden!)

Blatt-Nr.:

Von der Verzeichnisführenden Stelle auszufüllen!

Nur auszufüllen, wenn personenbezogene Daten[1] verarbeitet werden!

Anmerkung: Soweit der Platz dieses Formulars nicht ausreicht fügen Sie bitte zusätzliche Anlagen bei!

Allgemeines			
	Datum:	15.06.2022	
	Ausfüllende Person:	Susan Wilhelmi	
	Telefonnummer:	+49 40 428 31-2457	
	Bezeichnung des Verfahrens:	Digitales Ausbildungsmanagement – GuideCom Magellan Young Talents	
	Bezeichnung der Verarbeitung[2]:	☒ Erheben ☒ Erfassen ☒ Organisieren ☒ Ordnen ☒ Speichern ☒ Anpassen oder Verändern ☒ Auslesen ☒ Abfragen ☒ Verwenden ☒ Offenlegen durch Übermittlung, Verbreitung oder andere Form der Bereitstellung ☐ Abgleichen oder die Verknüpfen ☒ Einschränken ☒ Löschen ☐ Vernichten	
	Beginn der Verarbeitung[3]:	01.05.2022 Betriebsbereitschaft und Testbetrieb des AMS Produktivbetrieb (und damit auch tatsächliche Verarbeitung personenbezogener Daten) nach Vorliegen der abgestimmten §93-Vereinbarung	
	Änderung bestehende Verarbeitung : **Überführung bestehende Verarbeitung in geltende Rechtslage nach DS-GVO:**	☐ ja ☐ ja	
	Neue Verarbeitung:	☒ ja	
	Abmeldung bestehende Verarbeitung[4]:	☐ ja	

[1] Hinweis Nr. 1 der Anlage 1
[2] Hinweis Nr. 2 der Anlage 1
[3] Hinweis Nr. 3 der Anlage 1
[4] Hinweis Nr. 4 der Anlage 1

1. Grundsätzliche Angaben zur Verantwortlichkeit			
1.1	Verantwortliche Organisationseinheit[5] (optional):	Landesbetrieb ZAF/AMD Geschäftsführung Julia Sprei (GF)	
1.2	Vertreter der verantwortlichen Organisationseinheit (optional):	Michael Jenke (BS – Betriebliche Steuerung)	
1.3	Fachliche Leitstelle (bei IT-Verfahren) bzw. zuständige Stelle (bei nicht automatisierten Verfahren): Verantwortliche Führungskraft: Leitzeichen:	Markus Koops (ZAF 10ko), Lara Holtz (ZAF 10ho), Michel Steffens (ZAF 10st) Irmgard Mummenthey ZAF 1	
1.4	Ansprechpartner, sofern nicht verantwortliche Führungskraft: Telefonnummer:	Fachliche Leitstelle - Markus Koops +49 40 428 31-2442	
1.5	Name des Datenschutzbeauftragten (optional):	Dr. Christian Eggeling	
1.6	Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt[6]: Auftragsnummer:	Dataport AöR (Rechenzentrumsbetreiber) V17669/2140000 für den eHdB	

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung[7]			
2.1	Beschreibung und Zweckbestimmung der Verarbeitung von Daten[8]	Beschreibung der Verarbeitung: Das Verfahren „Digitales Ausbildungsmanagement“ dient der digitalen Abbildung des Ausbildungsmanagements der Freien und Hansestadt Hamburg in Bezug auf die vom Personalamt angebotenen Ausbildungen[9]. Hierfür kommt die Software „Magellan Young Talents“ des Softwareherstellers GuideCom zum Einsatz. Das Ausbildungsmanagement umfasst folgende Verarbeitungsbereiche: <u>Datenerfassung</u> Die Nachwuchskräfte[10] werden zu Beginn die Ausbildung im Verfahren erfasst und ihrer Klasse oder Studiengruppe zugeordnet. Dabei werden nur die zwingend erforderlichen Daten (siehe 3.2) erfasst. Die Führung der Personalakten der Nachwuchskräfte wird ausdrücklich nicht über dieses Verfahren abgelöst und sämtliche personalaktenrelevante Dokumente werden auch weiterhin außerhalb dieses Verfahrens verarbeitet. Den Nachwuchskräften	

[5] Hinweis Nr. 5 der Anlage 1

[6] Hinweis Nr. 6 der Anlage 1

[7] Hinweis Nr. 7 der Anlage 1

[8] Hinweis Nr. 8 der Anlage 1

[9] Der Begriff „Ausbildung“ umfasst sämtliche Ausbildungsgänge, duale Studiengänge und Vorbereitungsdienste

[10] Nachwuchskräfte im Sinne der unter 2.2. genannten §93er-Vereinbarung sind Personen, die sich beim Personalamt als Beamtinnen, Beamte, Arbeitnehmerinnen und Arbeitnehmer in einem Vorbereitungsdienst und/oder einem öffentlich-rechtlichen Ausbildungsverhältnis für die Laufbahngruppe 1 und die Laufbahngruppe 2 befinden oder eine zu diesen Laufbahngruppen und Einstiegsämtern vergleichbare Ausbildung durchlaufen

		steht es allerdings frei, ihre Daten im Verfahren selbst zu vervollständigen / ergänzen. Die Durchführung des Bewerbungsverfahrens sowie das Urlaubs- und Fehlzeitenmanagement erfolgen ebenfalls nicht über das Ausbildungsmanagementsystem. Folgende Personengruppen werden darüber hinaus im System angelegt: - Ausbilderinnen und Ausbilder sowie Koordinatoren - Je nach Berufsbild zuständige Ausbildungsleitungen - Beschäftigte, die Aufgaben in der Personalbetreuung übernehmen - Beschäftigte, die Aufgaben in der Ausbildungssteuerung übernehmen - Beschäftigte im Praxisbüro (Fachrichtung Soziale Arbeit) - Beschäftigte der Fachlichen Leitstelle Die Daten werden i.d.R. aus dem Active Directory im Rahmen eines Reports übernommen. <u>Organisation und Planung der berufspraktischen Ausbildungsphasen</u> Über die Funktion der Verteilungsplanung ist es möglich, manuell oder automatisiert die Nachwuchskräfte auf die freien Praxisstellen zu verteilen und für jede Nachwuchskraft einen Plan über die berufspraktischen Abschnitte der gesamten Ausbildungszeit zu generieren. Die Verteilungsplanung kann dabei über Verteilungskriterien und ein Prioritätensystem konfiguriert werden. <u>Beurteilungswesen und Evaluation</u> Das Verfahren ermöglicht die Abbildung der bisher in Papierform erstellten Beurteilungen, die nach jedem Praxisabschnitt zu erstellen sind. Nach Erstellung der Beurteilungen können diese per integriertem Workflow abgestimmt werden. Die Nachwuchskräfte können dabei lediglich ihre eigene Beurteilung einsehen und die Ausbilderinnen und Ausbilder sowie die Ausbildungsleitungen nur die, der ihnen zugeordneten Nachwuchskräfte (dies gilt auch für alle anderen Funktionen des Verfahrens). Zudem bietet das Verfahren die Möglichkeit für die Nachwuchskräfte, ihren Praxisstellen nach erfolgreichem Abschluss des jeweiligen Praxisabschnitts ein Feedback zu geben.	

		Berichtsheft Über die Berichtsheftfunktion können die Nachwuchskräfte ihre durchgeführten Tätigkeiten in der jeweiligen Praxisstelle dokumentieren. Das Berichtsheft ist nur von der Nachwuchskraft einsehbar und wird per Workflow den Ausbilderinnen und Ausbildern zur Abzeichnung vorgelegt. Dokumentenmanagement und Kommunikation Neben den vorgenannten Funktionen bietet das Verfahren auch ein Dokumentenmanagement sowie Kommunikationsmöglichkeiten. Z.B. Vordrucke oder Checklisten können hochgeladen und mit Zugriffsrechten versehen werden. Lernmaterialien können für alle einsehbar oder beschränkt auf die jeweilige Nachwuchskraft in deren Azubikarte eingestellt werden. Über die Nachrichtenfunktion können aus dem System heraus (einseitig) Einzelpersonen, Klassen und Studiengruppen oder Verteiler kontaktiert werden – die Kommunikation wird im Verfahren abgespeichert.	
2.2	Rechtsgrundlage (Zutreffendes bitte ankreuzen und ggf. erläutern):		
☐	Spezialgesetzliche Regelung außerhalb der DS-GVO	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Klicken Sie hier, um Text einzugeben.	
☐	Einwilligung des Betroffenen (Art. 6 Abs. 1 a DS-GVO):	*Bitte fügen Sie die Einwilligungsklausel und den Einwilligungsmechanismus hier ein* Klicken Sie hier, um Text einzugeben.	
☒	Kollektivvereinbarung (z.B. Vereinbarung gem. HmbPersVG, Tarifvertrag)	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Vereinbarung nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG) über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Ausbildungsmanagementsystem (AMS) – Vereinbarung befindet sich zum unter Allgemeines aufgeführten Datum noch in der Abstimmung	
☐	Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 4 HmbDSG n.F.)	Klicken Sie hier, um Text einzugeben.	

☒	Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§ 10 HmbDSG n.F. und national geregelt im BDSG):	Das Digitale Ausbildungsmanagement dient dem Zweck der Durchführung des Beschäftigungsverhältnisses (hier konkret: Die Ausbildung) und ist zur Organisation der Ausbildungsabläufe sowie zu der Personalplanung und des –einsatzes erforderlich.	
☐	Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b DS-GVO)	Klicken Sie hier, um Text einzugeben.	
☐	Interessenabwägung (Art. 6 Abs. 1 f DS-GVO)	*Bitte benennen Sie die vorrangigen Interessen:* Klicken Sie hier, um Text einzugeben.	
☐	Weitere:	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz*	
3. Beschreibung betroffener Personen- und Datenkategorien			
3.1	Beschreibung der betroffenen Personengruppen[11]:	Beschäftigte: - Nachwuchskräfte der vom Personalamt angebotenen Ausbildungen - Ausbilderinnen und Ausbilder sowie Koordinatoren - Je nach Berufsbild zuständige Ausbildungsleitungen - Beschäftigte, die Aufgaben in der Personalbetreuung übernehmen - Beschäftigte, die Aufgaben in der Ausbildungssteuerung übernehmen - Beschäftigte im Praxisbüro (Fachrichtung Soziale Arbeit) - Beschäftigte der Fachlichen Leitstelle Beschreibung: Von der Verarbeitung betroffen sind in erster Linie die sich in der Ausbildung befindenden Nachwuchskräfte. Die Ausbildungsleitungen und Koordinatoren in den Fachbehörden und Bezirksämtern sowie die Ausbilderinnen und Ausbilder, die an der berufspraktischen Ausbildung beteiligt sind, sind ebenfalls mit ihren dienstlichen Kontaktdaten erfasst.	
3.2	Beschreibung der Art der Daten[12] bzw. Datenkategorien	Identifikations- und Adressdaten Beschreibung: <u>Nachwuchskräfte</u> Identifikations- und Adressdaten (Name, Vorname, Geschlecht, Geburtsdatum und –ort, Staatsangehörigkeit, Familienstand, Telefonnummer, private E-Mail-Adresse (eigeninitiative Angabe), bei Minderjährigkeit Kontaktdaten der gesetzlichen Vertre-	

[11] Hinweis Nr. 9 der Anlage 1
[12] Hinweis Nr. 10 der Anlage 1

		ter); Mitarbeiterdaten (dienstliche Telefonnummer, dienstliche E-Mail-Adresse, HaSi-ID); Vorbildung (Schulform, Schulname, Abgangsklasse); Gesundheitsdaten (eigeninitiative Angabe zu Hilfsmitteln in Hinblick auf die Arbeitsplatzausstattung / örtliche Gegebenheiten des Einsatzortes); Ausbildungsdaten (Ausbildungsgang, Ausbildungszeitraum, Angaben zu den Einsatzorten, AusbilderInnen, Lernziele, Feedback (Kompetenz- und Potentialeinschätzung bzw. Befähigungsberichte), Beruf- oder Hochschulnoten (eigeninitiative Angabe) <u>Ausbildungsleitungen,Koordinatoren, AusbilderInnen</u> Mitarbeiterdaten (Name, Vorname, dienstliche Adresse, Leitzeichen, Funktion, dienstliche Telefonnummer, dienstliche E-Mail-Adresse, HaSi-ID)	
3.3	Werden besondere Kategorien[13] von Daten verarbeitet (Art. 9 Abs. 1 DS-GVO)?	☒ ja, welche? Gesundheitsdaten wie unter 3.2 beschrieben: eigeninitiative Angabe zu Hilfsmitteln in Hinblick auf die Arbeitsplatzausstattung / örtliche Gegebenheiten des Einsatzortes ☐ nein	
4. Datenweitergabe und deren Empfänger[14]			
4.1	Eine Datenübermittlung findet statt oder ist geplant.	☒ ja ☐ nein	
4.2	Interne Empfänger innerhalb der verantwortlichen Stelle	☒ ja ☐ nein	
	Interne Stelle (Organisationseinheit)	ZAF 1 Ausbildung	
	Art der Daten	Alle unter 3.2. genannten Daten können für eine Übermittlung relevant sein	
	Zweck der Daten-Mitteilung	Austausch zwischen Personal-Center und Ausbildungsteuerung	
4.3	Externe Empfänger und Dritte	☒ ja ☐ nein	
	Externe Stelle	Unbestimmt, sämtliche Ausbildungsleitungen und Koordinatoren der FHH, sämtliche Ausbilderinnen und Ausbilder in der FHH	
	Art der Daten	Personenbezogene Daten der zu betreuenden Nachwuchskräfte	
	Zweck der Daten-Mitteilung	Die Ausbildungsleitungen und Koordinatoren sowie die Ausbilderinnen und Ausbilder benötigen die Namen und Kontaktda-	

[13] Hinweis Nr. 11 der Anlage 1
[14] Hinweis Nr. 12 der Anlage 1

		ten der Nachwuchskräfte um die Ausbildung zu planen und die Nachwuchskräfte im Anschluss zu bewerten	
4.4	Geplante Datenübermittlung in Drittstaaten (außerhalb der EU) bzw. internationale Organisation	☐ ja ☒ nein	
	Drittstaat bzw. internationale Organisation	Klicken Sie hier, um Text einzugeben.	
	Art der Daten	Klicken Sie hier, um Text einzugeben.	
	Zweck der Daten Mitteilung	Klicken Sie hier, um Text einzugeben.	
	Welche geeigneten Garantien gem. Art. 46 DS-GVO werden im Zusammenhang mit der Übermittlung gegeben?	Garantien bestehen durch: ☐ verbindliche interne Datenschutzvorschriften, ☐ von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln ☐ von einer Aufsichtsbehörde genehmigte Vertragsklauseln	
	Bei Nichtvorliegen eines Angemessenheitsbeschlusses nach Art. 45 Abs. 3 DS-GVO und geeigneter Garantien nach Art. 46 DS-GVO: Welcher Ausnahmetatbestand nach Art. 49 Abs. 1 DS-GVO wird erfüllt?	Wählen Sie ein Element aus.	
5. Regelfristen für die Löschung der Daten[15]			
	Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Löschungsfristen?	☐ ja, falls ausgewählt bitte benennen: ☒ nein Es existieren noch keine gesetzlichen Vorschriften; im Rahmen der Reformen der Ausbildungs- und Prüfungsordnungen der Laufbahngruppen 1.2 und 2.1 werden Löschungsfristen vereinbart.	
	Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:	Aktuell erfolgt eine Löschung nach fünf Jahren nach Beendigung der Ausbildung. Das Löschkonzept kann der Anlage 2 Berechtigungs-, Rollen- und Löschkonzept entnommen werden.	
6. Mittel der Verarbeitung (optional) Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?[16]			
	Bezeichnung: Hersteller: Funktionsbeschreibung: Bereitstellung:	Magellan Young Talents GuideCom AG Klicken Sie hier, um Text einzugeben. ☐ Eigenentwickelte/ individuelle Software ☒ Standard-Software ☐ Cloud-Services ☐ Sonstige: Klicken Sie hier, um Text einzugeben.	

[15] Hinweis Nr. 13 der Anlage 1
[16] Hinweis Nr. 14 der Anlage 1

7. Zugriffsberechtigte Personengruppen (vereinfachtes Berechtigungskonzept)[17]			
	Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte Berechtigungskonzept:	Siehe Anlage 2 Berechtigungs-, Rollen- und Löschkonzept	
8. Sicherheit der Verarbeitung (Risikoprüfung), Datenschutz-Folgenabschätzung und Technische und organisatorische Maßnahmen[18]			
8.1	Hinsichtlich der Datensicherheitsmaßnahmen wurde der Bereich IT-Sicherheit (z.B. InSiBe der OE) eingebunden?	☒ ja ☐ nein	
8.2	Die allgemeine Zielsetzung aus dem Rahmensicherheitskonzept wurde sichergestellt.	☒ ja ☐ nein, Abweichungen erläutern: Klicken Sie hier, um Text einzugeben.	RaSiKo
8.3	Werden bei der Verarbeitung die Grundsätze des Datenschutzes durch Technikgestaltung (privacy by design) gem. Art 25 Abs. 1 DS-GVO und der datenschutzfreundlichen Voreinstellungen (privacy by default) gem. Art 25 Abs. 2 DS-GVO eingehalten?[19]	☒ ja (ggf. Betriebs-/Herstellerkonzept beifügen) ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
8.4	Es wurden die Schutzbedarfsfeststellung und die Risikoprüfung gem. Art. 32 DS-GVO mittels Datenbank (Tool Schutzbedarfsfeststellung) durchgeführt und die Ergebnisse gem. Nutzungshinweisen ausgedruckt bzw. elektronisch gespeichert. Alternativ wurde analog (auf Papier) gem. der Darstellung aus dem BSI-Standard 200-2 eine Risikoprüfung durchgeführt.	☒ ja ☐ nein Bitte Ergebnis der Risikoprüfung als Anlage beifügen.	Link zur Datenbank bzw. pdf-Format BSI-Standard
8.5	Es wurden die Erforderlichkeitsprüfung („Schwellwertanalyse“) und ggf. die Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO durchgeführt.	☒ ja, Ergebnis der Erforderlichkeitsprüfung („Schwellwertanalyse“) und ggf. die durchgeführte DSFA als Anlage beifügen ☐ nein	Schwellwertanalyse; DSFA
8.6	Bei Verfahren, die bei Dataport gehostet werden: Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMS der FHH sichergestellt (vgl. Anlage 3).	☒ Es liegt ein Verfahren vor, das bei Dataport gehostet wird.	
8.7	Bei Verfahren, die nicht bei Dataport gehostet werden: Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMs laut Anlage 2 sichergestellt.	☐ Es liegt kein Verfahren vor, das bei Dataport gehostet wird. ☐ Die Anlage 2 wurde ausgefüllt und liegt vor.	
8.8	Es liegen schriftlich vor	☐ interne Verhaltensregeln ☒ DSFA	

[17] Hinweis Nr. 15 der Anlage 1
[18] Hinweis Nr. 16 der Anlage 1
[19] Hinweis Nr. 17 der Anlage 1

		☒ Risikoprüfung/ Schutzbedarfsfeststellung ☐ allg. Datensicherheitsbeschreibung ☐ umfassendes Datensicherheitskonzept ☐ Wiederanlauf- bzw. Notfallkonzept ☒ Sonstiges: Anlage 2 Berechtigungs-, Rollen- und Löschkonzept, Anlage 3 Protokollierungs- und Infrastrukturkonzept, Anlage 4 Qualifizierungskonzept	
9. Datenübertragbarkeit[20] (Datenportabilität)			
	Nur bei - auf Grundlage einer Einwilligung- zur Verfügung gestellten Daten: Ist der Export der verarbeiteten Daten an den Betroffenen oder andere Dienste in einem gängigen, standardisierten Format möglich?	☐ ja, Format: Klicken Sie hier, um Text einzugeben. ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
10. Informationen der Betroffenen[21]			
	Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?	Im Rahmen der Einführungsveranstaltung sowie mit Benachrichtigung über Einstellungszusage und im IT-Verfahren selbst	Link zu den Formularen
11. Sonstiges			
	Anmerkungen:	Klicken Sie hier, um Text einzugeben.	

…….. …….. ……
Verantwortlicher Datum Unterschrift

[20] Hinweis Nr. 18 der Anlage 1
[21] Hinweis Nr. 19 der Anlage 1

.

Anlage 1**:**

Hinweise zum Formular

Hinweis Nr. 1
»Personenbezogene Daten« sind nach Art. 4 Nr.1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Dies umfasst z. B. Name, Geburtsdatum, Anschrift, Einkommen, Beruf, Kfz-Kennzeichen, Konto- oder Versicherungsnummer. Auch pseudonymisierte Daten, zum Beispiel eine IP-Adresse oder Personalnummer, aus denen die betroffene Person indirekt bestimmbar wird, gelten als personenbezogene Daten. Die Verarbeitung der personenbezogenen Daten muss im IT-Verfahren der Hauptzweck sein.

Hinweis Nr. 2
Gemeint ist, welche Verarbeitungstätigkeiten durch das Verfahren berührt werden. Folgende Definitionen beschreiben die einzelnen Verarbeitungsschritte:

Erheben	Beschaffen von Daten über eine betroffene Person. Gezielte Verwandlung eines unbekannten Datums in ein Bekanntes. Setzt aktives Handeln des Verantwortlichen voraus. Gilt nicht, wenn der/dem Verantwortlichen eine Information aufgezwungen wird.
Erfassung	Technische Formgebung erhobener Daten. Arbeitsvorgang mit dem eine erstmalige Speicherung des bekannten Datums auf einem Datenträger erfolgt. Ermöglicht die weitere technische Verarbeitung. Gilt auch, wenn Datum aufgezwungen wurde.
Organisieren	Strukturelle Neuanordnung/systematische Strukturierung der gespeicherten personenbezogenen Daten auf dem Datenträger. Organisation personenbezogener Daten bezeichnet das Ergebnis des Sammelns und Ordnen von Daten. Vereinfacht das Auffinden und Auswerten.
Ordnen	Sinnvoll strukturierte Ablage der gespeicherten personenbezogenen Daten auf dem Datenträger, z.B. nach Alphabet.
Speichern	Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Umfasst nicht nur die erstmalige Speicherung, sondern auch Zwischenspeicherungen auf Datenträger oder das Umspeichern von personenbezogenen Informationen, um diese für eine weitere Verwendung aufzubewahren. Die Aufbewahrung des Speichermediums zählt ebenfalls dazu. Gegenteil von Löschen und Vernichten.
Anpassen	Beispiel für Veränderung. Aktualisierung/Angleichung der personenbezogenen Daten an die reellen Lebensumstände, z.B. Änderung der Wohnanschrift.
Verändern	Bearbeitung bzw. inhaltliche Umgestaltung gespeicherter personenbezogener Daten oder ihrer Zuordnung. Es kommt zu einer Änderung des Informationsgehalts. Sie können jedoch auch verändert werden, indem sie ergänzt, in einen neuen Zusammenhang gestellt oder für einen anderen Zweck verwendet werden.
Auslesen	Bewusste Kenntnisnahme über die auf einem Datenträger befindlichen personenbezogenen Daten/Abrufen von Informationen. Daten werden aus einem Datenträger ausgelesen, um sie einer weiteren Bearbeitung zugänglich zu machen.
Abfragen	Gezielte Informationssuche auf einem Datenträger und Kenntnisnahme dieser/Gewinnung von Daten. Zum Beispiel mithilfe der Eingabe eines Suchbegriffs.
Verwenden	Alle Beispiele außer Erheben und Erfassen sind Unterbeispiele von Verwenden. Jeder gezielte Umgang mit personenbezogenen Daten kann als Verwendung der Daten gelten. Sinngemäße Nutzung einer bereits bekannten Information.
Offenlegen	Vorgang, der dazu führt, dass Daten für andere zugänglich gemacht werden und sie diese auslesen oder abfragen können. Bekanntgabe bekannter gespeicherter Daten an Dritte.
- **durch Übermittlung**	Gezielte Weitergabe von Daten an einen oder mehrere Empfänger.

.

- **durch Verbreitung**	Ungezielte Weitergabe an unbestimmte Adressaten z.B. Öffentlichkeit.
- **durch andere Form der Bereitstellung**	Passive Form der Offenlegung. Bereithaltung der Daten zum potenziellen Gebrauch, z.B. für eine Einsicht.
Abgleichen	Vergleich mehrerer zusammengehöriger bekannter, nicht am selben Ort gespeicherter Daten. Abweichungen oder Übereinstimmungen können festgestellt werden.
Verknüpfen	Zuordnung mehrerer zusammengehöriger bekannter, nicht am gleichen Ort gespeicherter Daten. Ziel ist die Entstehung einer neuen Datenstruktur durch Zusammenführung der Daten. (Dient z.B. der Erleichterung der Durchführung von Abfragen).
Einschränken	Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken (Art. 4 Nr. 3). Entspricht der Sperrung von Daten.
Löschen	Entfernung/Unkenntlichmachung einer gespeicherten Information von jedem Datenträger, sodass die Daten keinesfalls mehr ausgelesen bzw. wiederhergestellt werden können. Der Datenträger kann physisch erhalten bleiben. Es erfolgt kein Löschen durch Verschlüsselung oder Anonymisierung der Daten.
Vernichten	Physische Beseitigung der Daten. Vollständige Zerstörung des Datenträgers, sodass keinerlei Information mehr auslesbar ist.

Hinweis Nr. 3
Geplanter oder tatsächlicher Beginn der Verarbeitung von personenbezogenen Daten (wann ist das Verfahren in Betrieb genommen bzw. wann wird es in Betrieb gehen). Dabei ist schon die erstmalige Übertragung oder Speicherung von Daten relevant.

Hinweis Nr. 4
Nur bei Beendigung der Verarbeitung auszuwählen. Bei Auswahl kann das ursprüngliche Erfassungsformular verwendet werden. In Abstimmung mit dem Datenschutzbeauftragten der OE ist über die weitere Verwendung des Datenbestands zu entscheiden, also ob Löschung oder Migration in andere Verfahren erforderlich ist.

Hinweis Nr. 5
Gemeint ist die Behörde, das Bezirksamt oder eine sonstige Organisationseinheit (z.B. Landesbetrieb). Bei der Eintragung sollten keine konkreten Namen sondern Funktionsbezeichnungen (z.B. Präses der Behörde … , Geschäftsleitung des Landesbetriebes …) genannt werden.

Hinweis Nr. 6
Dient der Transparenz in der Auftragsverarbeitung, der Sicherstellung einer sorgfältigen Auswahl des Dienstleisters, dem Nachweis eines Vertrags und der Wahrnehmung der Kontrollpflichten.

Hinweis Nr. 7
Zieldefinition der Verarbeitung personenbezogener Daten und Nennung der darauf gerichteten rechtlichen Grundlage (Prinzip des Verarbeitungsverbots mit Erlaubnisvorbehalt).

Hinweis Nr. 8
Konkrete Beschreibung des Zwecks der Datenverarbeitung und der Datenverarbeitung selbst. Es empfiehlt sich, entsprechende Erläuterungen möglichst unter der in der Behörde bekannten Terminologie zu formulieren und in Zweifelsfällen Rücksprache mit dem Datenschutzbeauftragten der OE zu halten.

Hinweis Nr. 9
Nennung der durch die Verarbeitung betroffenen Personengruppen, z. B. Beschäftigte (Mitarbeiter(-gruppen)), Berater, Kunden, Lieferanten, Patienten, Schuldner, Versicherungsnehmer, Interessenten.

Hinweis Nr. 10
Datenkategorien werden verwendet, um die jeweiligen Metadaten kategorisiert abbilden zu können.
Beispiele für Datenkategorien: Identifikations- und Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten (z. B. Verbindungsdaten, Logging-Informationen).

Hinweis Nr. 11
Die Verarbeitung besonderer Kategorien personenbezogener Daten ist in Art. 9 Abs. 1 DS-GVO geregelt. Umfasst sind Verarbeitungen von Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Eine Verwendung dieser besonders schutzbedürftigen Daten führt zwangsläufig zu einem hohen Schutzbedarf und es ist in jedem Fall eine Datenschutzfolgenabschätzung durchzuführen.

Hinweis Nr. 12
Hier werden die Empfänger personenbezogener Daten zur Weiterverarbeitung bzw. Nutzung innerhalb der verantwortlichen Stelle oder im Rahmen einer Übermittlung an Dritte erfasst..

»Empfänger« ist jede Person oder Stelle, die Daten erhält, z. B. Vertragspartner, Kunden, Behörden, Versicherungen, ärztliches Personal, Auftragsverarbeiter (z. B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter), oder ein Verfahren, bzw. Geschäftsprozess, an den Daten weitergegeben werden.

Interne Empfänger sind jede Empfänger innerhalb des Verantwortungsbereiches bzw. innerhalb der Organisationseinheit. Organisationseinheit meint Behörde, Bezirksamt oder sonstige Organisationseinheit (z.B. Landesbetrieb).

Externe und Dritte sind jede Empfänger außerhalb des Verantwortungsbereiches, z.B. auch andere Behörden innerhalb der Verwaltung und Behörden der Bundesverwaltung und Empfänger außerhalb der Verwaltung.

Sobald Daten im Filesystem gespeichert werden, ist automatisch eine Übermittlung von Daten an Dritte, hier Dataport, gegeben.

Die Art der Daten oder Datenkategorien ist getrennt nach dem jeweiligen Drittstaat und den jeweiligen Empfängern oder Kategorien von Empfängern anzugeben.

Hinweis Nr. 13
Gemäß Art. 5 Abs. 1 lit. e DS-GVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Unter Beachtung (z.B. steuer-) gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen müssen die Daten nach Zweckfortfall unverzüglich gelöscht werden. Wird keine Löschung ausgewählt oder bei Zweifeln zu Aufbewahrungsfristen und Löschroutinen ist Rücksprache mit dem Datenschutzbeauftragten der OE zu halten.

Hinweis Nr. 14
Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur angegeben werden, um ein besseres Verständnis der Beschreibung der technischen und organisatorischen Maßnahmen zu ermöglichen.
Im Rahmen der Bürokommunikation werden verschiedene IT-Infrastrukturen (z.B. Computer Cloud Mail System, Telefonie, SharePoint) in Anspruch genommen. Diese sollen nicht extra erwähnt werden. Die entsprechenden IT-Infrastruktur-Beschreibungen müssen von den Fachlichen Leitstellen vorgenommen werden.

Hinweis Nr. 15
Skizzierung des Berechtigungsverfahrens und Nennung der berechtigten Gruppen. Sofern vorhanden kann auf ein umfassendes Berechtigungskonzept verwiesen werden.

Sollte bei zu überführenden Verfahren ein Zugriffsberechtigungskonzept bereits Teil der durchgeführten Risikoanalyse sein, dann auf dieses verwiesen werden.

Hinweis Nr. 16
Beschreibung der Schutzmaßnahmen im Hinblick auf die Kontrollziele für die jeweils verarbeiteten personenbezogenen Daten. Nähere Ausführungen zu den Anforderungen an Schutzmaßnahmen kann der Anlage 2 entnommen werden.

Ergänzend kann auf die ISO 27001 Bezug genommen werden. Die Kontrollziele zur angemessenen Sicherung der Daten vor Missbrauch und Verlust sind dabei nicht abschließend oder als in Gänze verpflichtender Maßnahmenkatalog zu sehen. So könnten aufgrund einer Spezialgesetzgebung zum Datenschutz weitere Kontrollziele und entsprechende Maßnahmen gefordert sein (z. B. aus dem Telekommunikationsgesetz, aus der Sozialgesetzgebung, oder aus den Landesdatenschutzgesetzen).

Bei nicht automatisierten Verfahren sind nur die organisatorischen Maßnahmen zu benennen.

Hinweis Nr. 17
Nach Art. 25 der DS-GVO müssen geeignete Mittel für die Verarbeitung festgelegt sowie technische und organisatorische Maßnahmen getroffen werden, die dazu ausgelegt sind, die Datenschutzvorgaben aus der Datenschutzverordnung wirksam umzusetzen und die Rechte der Betroffenen Personen zu schützen.

Hinweis Nr. 18
Bei Verarbeitungen auf Grundlage eines Vertrages oder einer Einwilligung, für die die Betroffenen den Behörden Daten bereitgestellt haben, haben sie nach Art. 20 DS-GVO das Recht, diese sie betreffenden personenbezogenen Daten, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder sie an einen anderen Verantwortlichen übermitteln zu lassen, sofern dies technisch machbar ist.

„Soweit technisch machbar“ bedeutet, dass Verantwortliche bereits über entsprechende Einrichtungen verfügen, diese aber nicht neu implementieren müssen, um ein Recht auf Datenportabilität erfüllen zu können.

Hinweis Nr. 19
Nach Art. 12 der DS-GVO müssen beim Verantwortlichen geeignete Maßnahmen getroffen werden, um den Betroffenen die in Art. 13 und 14 DS-GVO aufgeführten Angaben, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Dies kann schriftlich oder in einer anderen Form, z.B. elektronisch erfolgen.

Anlage 2

Übersicht und Erläuterungen zu den technischen und organisatorischen Maßnahmen

Grundwerte	ergriffene TOMs
Datenminimierung Art. 5 Abs. 1 lit.c DS-GVO	
Gewährleistung der **Integrität** Art. 32 Abs. 1 lit. b DS-GVO	
Gewährleistung der **Verfügbarkeit** Art. 32 Abs. 1 lit. b DS-GVO	
Gewährleistung der **Vertraulichkeit** Art. 32 Abs. 1 lit. b DS-GVO	
Intervenierbarkeit Art. 5 Abs. 1 lit. d,f DS-GVO	
Nichtverkettung Art. 5 Abs. 1 DS-GVO	
Transparenz Art. 5 Abs. 1 lit. a DS-GVO	
Gewährleistung der **Belastbarkeit der Systeme** Art. 32 Abs 1 lit. b DS-GVO	
Verfahren **regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** Art. 32 Abs. 1 lit. d DS-GVO	
Verfahren zur **Wiederherstellung der Verfügbarkeit** personenbezogener Daten nach einem physischen oder technischen Zwischenfall Art. 32 Abs. 1 lit. c DS-GVO	

Erläuterungen zu den Technischen und organisatorischen Maßnahmen gem. Art. 30 Abs. 1 S. 2 lit. g DS-GVO

Trotz der Formulierung „wenn möglich“ stellt die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO hier den Regelfall dar.
Art. 5 Abs. 2 DS-GVO verpflichtet den Verantwortlichen insbesondere auch zur Dokumentation der technischen und organisatorischen Maßnahmen (Art. 5 Abs. 1 lit. f DS-GVO). Zudem muss der Verantwortliche die Wirksamkeit dieser Maßnahmen regelmäßig überprüfen (Art. 32 Abs. 1 lit. d DS-GVO). Beide Forderungen kann der Verantwortliche nur erfüllen, wenn die technischen und organisatorischen Maßnahmen vollständig beschrieben sind (etwa in einem Sicherheitskonzept).

Eine Verarbeitung darf erst erfolgen, wenn der Verantwortliche seiner Pflicht nach Art. 24 DS-GVO nachgekommen ist. Darunter fallen neben den Verpflichtungen nach Art. 12 und 25 DS-GVO auch diejenigen nach Art. 32 DSGVO zur Bestimmung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das betrifft primär Fragen der Sicherheit der Verarbeitung, schließt somit aber

auch Maßnahmen zur Gewährleistung von Betroffenenrechten ein. In das Verzeichnis ist eine allgemeine, einfach nachvollziehbare Beschreibung der für diesen Zweck getroffenen Maßnahmen aufzunehmen.

Die Beschreibung der jeweiligen Maßnahme ist konkret auf die Kategorie betroffener Personen bzw. personenbezogener Daten im Sinne des Art. 30 Abs. 1 S. 2 lit. c DS-GVO zu beziehen, soweit eine entsprechende Differenzierung in ihrer Anwendung erfolgt.

Für die Bestimmung der zu treffenden Maßnahmen wird auf das Standard-Datenschutzmodell, die Leitlinien und Orientierungshilfen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und der Artikel-29-Arbeitsgruppe sowie auf die bestehenden nationalen und internationalen Standards (z. B. BSI-Grundschutz, ISO-Standards) verwiesen. Ist bei der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zu erwarten, hat die Bestimmung der Maßnahmen bereits im Rahmen einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO zu erfolgen.

Eine Verletzung der Sicherheit der Datenverarbeitung ist immer eine Verletzung des Schutzes personenbezogener Daten i. S. v. Art. 4 Nr. 12 DS-GVO.

Nach Art. 32 Abs. 1 DS-GVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der mit ihr verbundenen Risiken geeignete technische und organisatorische Maßnahmen zu treffen, um insbesondere Folgendes sicherzustellen:

Maßnahmenbereiche, die sich aus Art. 32 Abs. 1 DS-GVO ergeben:

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste
- Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
- Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Nachfolgend werden den einzelnen Bereichen typische, bewährte technische und organisatorische Maßnahmen zugeordnet. Die Auflistung ist nicht vollständig oder abschließend. In Abhängigkeit von den konkreten Verarbeitungstätigkeiten können weitere oder andere Maßnahmen geeignet und angemessen sein. Auch ist die Zuordnung einzelner Maßnahmen zu einem bestimmten Maßnahmenbereich nicht in jedem Fall eindeutig.

Hinweis: Wird das Verfahren in der IT-Infrastruktur der FHH betrieben (dazu zählt auch das Dataport Rechenzentrum) greifen grundlegend die TOMs Sicherheits- und Betriebskonzept Rechenzentrum Dataport und die Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten (vgl. teilweise Tabelle Anlage 3).

Maßnahmen zur Pseudonymisierung personenbezogener Daten

Hierzu zählen u. a.:

- Festlegung der durch Pseudonymisierung zu ersetzenden identifizierenden Daten
- Definition der Pseudonymisierungsregel, ggf. anknüpfend an Personal-, Kunden- oder Patienten-Kennziffern
- Autorisierung: Festlegung der Personen, die zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind
- Festlegung der zulässigen Anlässe für Pseudonymisierungs- und Depseudonymisie-rungsvorgänge
- zufällige Erzeugung der Zuordnungstabellen oder der in eine algorithmische Pseudony-misierung eingehenden geheimen Parameter
- Schutz der Zuordnungstabellen bzw. geheimen Parameter sowohl gegen unautorisierten Zugriff als auch gegen unautorisierte Nutzung
- Trennung der zu pseudonymisierenden Daten in die zu ersetzenden identifizierenden und die weiteren Angaben

Maßnahmen zur Verschlüsselung personenbezogener Daten
(z. B. in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport)

Schlüssel können flüchtig (z. B. für die Dauer eines Kommunikationsvorgangs) oder statisch (mittel- oder langfristig)

für den Schutz personenbezogener Daten eingesetzt werden.

Es sind Festlegungen zu treffen (z. B. im Rahmen eines Kryptokonzepts) u. a. zur Auswahl geeigneter kryptografischer Verfahren und Produkte, zur Organisation ihres Einsatzes, zu Maßnahmen bei der Entdeckung von Schwächen in Verschlüsselungsverfahren oder -produkten (Um- oder Überverschlüsselung) sowie zu Schlüssellängen. Voraussetzung für effektive Verschlüsselung ist ein adäquates Schlüsselmanagement, das u. a. folgende Aspekte betrifft:

- zufällige Erzeugung der Schlüssel
- Autorisierung von Personen zur Verwaltung und zur Nutzung von Schlüsseln bzw. ihre Zuweisung zu Geräten, in denen sie eingesetzt werden
- zuverlässige Schlüsselverteilung, Verknüpfung von Schlüsseln mit Identitäten von natürlichen Personen oder informationstechnischen Geräten, ggf. Einbringen in speziell gesicherte Speichermedien (z. B. Chipkarten)
- Schutz der Schlüssel vor nicht autorisiertem Zugriff oder Nutzung
- regelmäßiger oder situationsbezogener Schlüsselwechsel, ggf. eine Schlüsselarchivierung, stets sorgfältige Schlüssellöschung nach Ablauf des Lebenszyklusses
- Verwaltung des Lebenszyklus der Schlüssel von Erzeugung und Verteilung über Nutzung bis zu ihrer Archivierung und Löschung

Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste

Die folgenden Maßnahmen sollen eine spezifikationsgerechte Verarbeitung sichern und nicht autorisierte bzw. unberechtigte Verarbeitung sowie unbeabsichtigte Änderung, Verlust oder Schädigung personenbezogener Daten ausschließen; beim Verantwortlichen selbst oder auf dem Transportweg zu Auftragsverarbeitern oder Dritten.

Hierzu zählen u. a.:

- Formulierung von verbindlichen Sicherheitsleitlinien
- Definition der Verantwortlichkeiten für das Informationssicherheitsmanagement
- Inventarisierung der zu verarbeitenden personenbezogenen Daten
- Inventarisierung der Informationstechnik
- Erarbeitung eines Sicherheitskonzepts, ggf. unter Durchführung einer Risikoanalyse
- Personalsicherheit: Überprüfung und Verpflichtung des Personals, Sensibilisierung und Training, Aufgabentrennung
- Spezifikation der Sicherheitsanforderungen an Informationssysteme und deren Konfiguration, Prüfung ihrer Einhaltung
- Schutz vor unberechtigtem physischem Zugang, einschließlich Schutz von Mobilgeräten
- Erarbeitung eines Rollen- und Rechtekonzepts
- Maßnahmen zur Autorisierung von Personen für den Zugriff auf personenbezogene Daten und die Steuerung der Verarbeitung
- Zugriffskontrolle und sicherer Umgang mit Speichermedien, einschließlich der Maßnahmen zur zuverlässigen Authentisierung von Personen gegenüber der Informationstechnik, zur Sicherung der Revisionsfähigkeit der Eingabe und der Änderung von personen- bezogenen Daten sowie ggf. der Nutzung und des Zugriffs auf diese und zur Revision dieser Prozesse
- Maßnahmen der Betriebssicherheit, insbesondere zur Spezifikation der Bedienabläufe, zur Änderungssteuerung, zum Schutz vor Malware, zum Umgang mit technischen Schwachstellen, zur kontrollierten Installation und Konfiguration neuer Software, sowie zur Ereignisüberwachung und -protokollierung, einschließlich der regelmäßigen und anlassbezogenen Auswertung dieser Protokolle
- Maßnahmen, die (berechtigte oder unberechtigte) Veränderung gespeicherter oder übertragener Daten nachträglich feststellbar machen (z. B. Signaturverfahren, Hashverfahren)
- Maßnahmen zur Kommunikationssicherheit: Netzwerksicherheitsmanagement, insbesondere zur Kontrolle und Einschränkung des Datenverkehrs (Firewalls, Application Layer Gateways), Einrichtung von Sicherheitszonen, Authentisierung von Geräten gegeneinander
- sichere Gestaltung von Informationsübertragungen, einschließlich des Abschlusses von Vereinbarungen mit regelmäßigen Übermittlern und Empfängern personenbezogener Daten und der Authentisierung der Kommunikationspartner
- Sicherung und Überprüfung der Authentizität der übermittelten Daten
- sichere Einbeziehung von externen Diensten
- Management von Informationssicherheitsvorfällen
- Aufrechterhaltung der Informationssicherheit bei ungeplanten Systemzuständen
- Durchführung von internen oder externen Sicherheitsaudits
- logische oder physikalische Trennung der Datenverarbeitung z. B. nach verantwortlichen Stellen, den verfolgten Verarbeitungszwecken und nach Gruppen betroffener Personen

.

- sicheres, rückstandsfreies Löschen von Daten bzw. Vernichten von Datenträgern nach Ablauf der Aufbewahrungsfristen, Festlegungen zu Löschverfahren und zur Beauftragung von Dienstleistern

Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste

Die folgenden Maßnahmen sollen sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden.

Hierzu zählen u. a.:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage z. B. DDOS, höhere Gewalt)
- Dokumentation von Syntax und Semantik der gespeicherten Daten
- Redundanz von Hard- und Software sowie Infrastruktur
- Umsetzung von Reparaturstrategien und Ausweichprozessen
- Vertretungsregelungen für abwesende Mitarbeiter

Maßnahmen, um nach einem physischen oder technischen Zwischenfall (Notfall) die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen rasch wiederherzustellen.

Eine besondere Ausprägung der Gewährleistung von Verfügbarkeit ist hinsichtlich möglicher Notfälle (siehe dazu auch BSI Standard 100-4) erforderlich.

Hierzu sind u. a. folgende Maßnahmen erforderlich:

- Erstellung und Umsetzung eines Notfallkonzepts
- Erarbeitung eines Notfallhandbuches
- Integration des Notfallmanagements in Geschäftsprozesse
- Durchführung von Notfallübungen
- Erprobung von Wiederanlaufszenarien

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Hierzu zählen u. a.:

- regelmäßige Revision des Sicherheitskonzepts
- Information über neu auftretende Schwachstellen und andere Risikofaktoren, ggf. Überarbeitung der Risikoanalyse und -bewertung
- Prüfungen des Datenschutzbeauftragten und der IT-Revision auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme
- externe Prüfungen, Audits, Zertifizierungen

Weitere Maßnahmenbereiche, die sich aus der DS-GVO ergeben und deren Darstellung im Verzeichnis empfohlen wird:

Die Formulierung in Art. 32 Abs. 1 DS-GVO „diese Maßnahmen schließen unter anderem Folgen des ein“ verdeutlicht, dass die dort vorgenommene Aufzählung nicht abschließend ist. Die Sicherheit der Verarbeitung ist u. a. auch Voraussetzung dafür, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden (Zweckbindung), dass Betroffene, Verantwortliche und Kontrollinstanzen u. a. erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden (Transparenz) und dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden (Intervenierbarkeit). Entsprechend sind auch die Maßnahmenbereiche zu berücksichtigen, die vorrangig der Minimierung der Eingriffsintensität in die Grundrechte Betroffener dienen.

Maßnahmen zur Gewährleistung der Zweckbindung personenbezogener Daten (Nichtverkettung) – Art. 5 Abs. 1 lit. b) DS-GVO:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten

.

- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
- Trennung nach Organisations-/Abteilungsgrenzen
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten
- geregelte Zweckänderungsverfahren

Maßnahmen zur Gewährleistung der Transparenz für Betroffene, Verantwortliche und Kontrollinstanzen – Art. 5 Abs. 1 lit. a) DS-GVO:

- Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren
- Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren
- Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen
- Dokumentation von Einwilligungen und Widersprüchen
- Protokollierung von Zugriffen und Änderungen
- Nachweis der Quellen von Daten (Authentizität)
- Versionierung
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts
- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept

Maßnahmen zur Gewährleistung der Betroffenenrechte – Art. 13 ff. DS-GVO (Intervenierbarkeit):

- differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte
- Einrichtung eines Single Point of Contact (SPoC) für Betroffene
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten

.
Anlage 3

Darstellung der ergriffenen Technischen und Organisatorischen Maßnahmen (TOMs) der FHH im Vergleich zu den TOMS nach BDSG und Grundwerten nach Grundschutz und DS-GVO

Grundwerte nach DS-GVO	Definierte Technische und Organisatorische Maßnahmen (TOMs) nach § 64 BDSG	Ergriffene Technische und Organisatorische Maßnahmen (TOMs) der FHH
Datenminimierung Art. 5 Abs. 1 lit.c DS-GVO	-	Verwaltungsvorschrift IT-Projekte (bei kleineren IT-Projekten wird diese VV sinngemäß angewendet) Richtlinie über Mindestanforderungen an die Sicherheit der Datenverarbeitung auf UNIX-Rechnern (UNIX-Richtlinie)
Gewährleistung der **Integrität** Art. 32 Abs. 1 lit. b DS-GVO	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)
	Datenintegrität (§ 64 Abs. 3 Nr. 11 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Geschäftsbestimmungen der Behörden (Revisionfähige Prozessbeschreibungen, Überprüfbarkeit des Verwaltungshandelns)
	Datenträgerkontrolle (§ 64 Abs. 3 Nr. 2 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich Entsorgungs-Richtlinie
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich

	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzepte der jeweiligen Fachverfahren Grundsätze des Verwaltungshandelns nach Beamtenstatusgesetz bzw. Tarifvertrag (Verschwiegenheitspflicht)
	Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)	Betriebskonzept des jeweiligen Fachverfahrens Geschäftsordnungsbestimmungen der Behörden
	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO
	Zugangskontrolle (§ 64 Abs. 3 Nr. 1 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Datatport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept)
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
Gewährleistung der **Verfügbarkeit** Art. 32 Abs. 1 lit. b DS-GVO	Verfügbarkeitskontrolle (§ 64 Abs. 3 Nr. 13 BSDG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden Richtlinie Regelwerk ELDORADO
	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO

	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL)Rahmen-Sicherheitskonzept der FHH (RaSiKo)Sicherheits- und Betriebskonzept Rechenzentrum DataportGeschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
Gewährleistung der **Vertraulichkeit** Art. 32 Abs. 1 lit. b DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	Freigabe-Richtlinie Service-Level-Agreements Richtlinie zur Datensicherheit im IuK-Bereich
	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzepte der jeweiligen Fachverfahren Grundsätze des Verwaltungshandelns nach

		Beamtenstatusgesetz bzw. Tarifvertrag (Verschwiegenheitspflicht)
	Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)	Betriebskonzept des jeweiligen Fachverfahrens Geschäftsordnungsbestimmungen der Behörden
	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
Intervenierbarkeit Art. 5 Abs. 1 lit. d,f DS-GVO	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO
Nichtverkettung Art. 5 Abs. 1 DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	Freigabe-Richtlinie Service-Level-Agreements Richtlinie zur Datensicherheit im IuK-Bereich
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzepte der jeweiligen Fachverfahren Grundsätze des Verwaltungshandelns nach Beamtenstatusgesetz bzw. Tarifvertrag (Verschwiegenheitspflicht)
	Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)	Betriebskonzept des jeweiligen Fachverfahrens Geschäftsordnungsbestimmungen der Behörden
Transparenz Art. 5 Abs. 1 lit. a DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	Freigabe-Richtlinie Service-Level-Agreements Richtlinie zur Datensicherheit im IuK-Bereich

	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum DataportVorgaben für das Haushalts- und KassenrechtRichtlinie zur Verwaltung von PasswörternGeschäftsordnungsbestimmungen der Behörden
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
Verfahren **regelmäßiger Überprüfung**, **Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** Art. 32 Abs. 1 lit. d DS-GVO	-	turnusmäßige Überarbeitung der Richtlinien der FHH (PDCA-Modell im RaSiKo, IS-LL) turnusmäßige Überarbeitung des Sicherheitskonzeptes durch Dataport
Verfahren zur schnellen **Wiederherstellung der Verfügbarkeit** personenbezogener Daten nach einem physischen oder technischen Zwischenfall Art. 32 Abs. 1 lit. c DS-GVO	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO

Gewährleistung der **Belastbarkeit der Systeme** Art. 32 Abs. 1 lit. b DS-GVO	Verfügbarkeitskontrolle (§ 64 Abs. 3 Nr. 13 BSDG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden Richtlinie Regelwerk ELDORADO
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)

Definitionen der Grundwerte nach DS-GVO:

Datenminimierung:	Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.
Vertraulichkeit:	Gewährleistung, dass Informationen ausschließlich Berechtigten zugänglich sind
Verfügbarkeit:	Gewährleistung, dass Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang und in angemessener Zeit nutzbar sind
Integrität:	Gewährleistung, dass die Unverfälschtheit und Vollständigkeit von Informationen, Anwendungen und IT-Systemen überprüfbar sind
Nichtverkettung:	Erhobene personenbezogene Daten werden nur für den Zweck verarbeitet, zu dem sie erhoben wurden.
Transparenz:	Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.
Intervenierbarkeit:	Gewährleistung von Betroffenenrechten zu Berichtigung, Löschen, Widerspruch und zur Einschränkung der Verarbeitung sowie zur Datenportabilität..

Definitionen der TOMs gem. § 64 BDSG:

Zugangskontrolle:	Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte
Datenträgerkontrolle:	Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern
Speicherkontrolle:	Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten
Benutzerkontrolle:	Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte
Zugriffskontrolle:	Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben

Übertragungskontrolle:	Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können
Eingabekontrolle:	Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind
Transportkontrolle:	Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden
Wiederherstellbarkeit:	Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können
Zuverlässigkeit:	Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden
Datenintegrität:	Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können
Auftragskontrolle:	Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können
Verfügbarkeitskontrolle:	Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind
Trennbarkeit	Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

Funktionsübersicht
Ausbildungsmanagement-System

Der Softwareanbieter GuideCom bietet durch verschiedene Module seines digitalen Personalmanagementsystems „Magellan“ Lösungen für unterschiedlichste Anwendungs- und Aufgabenbereiche. Angeboten werden laut Internetseite (Stand 07.09.2022) von GuideCom eigenständige Module für:

- *Recruiting*
- **Ausbildungsmanagement**
- *Skill Management*
- *Feedbackgespräche*
- *Weiterbildungsmanagement*
- *Learning | LMS*
- *Personalplanung*
- *Digitale Personalakte*
- *HR Analytics*
- *HR-Serviceprozesse*
- *Gehalts- & Prämiensysteme*
- *Reisekostenmanagement*

Das Personalamt, vertreten durch den Landesbetrieb ZAF/AMD beabsichtigt das Modul „Young Talents – Ausbildungsmanagement“ einzusetzen, welches Gegenstand dieser Vereinbarung nach § 93 HmbPersVG ist.

Über das Ausbildungsmanagement-System (AMS) Young Talents soll die Ausbildung der Nachwuchskräfte in den vom Personalamt gemäß Anlage 3 angebotenen Ausbildungsgängen gesteuert werden. Das AMS unterstützt die Organisation und Ablaufplanung der berufspraktischen Ausbildungsphasen und versorgt die an der Ausbildung beteiligten Akteure und Nachwuchskräfte mit Informationen.

Das AMS wird insb. folgende Prozesse in der Ausbildung unterstützen, die nachfolgend aufgezählt werden:

1. **Aufnahme der für die Ausbildung und das AMS relevanten Daten**
   - Erfassung von Praxisstellen (im AMS „Einsatzorte“)
   - Erfassung von Ausbilder:innen in den Einsatzorten
   - Erfassung von Nachwuchskräften / Anlage der Azubi-Karten
   - Zuordnung der Nachwuchskräfte zu Jahrgängen und Klassen / Gruppen
   - Erfassung von Ausbildungsleitungen in den Behörden und Ämtern sowie deren Vertretungen

2. Erfassung von Ausbildungs- und Studiengängen (im AMS „Berufsbilder“)

- Erfassung des Ablaufs:
  - Start
  - Ende
  - Theorie- und Praxisphasen
  - Lerninhalte und Lernziele
  - Verantwortliche der Ausbildungssteuerung
- Einstellen von Lernmaterialien (übergeordnet und Ausbildungsplatz bezogen)
- Einstellen von berufsbildbezogenen Checklisten

3. Abbildung und Planung der Praxisphasen

- Planung von Klassen-/Gruppeneinsätzen wie z.B. Einführungstage
- Verteilung der Nachwuchskräfte auf die Einsatzorte, manuell oder per Automation anhand von Planungsparametern

4. Durchführung der Ausbildungs- und Studiengänge

- Erstellung und Abstimmung der Einsatzfeedbacks per Workflow pro Einsatzort
- Bei Bedarf: Erfassung der Tätigkeiten im Berichtsheft (gem. BBiG) und Vorlage per Workflow
- Erfassung der Berufs-/Hochschulnoten durch die Nachwuchskräfte
- Erstellung von Einsatz**ort**-Feedbacks durch die Nachwuchskräfte

5. Organisatorisches

- E-Mail-Kommunikation mit einzelnen Personen oder Gruppen
- Checklisten, Dokumente und Vorlagen können eingestellt und den Nachwuchskräften zugeordnet werden
- Im Bereich Lernmedien können Lernmaterialien freiwillig bereitgestellt werden
- Einfaches Veröffentlichen von Ausbildungsnews und -informationen unter dem Menüpunkt Infos (vgl. zu einem „schwarzen Brett“)

Da das Modul Young Talents eigenständig eingesetzt werden soll, entfallen Zusatz- / Querschnittsfunktionen, die in Kombination mit weiteren der oben aufgeführten Module möglich wären.

Hier sind insb. folgende auf der Homepage von GuideCom beworbene Funktionen zu nennen und abzugrenzen, die **nicht** genutzt werden:

1. *Recruiting & Onboarding*
   - *KI-basierte Bewerbungsanalysen (CV-Parsing) für automatisierte Datenerhebung und Vorselektierung*
   - *Preboarding bis zum Ausbildungsstart*

2. *Entwicklungsplanung*
   - *Verankerung der Entwicklungsziele*
   - *Kluge Verbindung von vorgegebenen Lernzielen und benötigten Skills*
   - *Smarte Abbildung von fachlichen und überfachlichen Skills*
   - *Fundament für spannende Entwicklungsperspektiven*
   - *Nahtloser Übergang zum Talent Management Prozess (Entwicklungspläne, Perspektivprogramme, Mitarbeiterportfolios)*

3. *Unter: Digitale Azubi-Karte & Collaboration*
   - *Zentrales Archiv für alle Dokumente und Dateien*

4. *Unter: Leistungsübersichten & Feedbacks*
   - *Clevere Anzeige auffälliger Beurteilungen*

5. *Digitale Prozesse & Workflows*
   - *Zeugniserstellung auf Basis erzielter Leistungen*

6. *Unter: Digitale Lernplattform & Blended Learning*
   - *Effiziente Zusammenarbeit mit führenden Anbietern für beste Inhalte*

Explizit und abschließend zu erwähnen ist, dass das AMS **nicht die Funktion einer Personalakte** übernimmt bzw. diese ersetzt.

Auflistung der im „Ausbildungsmanagement-System (AMS)“ verwalteten Ausbildungs- und Studiengänge sowie Berufsvorbereitungen

Folgende vom Personalamt angebotenen Ausbildungs- und Studiengänge sowie Berufsvorbereitungen werden im Rahmen des „Ausbildungsmanagement-Systems (AMS)“ erfasst und verwaltet:

a) Ausbildung zur/zum Verwaltungsfachangestellten
b) Ausbildung zur/zum Regierungssekretär/in
c) Ausbildung zur/zum Regierungsinspektor/in im Bachelor-Studiengang Public Management
d) Soziale Arbeit im Bachelor-Studiengang
e) E-Government im Bachelor-Studiengang

Berechtigungs-, Rollen- und Löschkonzept für das IT-Verfahren

„Ausbildungsmanagement-System (AMS)“

Im Folgenden wird beschrieben, wie „Rollen“ und „Berechtigungen“ im IT-Verfahren AMS (bzw. im Produkt Magellan Young Talents) verwendet und vergeben werden und die „Löschungen“ erfolgen.

1. Grundlagen: Berechtigung, Benutzergruppe, Benutzer, Rolle und deren Zusammenspiel

Um den Zugriff auf ausgewählte Funktionalitäten und Daten nur bestimmten Benutzern zugänglich zu machen, verfügt das AMS über eine Vielzahl an **Berechtigungen**. Berechtigungen werden sowohl dafür genutzt, um Berechtigungen an Objekten, wie deren Anzeige, Bearbeitung oder Löschung zu berechtigen, als auch für die Vergabe von Menüpunkten in der Anwendung. Eine solche Berechtigung kann z. B. heißen: Import durchführen.

Diese Berechtigung kann dann **Benutzergruppen** zugewiesen werden. Eine Benutzergruppe bündelt eine Reihe von Berechtigungen. Dadurch können Benutzergruppen für verschiedene Typen von Anwendern definiert werden.

Einzelne Benutzer können Benutzergruppen zugewiesen werden, wobei ein Benutzer dabei beliebig viele Benutzergruppen erhalten könnte. Auf diese Weise können die Berechtigungen sehr detailliert und gleichzeitig schnell zugewiesen werden.

Folgende Benutzergruppen sind für das AMS aktuell vorgesehen:

Benutzergruppe	Betroffene Benutzer
Modul: Ausbildung – Alle Rechte	• Beschäftigte der Fachlichen Leitstelle • Beschäftigte, die Aufgaben in der Personalbetreuung übernehmen, • Beschäftigte, die Aufgaben in der Ausbildungssteuerung übernehmen
Modul: Ausbildung – Ausbildungsleitung	Die je nach Berufsbild zuständigen Ausbildungsleitungen
Modul: Ausbildung – Ausbildungs-verantwortliche Praxisstellen	• Ausbilderinnen und Ausbilder in den Behörden und Bezirksämtern • Koordinatoren in den Behörden und Bezirksämtern
Modul: Ausbildung – Auszubildende	Nachwuchskräfte der vom Personalamt angebotenen Ausbildungen
Modul: Ausbildung – Praxisbüro	Beschäftigte im Praxisbüro (Fachrichtung Soziale Arbeit)
Modul: Basis – Alle Rechte	Beschäftigte der Fachlichen Leitstelle
Modul: Basis – Import	Beschäftigte im Praxisbüro (Fachrichtung Soziale Arbeit)

Zusätzlich zu den Berechtigungen und Benutzergruppen arbeitet das AMS mit **Rollen.** Sie werden wie eine Berechtigung einer Benutzergruppe zugeordnet und geben den Rolleninhabern vor allem die Möglichkeit, Prozesse für Personen im AMS zu veranlassen, die nicht hierarchisch dieser Person zugeordnet sind. Folgende Rollen sind für das AMS vorgesehen:

Rolle	Betroffene Benutzergruppe
Zentral	Ausbildung – Alle Rechte Ausbildung – Ausbildungsleitung Ausbildung – Praxisbüro
Dezentral	Ausbildung - Ausbildungsverantwortliche Praxisstellen Ausbildung – Auszubildende
Administrator	Basis – Alle Rechte Basis – Import

1.1. Manuelle Vergabe von Berechtigungen

Für die Vergabe von Berechtigungen dient das Modul „Basis“.

1.2 Automatische Berechtigungsvergabe

In zwei Anwendungsfällen ist es möglich, automatisch und ohne weiteres manuelles Zutun Berechtigungen zu vergeben werden.

1.2.1 Zuweisung von Benutzern zu Benutzergruppen im Rahmen des Stammdatenimports

Im Rahmen des Imports von Stammdaten aus dem Active Directory (per Excel-Import-Datei) werden in der Regel auch verschiedene Mitarbeiterkennzeichen (Auszubildende, Zentrale Verantwortliche, Dezentrale Verantwortliche) direkt oder abgeleitet importiert. Diese können zur Vereinfachung der Berechtigungsvergabe genutzt werden, um neue oder umgesetzte Personen automatisch in Benutzergruppen einzufügen.

1.2.2 Dynamische Berechtigungsvergabe im Rahmen von Tätigkeiten in Fachmodulen

Auf Basis von bestimmten Aktionen werden automatisch Benutzer oder Berechtigungen zu Benutzergruppen zugewiesen. Dies ist bspw. bei der Hinterlegung von Benutzern als sog. Einsatzortverantwortliche (d.h. Ausbilderin oder Ausbilder einer Behörde oder eines Bezirksamtes) oder bei der Hinterlegung der Ausbildungsleitung einer Behörde oder eines Bezirksamtes der Fall. Die Person erhält dann die Berechtigung, die Azubikarte der ihr zugewiesenen bzw. der ihrer Behörde bzw. Bezirksamt zugewiesenen Nachwuchskräfte einzusehen sowie Aktionen wie Feedbacks auszuführen.

1.3 Protokollierung der Berechtigungsvergabe

Bezüglich der Berechtigungsvergabe sind zwei Tätigkeiten relevant, da diese eine Anpassung von Berechtigungen für konkrete Benutzer ergeben können.

1. Die Zuweisung eines Benutzers zu einer Benutzergruppe wird geändert:
   Diese Tätigkeit wird protokolliert mit den folgenden Inhalten:
   - Benutzer, dessen Zuweisung zu Benutzergruppen geändert wurde
   - Art der Änderung („Hinzufügen“, „Entfernen“)

- Betroffene Benutzergruppe
- Änderungsdatum
- Benutzer, der die Änderung durchgeführt hat (leer, wenn Änderung durch automatische Berechtigungsvergabe induziert wurde (siehe Kapitel 1.2.1)

2. Die Zuweisung einer Berechtigung zu einer Benutzergruppe wird geändert:
   - Diese Tätigkeit wird protokolliert mit den folgenden Inhalten:
   - Benutzergruppe, in der die Zuweisung einer Berechtigung geändert wurde
   - Art der Änderung („Hinzufügen“, „Entfernen“)
   - Betroffene Berechtigung
   - Änderungsdatum

Diese Protokollierung ist nicht optional deaktivierbar und über das AMS nicht änderbar.

1.4 Arten von Berechtigungen

Die im Produkt Magellan vorhandenen Berechtigungen umfassen verschiedene Bereiche: Zugriff auf das Produkt Magellan und die Fachmodule, Sichtbarkeit von Menüpunkten und Funktionen (an Objekten).

Durch die stete Weiterentwicklung von Magellan ändern sich die einzelnen Berechtigungen im Zeitablauf. Berechtigungen werden stets ersetzt oder ergänzt, nicht in ihrer Bedeutung geändert. Werden neue Berechtigungen durch ein Update ergänzt, werden diese nicht automatisch vergeben. In allen Fällen wird in den Versionshinweisen der Fachmodule auf diese Änderung hingewiesen.

1.4.1 Zugriff auf Magellan / Fachmodule

Um auf Magellan zuzugreifen, ist der Zugriff auf mindestens ein Fachmodul notwendig. Im Rahmen des AMS kommen die Module „Basis“ und „Young Talents / Ausbildung“ zum Einsatz. Der Zugriff wird über die Berechtigungen „Zugriff“ gesteuert. Für den Zugriff auf das Modul „Young Talents“ muss folgende Kombination vorliegen:

Berechtigung „*Zugriff*“, Beschreibung „*Zugriff auf die Anwendung*“, Modul „*Young Talents*“

1.4.2 Sichtbarkeit von Menüpunkten

Sichtbarkeiten von Menüpunkten sind über die Berechtigungsbezeichnungen identifizierbar, diese verfügen nur über den entsprechenden Namen, der in der Regel dem Menüpunkt ähnelt. In der Beschreibung wird sie i.d.R. über „Pfad: …“ beschrieben. Wenn nicht anders in der Beschreibung angegeben, ist über die Vergabe der Berechtigung auf diesen Menüpunkt das Leserecht dieser Objekte inkludiert. Für die Berechtigung zum Einsehen ihrer Feedbacks benötigt eine Nachwuchskraft folgende Kombination:

Berechtigung „Überblick – Feedbacks“, Beschreibung „Pfad: Überblick-Feedbacks“, Modul „Young Talents“

1.4.3 Funktionen (an Objekten)

Anpassungen an Objekten sind über die Bezeichnung des Objekts sowie die Verrichtung identifizierbar und nachvollziehbar. Für die Berechtigung zum Bearbeiten von Angaben im Register Leistungen der Azubikarte benötigt eine Nachwuchskraft folgende Kombination:

Berechtigung „Azubis - Register Leistungen bearbeiten“, Beschreibung „Ermöglicht bearbeiten im Register Leistungen“, Modul „Young Talents“

1.5. Ausgabe der vergebenen Berechtigungen

Benutzer, die die Berechtigungsvergabe im Fachmodul „Basis“ (im AMS: Qualitätsmanagement im ZAF / Fachlichte Leitstelle) durchführen können, können die aktuell vergebenen Berechtigungen per Bericht ausgeben. Dazu steht im Menüpunkt Benutzerverwaltung > Benutzergruppen die Schaltfläche Auswertung > Bericht zur Verfügung. Dieser Bericht listet für jeden Benutzer auf, aus welcher Benutzergruppe dieser seine aktuell vorhandenen Berechtigungen erhält.

Eine Übersicht mit beispielhaften Berechtigungen für die Nachwuchskräfte ist am Ende des Dokuments aufgeführt.

2. Eingesetzte Authentifizierungsmechanismen im Überblick

2.1 Form-Login

Der Anwender loggt sich über eine von der Anwendung bereitgestellte Loginmaske ein und wird von der Anwendung als Identity Provider authentifiziert. Dazu muss das AMS alle Benutzer in einer Datenbank vorhalten und hat keine Abhängigkeit auf ein weiteres System. Für den Start des AMS wird diese Variante eingesetzt.

2.2 Kerberos / Integrated Windows Authentication

Der Browser des Anwenders und die Anwendung handeln einen Authentifizierungsmechanismus aus, der auf der Windows-Domäne basiert. Über diesen Weg wird für das AMS die Nutzung von Single-Sign-On ermöglicht. Da zunächst Erfahrungswerte gesammelt werden müssen, ob für alle Kennungen Single-Sing-On händelbar ist, wird diese Variante in einem zweiten Schritt umgesetzt.

2.3 Automatische Abmeldung

Im Standard wird ein angemeldeter User nach 30 Min. Inaktivität ausgeloggt. Eine Sitzung endet auch immer dann, wenn der genutzte Browser vollständig geschlossen wird. Die Zeitspanne bis zur automatischen Abmeldung lässt sich individuell anpassen.

3. Löschkonzept

In Bezug auf das AMS ist unter dem Begriff „Löschen“ zwischen einem "harten" Löschen und einem "weichen" Löschen zu unterscheiden.

<u>„Weiches“ Löschen</u>
Grundsätzlich gilt, dass wenn Einträge im AMS gelöscht werden, diese grundsätzlich „weich“ gelöscht werden. Dies bedeutet, dass die Daten in der Datenbank mit einem „Delete-Flag“ versehen werden. Die Daten sind in der Datenbank noch vorhanden, an der Oberfläche von Magellan allerdings nicht mehr sichtbar.

<u>„Hartes“ Löschen</u>
In Ausnahmefällen wird im AMS direkt „hart“ gelöscht. Einen solchen Fall stellt z.B. das Löschen einer Nachwuchskraft aus der Auszubildendenübersicht dar. Die Nachwuchskraft wird dann mit allen abhängigen Einträgen „hart“ gelöscht. Dies gilt auch für das Löschen von überfälligen Einträgen, d.h. von Einträgen, deren Löschfrist abgelaufen ist. Die „hart“ gelöschten Daten werden dann in der Datenbank mit „Pseudo-Werten“ (x) ersetzt. Persönliche

Daten sind somit sowohl an der Oberfläche des AMS als auch in der Datenbank selbst unkenntlich.

Um das Löschen anzustoßen und im Blick zu behalten, werden im AMS Aufbewahrungsfristen definiert. Diese fordern nach Fristablauf zum Löschen auf. Die Aufbewahrungsfristen können im AMS frei und unabhängig voneinander für folgende Bereiche definiert werden:

- Frist für Ausbilderinnen und Ausbilder, Praxisbüro, Ausbildungsleitungen und Koordinatoren, Personalbetreuung, Ausbildungssteuerung, Fachlichen Leitstelle (im System: Mitarbeiter)
- Frist für Nachwuchskräfte (im System: Auszubildende)
- Frist für E-Mails
- Loginversuche im System

Für das AMS (als eine die Ausbildung begleitende Dokumentation) ist gemäß geltender Regularien (bspw. § 18 Abs. 1 APO-AllgVwD-Lg2Ea1) aktuell eine Löschfrist von fünf Jahren nach Beendigung der Ausbildung vorgesehen. Das Löschen der Konten der Ausbilderinnen und Ausbilder, Praxisbüro, Ausbildungsleitungen und Koordinatoren, Personalbetreuung, Ausbildungssteuerung und Fachlichen Leitstelle erfolgt nach Bekanntwerden über deren Ausscheiden aus der entsprechenden Tätigkeit bzw. wenn Einsatzorte den Ausbildungsleitungen und der Ausbildungssteuerung zurückmelden, dass sie nicht mehr geführt werden möchten.

Bei Erreichen der Löschfrist schlägt das AMS die zu löschenden User vor. Die Löschung muss dann durch die Beschäftigten der Fachlichen Leitstelle bzw. die Beschäftigten, die Aufgaben der Personalbetreuung wahrnehmen, angestoßen werden. Die Zuständigkeit verteilt sich voraussichtlich wie folgt:

Löschen von...	... erfolgt durch
Mitarbeiter	Beschäftigte der Fachlichen Leitstelle
E-Mails der Mitarbeiter	
Auszubildende	Beschäftigte, die Aufgaben in der Personalbetreuung übernehmen
E-Mails der Auszubildenden	

Hinweis:
- Die Löschfristen bezüglich der Mitarbeiter beginnen zum Ende des Jahres zu laufen
- E-Mails können bereits vor der Löschung der User gelöscht werden; wird ein User gelöscht, werden immer auch alle E-Mails gelöscht

4. Beschreibung der Berechtigungen innerhalb der Benutzergruppen[1]

Da der Zugriff auf ausgewählte Funktionalitäten und Daten nur bestimmten Benutzern zugänglich zu machen ist, kann eine Vielzahl an Berechtigungen genutzt werden. Für die vorgesehenen Benutzergruppen:

Benutzergruppe	Betroffene Benutzer
Modul: Ausbildung – Alle Rechte	• Beschäftigte der Fachlichen Leitstelle • Beschäftigte, die Aufgaben in der Personalbetreuung übernehmen, • Beschäftigte, die Aufgaben in der Ausbildungssteuerung übernehmen

[1] Stand 07.09.2022 in der Test-Umgebung

Modul: Ausbildung – Ausbildungsleitung	Die je nach Berufsbild zuständigen Ausbildungsleitungen
Modul: Ausbildung – Ausbildungs-verantwortliche Praxisstellen	• Ausbilderinnen und Ausbilder in den Behörden und Bezirksämtern • Koordinatoren in den Behörden und Bezirksämtern
Modul: Ausbildung – Auszubildende	Nachwuchskräfte der vom Personalamt angebotenen Ausbildungen
Modul: Ausbildung – Praxisbüro	Beschäftigte im Praxisbüro (Fachrichtung Soziale Arbeit)
Modul: Basis – Alle Rechte	Beschäftigte der Fachlichen Leitstelle
Modul: Basis – Import	Beschäftigte im Praxisbüro (Fachrichtung Soziale Arbeit)

sind die nachfolgend beschriebenen Berechtigungen vorgesehen. Ihnen ist eine Erläuterung beigefügt, um die Funktionen verständlicher und näher zu beschreiben.

Übersicht über die Benutzergruppen

Name	Beschreibung	Module
Ausbildung - Alle Rechte	Ausbildung - Alle Rechte	Ausbildung
Ausbildung - Ausbildungsleitung	Ausbildung - Ausbildungsleitung	Ausbildung
Ausbildung - Ausbildungsverantwortliche Praxisstellen	Ausbildung - Ausbilder Fachabteilung	Ausbildung
Ausbildung - Auszubildende	Ausbildung - Auszubildende	Ausbildung
Ausbildung - Praxisbüro	Einsatzorte bearbeiten	Ausbildung
Basis - Alle Rechte	Basis - Alle Rechte	Basis
Basis - Import	Basis - Import	Basis

Benutzergruppe: Ausbildung – Alle Rechte

Berechtigung	Beschreibung
Ausbilder-Auslastung	Ermöglicht den Zugriff auf den Menüpunkt "Einsätze > Prüfen > Ausbilder-Auslastung" (für die zentrale Rolle).
Azubikarten	Ermöglicht den Zugriff auf den Menüpunkt "Auszubildende" (für die zentrale Rolle).
Azubikarten - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Auszubildende (nicht möglich in Kombination mit der Light-Version)
Azubikarten - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Auszubildende (nicht möglich in Kombination mit der Light-Version)
Azubikartentypen	Ermöglicht das Bearbeiten von Azubikartentypen (Definition der gewünschten Zusatzfelder) und den Zugriff auf den Menüpunkt "Einstellungen > Ausbildung > Azubikartentypen" (für die zentrale Rolle).
Azubis - Alle bearbeiten	Lesender & schreibender Zugriff auf alle Auszubildenden.

Azubis - Foto ändern und entfernen	Ermöglicht das Ändern und Entfernen des Fotos des Azubis - ausgeschlossen in der Light-Version.
Azubis - Register Anmerkungen bearbeiten	Ermöglicht das Bearbeiten des Registers "Anmerkungen" der Azubikarte. Dezentral wird das Register eingeschränkt auf die Box "Hinweise Ausbildungsportal".
Azubis - Register Anmerkungen: Interne Anmerkungen bearbeiten	Ermöglicht das Bearbeiten der Box "interne Anmerkungen" im Register "Anmerkungen" der Azubikarte (in der zentralen Rolle).
Azubis - Register Auf einen Blick bearbeiten	Ermöglicht die Einsicht in das Register "Übersicht" der Azubikarte.
Azubis - Register Checkliste	Ermöglicht die Einsicht in das Register "Checkliste " der Azubikarte. Checklisteneinträge können je nach Konfiguration auf Zuständigkeit eingeschränkt sein.
Azubis - Register Checkliste - Bearbeiten	Ermöglicht das Bearbeiten des Registers "Checkliste " der Azubikarte. Checklisteneinträge können je nach Konfiguration auf Zuständigkeit eingeschränkt sein.
Azubis - Register Dateianhänge bearbeiten	Ermöglicht das Bearbeiten des Registers "Anhänge" der Azubikarte. Je nach Konfiguration stehen unterschiedliche Dateianhangkategorien zur Einsicht zur Verfügung.
Azubis - Register Einsätze bearbeiten	Ermöglicht das Bearbeiten des Registers "Einsätze" der Azubikarte.
Azubis - Register Korrespondenz bearbeiten	Ermöglicht das Bearbeiten des Registers "Kommunikation" der Azubikarte.
Azubis - Register Leistungen bearbeiten	Ermöglicht das Bearbeiten des Registers "Leistungen" der Azubikarte. Je nach Konfiguration im Leistungsprofil können Leistungsmerkmale sichtbar, verborgen oder bearbeitbar sein.
Azubis - Register pers. Daten bearbeiten	Ermöglicht das Bearbeiten des Registers "persönliche Daten" der Azubikarte.
Azubis - Register pers. Daten sehen	Ermöglicht die Einsicht in das Register "persönliche Daten" der Azubikarte.
Azubis - Register Persönliche Daten: Alter sehen	Ermöglicht die Anzeige des Alters auf der Azubikarte (persönliche Daten).
Azubis - Register Persönliche Daten: Bild sehen	Ermöglicht die Anzeige des Bildes auf der Azubikarte.
Azubis - Register Persönliche Daten: Familienstand sehen	Ermöglicht die Anzeige des Familienstands auf der Azubikarte (persönliche Daten).
Azubis - Register Persönliche Daten: Geburtsdatum sehen	Ermöglicht die Anzeige des Geburtsdatums auf der Azubikarte (persönliche Daten).
Azubis - Register Persönliche Daten: Schulname sehen	Ermöglicht die Anzeige des Schulnamens auf der Azubikarte (persönliche Daten).
Azubis - Register Planung bearbeiten	Ermöglicht das Bearbeiten des Registers "Planung" der Azubikarte.
Azubis - Register Planung sehen	Ermöglicht die Einsicht in das Register "Planung" der Azubikarte.
Azubis löschen	Ermöglicht das Löschen Von Auszubildenden im Menüpunkt "Auszubildende".
Berichtshefte	Ermöglicht die Bearbeitung von Berichtsheften (gem. der definierten Zuständigkeit und Workflow) und den Zugriff auf den Menüpunkt "Berichtshefte".
Berichtshefte - Definition	Ermöglicht die Bearbeitung von Berichtsheft-Definitionen nd den Zugriff auf den Menüpunkt "Einstellungen > Ausbildung > Berichtshefte" (in der zentralen Rolle).
Berichtshefte - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Berichtshefte
Berichtshefte - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Berichtshefte
Briefe	Ermöglicht den Zugriff auf den Menüpunkt "Korrespondenz > Briefe".
Briefe erstellen	Ermöglicht die Erstellung von neuen Briefen, u.a. im Menüpunkt "Korrespondenz > Briefe".
Checklisten - Bearbeiten (Auszubildende)	Ermöglicht die Bearbeitung von Checklisteneinträgen (in Bezug auf Auszubildende)

Checklisten - Sichtbarkeit der Einträge anpassen (zentral)	Ermöglicht das Bearbeiten der Sichtbarkeitseinstellungen für Checklisteneinträge (in der zentralen Rolle).
Checklisten (Auszubildende)	Ermöglicht das Bearbeiten von Checklisteneinträgen (in Bezug auf Auszubildende) und den Zugriff auf den Menüpunkt "Checklisten (Auszubildende). Die Sichtbarkeit der Checklisteneinträge wird ggf. auf den Zuständigkeitsbereich eingeschränkt.
Checklisten (Auszubildende) - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Checklisten (Auszubildende)
Checklisten (Auszubildende) - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Checklisten (Auszubildende)
Checklisten (Zentral)	Ermöglicht die Bearbeitung von Checklisteneinträgen und den Zugriff auf den Menüpunkt Checklisten (zentral) in der zentralen Rolle.
Checklisten (Zentral) - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Checklisten (Zentral)
Checklisten (Zentral) - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Checklisten (Zentral)
Checklisten: Uhrzeit letzte Bearbeitung sehen	Ermöglicht die Anzeige der Uhrzeit der letzten Bearbeitung in Checklisteineinträgen
Dashboard - Hinweis auf Geburtstage anzeigen	Ermöglicht den Hinweis auf Geburtstage von Azubis im Dashboard.
Einsatzdetails - Alle bearbeiten	Ermöglicht die Bearbeitung aller Einsätze für zentrale Mitarbeiter
Einsatzdetails - Alle sehen	Ermöglicht die Detailansicht aller Einsätze für zentrale Mitarbeiter
Einsätze - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Einsätze > Planen
Einsätze - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Einsätze > Planen
Einsätze veröffentlichen	Ermöglicht das Veröffentlichen von Einsätzen und den Zugriff auf den Menüpunkt "Einsätze > Veröffentlichen" (für die zentrale Rolle).
Einsätze versenden	Ermöglicht das Versenden von Einsätzen und den Zugriff auf den Menüpunkt "Einsätze > Versenden" (für die zentrale Rolle).
Einsätze vorschlagen	Ermöglicht das Durchführen einer automatischen Einsatzplanung und den Zugriff auf den Menüpunkt Einsätze > Vorschlagen (in der zentralen Rolle).
Einsatzort-Auslastung	Ermöglicht den Zugriff auf den Menüpunkt "Einsätze > Prüfen > Einsatzort-Auslastung" (für die zentrale Rolle).
Einsatzperspektive Funktionen	Ermöglicht das Erstellen von neuen Einsätzen, u.a. im Menüpunkt "Einsätze > Planen".
Einsatzperspektive Navigation	Ermöglicht den Zugriff auf den Menüpunkt "Einsätze > Planen".
Einstellungen - Azubitypen	Ermöglicht das Bearbeiten von Azubitypen und den Zugriff auf den Menüpunkt "Einstellungen > Personen und Orte > Azubitypen" (für die zentrale Rolle).
Einstellungen - Berufsbilder	Ermöglicht das Bearbeiten von Berufsbildern und den Zugriff auf den Menüpunkt "Einstellungen > Ausbildung > Berufsbilder" (für die zentrale Rolle).
Einstellungen - Berufsschulen	Ermöglicht das Bearbeiten von Berufsschulen und den Zugriff auf den Menüpunkt "Einstellungen > Ausbildung > Berufsschulen" (für die zentrale Rolle).
Einstellungen - Briefvorlagen	Ermöglicht das Bearbeiten von Brief-Vorlagen und den Zugriff auf den Menüpunkt "Einstellungen > Kommunikation > Brief-Vorlagen" (für die zentrale Rolle).
Einstellungen - Checklistenkategorien	Ermöglicht das Bearbeiten von Checklistenkategorien und den Zugriff auf den Menüpunkt "Einstellungen > Checklisten > Checklistenkategorien" (für die zentrale Rolle).
Einstellungen - Checklistenvorlagen	Ermöglicht das Bearbeiten von Checklistenvorlagen und den Zugriff auf den Menüpunkt "Einstellungen > Checklisten > Checklistenvorlagen" (für die zentrale Rolle).
Einstellungen - Dateianhangkategorien	Ermöglicht die Bearbeitung von Dateianhangkategorien und den Zugriff auf den Menüpunkt Einstellungen > Ausbildung > Dateianhangkategorien (in der zentralen Rolle).
Einstellungen - Einsatzorte	Ermöglicht das Bearbeiten von Einsatzorten und den Zugriff auf den Menüpunkt "Einstellungen > Leistungen > Einsatzorte" (für die zentrale Rolle).

Einstellungen - Einsatzortkategorien	Ermöglicht das Bearbeiten von Einsatzortkategorien und den Zugriff auf den Menüpunkt Einstellungen > Personen und Orte > Einsatzortkategorien(in der zentralen Rolle).
Einstellungen - E-Mail-Vorlagen	Ermöglicht das Bearbeiten von Brief-Vorlagen und den Zugriff auf den Menüpunkt "Einstellungen > Kommunikation > Brief-Vorlagen" (für die zentrale Rolle).
Einstellungen - Feedbackvorlagen	Ermöglicht das Bearbeiten von Feedbackvorlagen und den Zugriff auf den Menüpunkt "Einstellungen > Leistungen > Feedbackvorlagen" (für die zentrale Rolle).
Einstellungen - Gruppen	Ermöglicht das Bearbeiten von Gruppen und den Zugriff auf den Menüpunkt "Einstellungen > Personen und Orte >Gruppen" (für die zentrale Rolle).
Einstellungen - IHKs/HWKs	Ermöglicht das Bearbeiten von IHKs/HWKs und den Zugriff auf den Menüpunkt "Einstellungen > Ausbildung > IHKs/HWKs" (für die zentrale Rolle).
Einstellungen - Import	Ermöglicht das Importieren von Daten und den Zugriff auf den Menüpunkt "Synchronisation > weitere Module" (für die zentrale Rolle). Bitte nur nach Absprache mit GuideCom verwenden.
Einstellungen - Leistungsprofile	Ermöglicht das Bearbeiten von Leistungsprofilen und den Zugriff auf den Menüpunkt "Einstellungen > Leistungen > Leistungsprofile" (für die zentrale Rolle).
Einstellungen - Lerninhalte	Ermöglicht das Bearbeiten von Lerninhalten und den Zugriff auf den Menüpunkt "Einstellungen > Lerninhalte und -ziele > Lerninhalte" (für die zentrale Rolle).
Einstellungen - Lernziele	Ermöglicht die Verwaltung und Bearbeitung von Lernzielen und den Zugriff auf den Menüpunkt Einstellungen > Lerninhalte und -ziele > Lernziele (in der zentralen Rolle).
Einstellungen - Lernzielkategorien	Ermöglicht die Verwaltung und Bearbeitung von Lernzielkategorien und den Zugriff auf den Menüpunkt Einstellungen > Lerninhalte und -ziele > Lernzielkategorien (in der zentralen Rolle).
Einstellungen - Mitarbeiter	Ermöglicht die Übernahme von Mitarbeitern als neue Azubis und den Zugriff auf den Menüpunkt "Einstellungen > Personen und Orte > Mitarbeiter" (für die zentrale Rolle).
Einstellungen - Nach Ausbildung	Ermöglicht das Bearbeiten von Auswahlmöglichkeiten für das Feld "nach Ausbildung" auf der Azubikarte und den Zugriff auf den Menüpunkt "Einstellungen > Ausbildung > Nach Ausbildung" (für die zentrale Rolle).
Einstellungen - Neue Azubis	Ermöglicht die Übernahme neuer Azubis und den Zugriff auf den Menüpunkt "Einstellungen > Personen und Orte > Neue Azubis" (für die zentrale Rolle).
Einstellungen - Regionen	Ermöglicht das Bearbeiten von Regionen und den Zugriff auf den Menüpunkt "Einstellungen > Personen und Orte > Regionen" (für die zentrale Rolle).
Einstellungen - Skalen	Ermöglicht das Bearbeiten von Skalen und den Zugriff auf den Menüpunkt "Einstellungen > Leistungen > Skalen" (für die zentrale Rolle).
Einstellungen - Starthelfer-Management	Ermöglicht das Bearbeiten der Starthelfer-Einstellungen im Menüpunkt Einstellungen > Wartung (in der zentralen Rolle).
Einstellungen - Synchronisationsprotokoll	Ermöglicht das Anstoßen der Synchronisation mit weiteren Modulen und den Zugriff auf den Menüpunkt "Synchronisation > weitere Module" (für die zentrale Rolle).
Einstellungen - Unternehmen	Ermöglicht das Bearbeiten von Unternehmen und den Zugriff auf den Menüpunkt "Einstellungen > Ausbildung > Unternehmen" (für die zentrale Rolle).
Einstellungen - Zusatzfelder	Ermöglicht das Bearbeiten von Zusatzfeldern für die Azubikarte und den Zugriff auf den Menüpunkt "Einstellungen > Ausbildung > Zusatzfelder" (für die zentrale Rolle).
Einstellungen - Zusatzfeldkategorien	Ermöglicht das Bearbeiten von Zusatzfeldkategorien und den Zugriff auf den Menüpunkt "Einstellungen > Ausbildung > Zusatzfeldkategorien" (für die zentrale Rolle).

E-Mails	Ermöglicht den Zugriff auf den Menüpunkt "Korrespondenz > E-Mails".
E-Mails erstellen	Ermöglicht die Erstellung von neuen E-Mails, u.a. im Menüpunkt "Korrespondenz > E-Mails".
Feedbacks - Delegieren	Ermöglicht das Delegieren von Feedbacks an andere User im Menüpunkt Feedbacks > Nachverfolgen.
Feedbacks (Einsehen) - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Feedbacks > Einsehen
Feedbacks (Einsehen): Einsatzort-Feedback einsehen	Ermöglicht das Einsehen des Einsatzort-Feedbacks im Menüpunkt Feedbacks > Nachverfolgen (sofern die Einsicht in der Feedbackvorlage nicht weiter eingeschränkt wird).
Feedbacks (Nachverfolgen) - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Feedbacks > Nachverfolgen
Feedbacks einsehen	Ermöglicht das Einsehen von abgeschlossenen Feedbacks und den Zugriff auf den Menüpunkt "Feedbacks > einsehen" (in der zentralen Rolle). Die Ansicht wird eingeschränkt auf die Azubimenge, für die der Benutzer zuständig/berechtigt ist.
Feedbacks nachverfolgen	Ermöglicht das Nachverfolgen und Bearbeiten von offenen Feedbacks und den Zugriff auf den Menüpunkt "Feedbacks > nachverfolgen" (in der zentralen Rolle). Die Ansicht wird eingeschränkt auf die Azubimenge, für die der Benutzer zuständig/berechtigt ist.
Fehlende Lerninhalte	Ermöglicht den Zugriff auf den Menüpunkt "Einsätze > Prüfen > Fehlende Lerninhalte" (für die zentrale Rolle).
Gruppeneinsätze planen	Ermöglicht das Planen von Gruppeneinsätzen (für die zentrale Rolle).
Import der Installationstabelle	Ermöglicht das Importieren einer Installationstabelle unter Einstellungen > Synchronisation > Weitere Module (in der zentralen Rolle)
Importierte Abwesenheiten anzeigen (Kalender)	Ermöglicht die Anzeige importierter Abwesenheiten in der Kalender-Ansicht der Einsatzplanung
Importierte Abwesenheiten anzeigen (Tabelle)	Ermöglicht die Anzeige importierter Abwesenheiten in der Tabelle der Einsatzplanung und der Einsatzübersicht auf der Azubikarte
Infoportal	Ermöglicht den Zugriff auf den Menüpunkt "Info".
Infoportal: Einträge anlegen	Ermöglicht das Bearbeiten von Einträgen für den Menüpunkt "Info" und den Zugriff auf den Menüpunkt Einstellungen > Infos > Inhalte (in der zentralen Rolle).
Infoportal: Eintrag-Kategorien	Ermöglicht das Bearbeiten von Einträgen für den Menüpunkt "Info" und den Zugriff auf den Menüpunkt Einstellungen > Infos > Kategorien (in der zentralen Rolle).
Lernmedien in der Navigation	Ermöglicht die Bearbeitung von Lernmedien und den Zugriff auf den Menüpunkt Lernmedien (in der zentralen Rolle oder als Auszubildender).
Lernziele	Ermöglicht das Bearbeiten von Lernzielen und den Zugriff auf den Menüpunkt "Lernziele". Die Sichtbarkeit der Lernziele wird ggf. auf den Zuständigkeitsbereich eingeschränkt.
Lernziele - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Lernziele
Lernziele - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Lernziele
Personenbezogene Daten	Ermöglicht die Verwaltung der Aufbewahrungsfristen sowie die Löschung personenbezogener Daten inkl. Protokollierung.
Rolle Mitarbeiter zentral	Rolle
Veröffentlichte Einsätze	Ermöglicht den Zugriff auf den Menüpunkt "Einsatzplan" (für die dezentrale Rolle).
Veröffentlichte Einsätze - Adress-Details zum Einsatzort anzeigen	Zeigt im Einsatz-Detail die Adresse des Einsatzortes an
Veröffentlichte Einsätze - Alle sehen	Ermöglicht die Sicht auf Einsätze aller Azubis.
Veröffentlichte Einsätze - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Einsatzplan
Veröffentlichte Einsätze - Lernziele anzeigen	Ermöglicht die Ansicht der Lernziele im Einsatz-Detail
Veröffentlichte Einsätze - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Einsatzplan

Wartung - Benutzereinstellungen zurücksetzen	Ermöglicht das Zurücksetzen von Benutzereinstellungen. Wird ggfs. in Supportfällen benötigt.
Wartung - Sperren verwalten	Ermöglicht die Verwaltung gesperrter Objekte ("Sperren"). Diese können mit diesem Recht wieder freigegeben werden.
Zugriff	Zugriff auf die Anwendung

Benutzergruppe: Ausbildung – Ausbildungsleitung

Berechtigung	Beschreibung
Azubis - Foto ändern und entfernen	Ermöglicht das Ändern und Entfernen des Fotos des Azubis - ausgeschlossen in der Light-Version.
Azubis - Register Dateianhänge bearbeiten	Ermöglicht das Bearbeiten des Registers "Anhänge" der Azubikarte. Je nach Konfiguration stehen unterschiedliche Dateianhangkategorien zur Einsicht zur Verfügung.
Azubis - Register Anmerkungen bearbeiten (Unternehmensverantwortlicher)	Ermöglicht das Bearbeiten des Registers "Anmerkungen" der Azubikarten als Unternehmensverantwortlicher. Dezentral wird das Register eingeschränkt auf die Box "Hinweise Ausbildungsportal".
Azubis - Register Checkliste - Bearbeiten (Unternehmensverantwortlicher)	Ermöglicht das Bearbeiten des Registers "Checkliste " der Azubikarten als Unternehmensverantwortlicher. Checklisteneinträge können je nach Konfiguration auf weitere Zuständigkeiten eingeschränkt sein.
Azubis - Register Einsätze bearbeiten (Unternehmensverantwortlicher)	Ermöglicht das Bearbeiten des Registers "Einsätze" der Azubikarten als Unternehmensverantwortlicher.
Azubis - Register Korrespondenz bearbeiten (Unternehmensverantwortlicher)	Ermöglicht das Bearbeiten des Registers "Kommunikation" der Azubikarten als Unternehmensverantwortlicher.
Azubis - Register pers. Daten bearbeiten (Unternehmensverantwortlicher)	Ermöglicht das Bearbeiten des Registers "persönliche Daten" der Azubikarten als Unternehmensverantwortlicher.
Azubis - Register Planung bearbeiten (Unternehmensverantwortlicher)	Ermöglicht das Bearbeiten des Registers "Planung" der Azubikarten als Unternehmensverantwortlicher.
Einstellungen - Einsatzorte	Ermöglicht das Bearbeiten von Einsatzorten und den Zugriff auf den Menüpunkt "Einstellungen > Leistungen > Einsatzorte" (für die zentrale Rolle).
Einstellungen - Einsatzortkategorien	Ermöglicht das Bearbeiten von Einsatzortkategorien und den Zugriff auf den Menüpunkt Einstellungen > Personen und Orte > Einsatzortkategorien(in der zentralen Rolle).
Infoportal: Einträge anlegen	Ermöglicht das Bearbeiten von Einträgen für den Menüpunkt "Info" und den Zugriff auf den Menüpunkt Einstellungen > Infos > Inhalte (in der zentralen Rolle).
Infoportal: Eintrag-Kategorien	Ermöglicht das Bearbeiten von Einträgen für den Menüpunkt "Info" und den Zugriff auf den Menüpunkt Einstellungen > Infos > Kategorien (in der zentralen Rolle).
Lernziele	Ermöglicht das Bearbeiten von Lernzielen und den Zugriff auf den Menüpunkt "Lernziele". Die Sichtbarkeit der Lernziele wird ggf. auf den Zuständigkeitsbereich eingeschränkt.
Einsätze vorschlagen	Ermöglicht das Durchführen einer automatischen Einsatzplanung und den Zugriff auf den Menüpunkt Einsätze > Vorschlagen (in der zentralen Rolle).
Feedbacks einsehen	Ermöglicht das Einsehen von abgeschlossenen Feedbacks und den Zugriff auf den Menüpunkt "Feedbacks > einsehen" (in der zentralen Rolle). Die Ansicht wird eingeschränkt auf die Azubimenge, für die der Benutzer zuständig/berechtigt ist.
Einsatzperspektive Funktionen	Ermöglicht das Erstellen von neuen Einsätzen, u.a. im Menüpunkt "Einsätze > Planen".
Feedbacks nachverfolgen	Ermöglicht das Nachverfolgen und Bearbeiten von offenen Feedbacks und den Zugriff auf den Menüpunkt "Feedbacks > nachverfolgen" (in der

	zentralen Rolle). Die Ansicht wird eingeschränkt auf die Azubimenge, für die der Benutzer zuständig/berechtigt ist.
Gruppeneinsätze planen	Ermöglicht das Planen von Gruppeneinsätzen (für die zentrale Rolle).
Einsätze veröffentlichen	Ermöglicht das Veröffentlichen von Einsätzen und den Zugriff auf den Menüpunkt "Einsätze > Veröffentlichen" (für die zentrale Rolle).
Einsätze versenden	Ermöglicht das Versenden von Einsätzen und den Zugriff auf den Menüpunkt "Einsätze > Versenden" (für die zentrale Rolle).
Azubikarten - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Auszubildende (nicht möglich in Kombination mit der Light-Version)
Berichtshefte - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Berichtshefte
Einsätze - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Einsätze > Planen
Veröffentlichte Einsätze - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Einsatzplan
Lernziele - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Lernziele
Dashboard - Hinweis auf Geburtstage anzeigen	Ermöglicht den Hinweis auf Geburtstage von Azubis im Dashboard.
Azubikarten - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Auszubildende (nicht möglich in Kombination mit der Light-Version)
Berichtshefte - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Berichtshefte
Einsätze - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Einsätze > Planen
Veröffentlichte Einsätze - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Einsatzplan
Feedbacks (Einsehen) - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Feedbacks > Einsehen
Feedbacks (Nachverfolgen) - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Feedbacks > Nachverfolgen
Lernziele - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Lernziele
Infoportal	Ermöglicht den Zugriff auf den Menüpunkt "Info".
Azubikarten	Ermöglicht den Zugriff auf den Menüpunkt "Auszubildende" (für die zentrale Rolle).
Einsatzperspektive Navigation	Ermöglicht den Zugriff auf den Menüpunkt "Einsätze > Planen".
Fehlende Lerninhalte	Ermöglicht den Zugriff auf den Menüpunkt "Einsätze > Prüfen > Fehlende Lerninhalte" (für die zentrale Rolle).
Briefe	Ermöglicht den Zugriff auf den Menüpunkt "Korrespondenz > Briefe".
E-Mails	Ermöglicht den Zugriff auf den Menüpunkt "Korrespondenz > E-Mails".
Veröffentlichte Einsätze - Lernziele anzeigen	Ermöglicht die Ansicht der Lernziele im Einsatz-Detail
Azubis - Register Persönliche Daten: Alter sehen	Ermöglicht die Anzeige des Alters auf der Azubikarte (persönliche Daten).
Azubis - Register Persönliche Daten: Bild sehen	Ermöglicht die Anzeige des Bildes auf der Azubikarte.
Importierte Abwesenheiten anzeigen (Kalender)	Ermöglicht die Anzeige importierter Abwesenheiten in der Kalender-Ansicht der Einsatzplanung
Importierte Abwesenheiten anzeigen (Tabelle)	Ermöglicht die Anzeige importierter Abwesenheiten in der Tabelle der Einsatzplanung und der Einsatzübersicht auf der Azubikarte
Einsatzdetails - Als Unternehmensverantwortlicher bearbeiten	Ermöglicht die Bearbeitung aller Einsätze als Unternehmensverantwortlicher für zentrale Mitarbeiter
Einsatzdetails - Alle bearbeiten	Ermöglicht die Bearbeitung aller Einsätze für zentrale Mitarbeiter
Berichtshefte	Ermöglicht die Bearbeitung von Berichtsheften (gem. der definierten Zuständigkeit und Workflow) und den Zugriff auf den Menüpunkt "Berichtshefte".
Lernmedien in der Navigation	Ermöglicht die Bearbeitung von Lernmedien und den Zugriff auf den Menüpunkt Lernmedien (in der zentralen Rolle oder als Auszubildender).
Azubis - Register Auf einen Blick bearbeiten (Unternehmensverantwortlicher)	Ermöglicht die Einsicht in das Register "Übersicht" der Azubikarte.

Briefe erstellen	Ermöglicht die Erstellung von neuen Briefen, u.a. im Menüpunkt "Korrespondenz > Briefe".
E-Mails erstellen	Ermöglicht die Erstellung von neuen E-Mails, u.a. im Menüpunkt "Korrespondenz > E-Mails".
Veröffentlichte Einsätze - Alle sehen	Ermöglicht die Sicht auf Einsätze aller Azubis.
Azubis - Als Unternehmensverantwortlicher bearbeiten	Grenzt die Azubi-Menge diverser Menüpunkte auf die Zuständigkeit als "Unternehmensverantwortlicher" ein und ermöglicht die Bearbeitung in die Azubikarten dieser Azubis.
Rolle Mitarbeiter zentral	Rolle
Veröffentlichte Einsätze - Adress-Details zum Einsatzort anzeigen	Zeigt im Einsatz-Detail die Adresse des Einsatzortes an
Zugriff	Zugriff auf die Anwendung

Benutzergruppe: Ausbildung – Ausbildungsverantwortliche Praxisstellen

Berechtigung	Beschreibung
Azubikarte dezentral für Verantwortliche	Ermöglicht den Zugriff auf den Menüpunkt "Auszubildende" (für die dezentrale Rolle).
Azubikarten	Ermöglicht den Zugriff auf den Menüpunkt "Auszubildende" (für die zentrale Rolle).
Azubikarten - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Auszubildende (nicht möglich in Kombination mit der Light-Version)
Azubikarten - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Auszubildende (nicht möglich in Kombination mit der Light-Version)
Azubis - Als Einsatzortverantwortlicher sehen	Grenzt die Azubi-Menge diverser Menüpunkte auf die Zuständigkeit als "Einsatzortverantwortlicher " ein und ermöglicht die Einsicht in die Azubikarten dieser Azubis.
Azubis - Register Anmerkungen sehen (Einsatzortverantwortlicher)	Ermöglicht die Einsicht in das Register "Anmerkungen" der Azubikarten als Einsatzortverantwortlicher. Dezentral wird das Register eingeschränkt auf die Box "Hinweise Ausbildungsportal".
Azubis - Register Checkliste (Einsatzortverantwortlicher)	Ermöglicht die Einsicht in das Register "Checkliste " der Azubikarten als Einsatzortverantwortlicher. Checklisteneinträge können je nach Konfiguration auf weitere Zuständigkeiten eingeschränkt sein.
Azubis - Register Einsätze sehen (Einsatzortverantwortlicher)	Ermöglicht die Einsicht in das Register "Einsätze" der Azubikarten als Einsatzortverantwortlicher.
Azubis - Register Leistungen bearbeiten (Einsatzortverantwortlicher)	Ermöglicht das Bearbeiten des Registers "Leistungen" der Azubikarten als Einsatzortverantwortlicher. Je nach Konfiguration im Leistungsprofil können Leistungsmerkmale sichtbar, verborgen oder bearbeitbar sein.
Azubis - Register Leistungen sehen (Einsatzortverantwortlicher)	Ermöglicht die Einsicht in das Register "Leistungen" der Azubikarten als Einsatzortverantwortlicher. Je nach Konfiguration im Leistungsprofil können Leistungsmerkmale sichtbar, verborgen oder bearbeitbar sein.
Azubis - Register pers. Daten sehen (Einsatzortverantwortlicher)	Ermöglicht die Einsicht in das Register "persönliche Daten" der Azubikarten als Einsatzortverantwortlicher.
Azubis - Register Persönliche Daten: Alter sehen	Ermöglicht die Anzeige des Alters auf der Azubikarte (persönliche Daten).
Azubis - Register Persönliche Daten: Bild sehen	Ermöglicht die Anzeige des Bildes auf der Azubikarte.
Azubis - Register Planung sehen (Einsatzortverantwortlicher)	Ermöglicht die Einsicht in das Register "Planung" der Azubikarten als Einsatzortverantwortlicher.
Berichtshefte	Ermöglicht die Bearbeitung von Berichtsheften (gem. der definierten Zuständigkeit und Workflow) und den Zugriff auf den Menüpunkt "Berichtshefte".
Briefe erstellen	Ermöglicht die Erstellung von neuen Briefen, u.a. im Menüpunkt "Korrespondenz > Briefe".
Einsatzdetails - Als Einsatzortverantwortlicher sehen	Ermöglicht die Detailansicht aller Einsätze als Einsatzortverantwortlicher für zentrale Mitarbeiter

Einsatzperspektive Funktionen	Ermöglicht das Erstellen von neuen Einsätzen, u.a. im Menüpunkt "Einsätze > Planen".
E-Mails	Ermöglicht den Zugriff auf den Menüpunkt "Korrespondenz > E-Mails".
Feedbacks einsehen (dezentral)	Ermöglicht das Einsehen von abgeschlossenen Feedbacks und den Zugriff auf den Menüpunkt "Feedbacks > einsehen" (in der dezentralen Rolle). Die Ansicht wird eingeschränkt auf die Feedbacks, für die der Benutzer zuständig/berechtigt ist.
Feedbacks nachverfolgen (dezentral)	Ermöglicht das Nachverfolgen und Bearbeiten von offenen Feedbacks und den Zugriff auf den Menüpunkt "Feedbacks > nachverfolgen" (in der zentralen Rolle). Die Ansicht wird eingeschränkt auf die Feedbacks, für die der Benutzer zuständig/berechtigt ist.
Gruppeneinsätze planen	Ermöglicht das Planen von Gruppeneinsätzen (für die zentrale Rolle).
Infoportal	Ermöglicht den Zugriff auf den Menüpunkt "Info".
Lernmedien in der Navigation	Ermöglicht die Bearbeitung von Lernmedien und den Zugriff auf den Menüpunkt Lernmedien (in der zentralen Rolle oder als Auszubildender).
Lernziele	Ermöglicht das Bearbeiten von Lernzielen und den Zugriff auf den Menüpunkt "Lernziele". Die Sichtbarkeit der Lernziele wird ggf. auf den Zuständigkeitsbereich eingeschränkt.
Rolle Mitarbeiter dezentral	Rolle
Veröffentlichte Einsätze	Ermöglicht den Zugriff auf den Menüpunkt "Einsatzplan" (für die dezentrale Rolle).
Veröffentlichte Einsätze - Adress-Details zum Einsatzort anzeigen	Zeigt im Einsatz-Detail die Adresse des Einsatzortes an
Veröffentlichte Einsätze - Als Einsatzortverantwortlicher sehen	Schränkt die Sicht auf Einsätze auf die Zuständigkeit als Einsatzortverantwortlicher ein (dezentrale Rolle).
Zugriff	Zugriff auf die Anwendung

Benutzergruppe: Ausbildung – Auszubildende

Berechtigung	Beschreibung
Azubikarte dezentral für Auszubildende	Ermöglicht den Zugriff auf den Menüpunkt "meine Azubikarte" (für die Rolle "Auszubildender").
Azubikarte dezentral: Feld "E-Mail (privat)" bearbeiten	Ermöglicht die Bearbeitung des Feldes "E-Mail (privat)" auf der Azubikarte (in der dezentralen Rolle).
Azubikarte dezentral: Feld "Telefon (privat)" bearbeiten	Ermöglicht die Bearbeitung des Feldes "Telefon (privat)" auf der Azubikarte (in der dezentralen Rolle).
Azubikarte dezentral: Felder für Bankverbindung anzeigen	Ermöglicht die Anzeige der Felder für die Bankverbindung auf der Azubikarte.
Azubis - Berufsschule-Box sehen (dezentral)	Ergänzt die Azubikarten um die Berufsschul-Box (in der dezentralen Rolle).
Azubis - Definierbare Felder sehen (dezentral)	Sichtbarkeit von Zusatzfeldern auf den Azubikarten (Reiter persönliche Daten) innerhalb des Zuständigkeitsbereichs. Je nach Konfiguration können Felder verborgen, sichtbar oder bearbeitbar sein.
Azubis - Foto ändern und entfernen	Ermöglicht das Ändern und Entfernen des Fotos des Azubis - ausgeschlossen in der Light-Version.
Azubis - Register Checkliste	Ermöglicht die Einsicht in das Register "Checkliste " der Azubikarte. Checklisteneinträge können je nach Konfiguration auf Zuständigkeit eingeschränkt sein.
Azubis - Register Checkliste - Bearbeiten	Ermöglicht das Bearbeiten des Registers "Checkliste " der Azubikarte. Checklisteneinträge können je nach Konfiguration auf Zuständigkeit eingeschränkt sein.
Azubis - Register Dateianhänge bearbeiten	Ermöglicht das Bearbeiten des Registers "Anhänge" der Azubikarte. Je nach Konfiguration stehen unterschiedliche Dateianhangkategorien zur Einsicht zur Verfügung.
Azubis - Register Einsätze sehen	Ermöglicht die Einsicht in das Register "Einsätze" der Azubikarte.
Azubis - Register Einsatztage sehen	Ermöglicht die Einsicht in das Register "Einsatztage" der Azubikarte.

Azubis - Register Korrespondenz sehen	Ermöglicht die Einsicht in das Register "Kommunikation" der Azubikarte.
Azubis - Register Leistungen bearbeiten	Ermöglicht das Bearbeiten des Registers "Leistungen" der Azubikarte. Je nach Konfiguration im Leistungsprofil können Leistungsmerkmale sichtbar, verborgen oder bearbeitbar sein.
Azubis - Register pers. Daten sehen	Ermöglicht die Einsicht in das Register "persönliche Daten" der Azubikarte.
Azubis - Register Persönliche Daten: Alter sehen	Ermöglicht die Anzeige des Alters auf der Azubikarte (persönliche Daten).
Azubis - Register Persönliche Daten: Bild sehen	Ermöglicht die Anzeige des Bildes auf der Azubikarte.
Azubis - Register Persönliche Daten: Familienstand sehen	Ermöglicht die Anzeige des Familienstands auf der Azubikarte (persönliche Daten).
Azubis - Register Persönliche Daten: Geburtsdatum sehen	Ermöglicht die Anzeige des Geburtsdatums auf der Azubikarte (persönliche Daten).
Azubis - Register Persönliche Daten: Schulname sehen	Ermöglicht die Anzeige des Schulnamens auf der Azubikarte (persönliche Daten).
Azubis - Register Planung sehen	Ermöglicht die Einsicht in das Register "Planung" der Azubikarte.
Berichtshefte	Ermöglicht die Bearbeitung von Berichtsheften (gem. der definierten Zuständigkeit und Workflow) und den Zugriff auf den Menüpunkt "Berichtshefte".
Berichtshefte - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Berichtshefte
Feedbacks einsehen (dezentral)	Ermöglicht das Einsehen von abgeschlossenen Feedbacks und den Zugriff auf den Menüpunkt "Feedbacks > einsehen" (in der dezentralen Rolle). Die Ansicht wird eingeschränkt auf die Feedbacks, für die der Benutzer zuständig/berechtigt ist.
Feedbacks nachverfolgen (dezentral)	Ermöglicht das Nachverfolgen und Bearbeiten von offenen Feedbacks und den Zugriff auf den Menüpunkt "Feedbacks > nachverfolgen" (in der zentralen Rolle). Die Ansicht wird eingeschränkt auf die Feedbacks, für die der Benutzer zuständig/berechtigt ist.
Infoportal	Ermöglicht den Zugriff auf den Menüpunkt "Info".
Lernmedien in der Navigation	Ermöglicht die Bearbeitung von Lernmedien und den Zugriff auf den Menüpunkt Lernmedien (in der zentralen Rolle oder als Auszubildender).
Lernziele	Ermöglicht das Bearbeiten von Lernzielen und den Zugriff auf den Menüpunkt "Lernziele". Die Sichtbarkeit der Lernziele wird ggf. auf den Zuständigkeitsbereich eingeschränkt.
Lernziele - Excel-Export	Ermöglicht den Excel-Export im Menüpunkt Lernziele
Lernziele - PDF-Export	Ermöglicht den PDF-Export im Menüpunkt Lernziele
Rolle Auszubildender	Rolle
Veröffentlichte Einsätze	Ermöglicht den Zugriff auf den Menüpunkt "Einsatzplan" (für die dezentrale Rolle).
Veröffentlichte Einsätze - Adress-Details zum Einsatzort anzeigen	Zeigt im Einsatz-Detail die Adresse des Einsatzortes an
Veröffentlichte Einsätze - Als Azubi sehen	Schränkt die Sicht auf Einsätze auf die eigenen ein (Rolle Auszubildender).
Veröffentlichte Einsätze - Lernziele anzeigen	Ermöglicht die Ansicht der Lernziele im Einsatz-Detail
Zugriff	Zugriff auf die Anwendung

Benutzergruppe: Ausbildung – Praxisbüro

Berechtigung	Beschreibung
Einstellungen - Einsatzorte	Ermöglicht das Bearbeiten von Einsatzorten und den Zugriff auf den Menüpunkt "Einstellungen > Leistungen > Einsatzorte" (für die zentrale Rolle).
Rolle Mitarbeiter zentral	Rolle

Veröffentlichte Einsätze - Adress-Details zum Einsatzort anzeigen	Zeigt im Einsatz-Detail die Adresse des Einsatzortes an
Zugriff	Zugriff auf die Anwendung

Benutzergruppe: Basis – Alle Rechte

Berechtigung	Beschreibung
Benutzereinstellungen zurücksetzen	Ermöglicht das Zurücksetzen von Benutzereinstellungen. Wird ggfs. in Supportfällen benötigt.
Zeitscheiben	Ermöglicht die Aktualisierung und Generierung von sog. Zeitscheiben, die als Grundlage für das Reporting im Sextant verwendet werden.
Import durchführen	Ermöglicht die Durchführung der konfigurierten Importe, wie bspw. Stammdaten, Entgeltabrechnungen und weiteres.
Performance-Check	Ermöglicht die Durchführung des Performance-Checks. Bitte nur nach Rücksprache mit GuideCom durchführen.
Technische Protokolle	Ermöglicht die Einsicht in die technischen Protokolle zur Analyse.
Funktionspruefung	Ermöglicht die Initiierung einiger Testszenarien, wie bspw. Versendung von E-Mails oder Aufruf von Fehlerseiten.
Import einstellen	Ermöglicht die Konfiguration der Import-Einstellungen.
Auswertungsdaten	Ermöglicht die Konfiguration von Datenwürfeln, deren Dimensionen und Kennzahlen als Grundlage für das Reporting im Sextant verwendet werden.
Benutzergruppen	Ermöglicht die Verwaltung der Berechtigungen in Magellan durch Zuordnung von Berechtigungen und Benutzern zu Benutzergruppen.
Personen	Ermöglicht die Verwaltung der Stammdaten von Personen. Je nach Konfiguration können diese bearbeitet oder angesehen werden.
Sperren verwalten	Ermöglicht die Verwaltung gesperrter Objekte ("Sperren"). Diese können mit diesem Recht wieder freigegeben werden.
Externe Benutzer	Ermöglicht die Verwaltung von externen Benutzern.
Interne Benutzer	Ermöglicht die Verwaltung von internen Benutzern.
OE-Kategorien	Ermöglicht die Verwaltung von OE-Kategorien (Clusterung von Organisationseinheiten). Je nach Konfiguration können diese bearbeitet oder angesehen werden.
Organisationseinheiten	Ermöglicht die Verwaltung von Organisationseinheiten. Je nach Konfiguration können diese bearbeitet oder angesehen werden.
Qualifikationen	Ermöglicht die Verwaltung von Qualifikationen. Je nach Konfiguration können diese bearbeitet oder angesehen werden.
Qualifikations-Kategorien	Ermöglicht die Verwaltung von Qualifikations-Kategorien (Clusterung von Qualifikationen). Je nach Konfiguration können diese bearbeitet oder angesehen werden.
Schulabschlüsse	Ermöglicht die Verwaltung von Schulabschlüssen. Je nach Konfiguration können diese bearbeitet oder angesehen werden.
Zugriff	Zugriff auf die Anwendung
Funktion "Benutzerwechsler"	Nur in der Test-Umgebung möglich – Wechselt die Ansichten zwischen verschiedenen Benutzerkonten und Rollen.

Benutzergruppe: Basis – Import

Berechtigung	Beschreibung
Import durchführen	Ermöglicht die Durchführung der konfigurierten Importe, wie bspw. Stammdaten, Entgeltabrechnungen und weiteres.
Import einstellen	Ermöglicht die Konfiguration der Import-Einstellungen.
Zugriff	Zugriff auf die Anwendung

Protokollierungs- und Infrastrukturkonzept für das IT-Verfahren

„Ausbildungsmanagement-System (AMS)“

1. Grundlegendes zur Protokollierung

Die Protokollierung im AMS erfolgt sowohl auf System- als auch auf fachlicher Ebene. Die Protokollierung auf Systemebene dient vor allem zur Überwachung des Systembetriebs, während sich die fachliche Protokollierung auf die eingesetzten Module „Basis“ und „Young Talents“ des eingesetzten Produkts Magellan bezieht.

1.1 Datenminimierung

Um dem Prinzip der Datenvermeidung und Datensparsamkeit gerecht zu werden, verfügt das IT-Verfahren AMS über eine differenzierte Rollen- und Rechteverwaltung. Hierüber kann gesteuert werden, dass jeder Anwendende nur Einblick in die Daten erhält, die für die individuelle Aufgabe erforderlich sind. Die Administration der Rechte und Rollen kann spezifisch für jedes Modul vorgenommen werden und erfolgt über das Modul „Basis“.

1.2 Zeitsynchronisierung

Das eingesetzte Produkt Magellan ist eine Java-Applikation und nutzt über die Java Virtual Machine die Systemzeit des Betriebssystems. Da es sich hier um kein verteiltes System handelt, findet eine Synchronisierung im eigentlichen Sinne nicht statt.

2. Systemprotokollierung

Das IT-Verfahren wird in der On-Premise-Variante bei Dataport im Rechenzentrum betrieben wird. Die Systemprotokollierung zur Überwachung des Systembetriebs erfolgt in Form von Log-Dateien.

2.1.1 Inhalte, Aufbewahrung und Löschung der Protokolldateien

Im Rahmen der Systemprotokollierung werden Ereignisse und Statusmeldungen inkl. Zeitstempel aus dem laufenden Systembetrieb protokolliert. Konkrete Inhalte der Anwendungsprotokolldateien sind bspw. Fehlermeldungen, die der Fehleranalyse dienen.

2.1.2 Speicherort der Protokolldateien (Logs)

Die Log-Dateien werden auf dem vom Dataport für das IT-Verfahren AMS eingerichteten Server im Rechenzentrum RZ² gespeichert

2.1.3 Auswertungszweck und Rhythmus

Die Dateien können im Rahmen der Fehleranalyse bedarfsorientiert ausgewertet werden.

2.1.4 Ordnungsmäßigkeit der Auswertung

In den Log-Dateien werden keine personenbezogenen Daten gespeichert. Dort wo sie gespeichert werden, ist dies für die Sicherheit der Systemumgebung notwendig.
Die Inhalte der Auswertungen sind initial unbearbeitet und weder pseudonymisiert noch anonymisiert.

2.1.5 Zugriff/Manipulation der Logdateien

Der Zugriff auf die Dateien erfolgt ausschließlich durch fachkundige Mitarbeitende bei Dataport, die über entsprechende Zugriffsrechte auf den Server des IT-Verfahrens AMS verfügen. Die Logdateien sind mit entsprechenden Zugriffsrechten auf den o.g. Server bearbeitbar; Änderungen der Protokolldateien über das IT-Verfahren sind nicht möglich.

3. Fachliche Protokollierung

Im Folgenden wird auf die fachliche Protokollierung im IT-Verfahren AMS eingegangen. Diese ist abhängig von den eingesetzten Modulen des Produkts Magellan; hier Basis und Young Talents.

Alle Protokollierungen geschehen automatisiert und sind nicht optional abschaltbar. Die Aufbewahrungsfristen sind in einstellbar und i.d.R. abhängig vom Primärobjekt, wie bspw. der Auszubildende im Modul Young Talents. Die Löschung erfolgt manuell.

3.1 Inhalte, Aufbewahrung und Löschung der Protokolldaten

Insbesondere werden die folgenden Inhalte protokolliert:

- Automatische Protokollierung der Rechtevergabe
- Dokumentation der Stammdatenimporte
- Veränderungen der Aufbewahrungsfristen für personenbezogene Daten
- Korrespondenz (insbesondere E-Mail-Versand und Dokumentenerzeugung)

Generell werden an relevanten Stellen Protokollierungen des Zeitstempels, Erstellers / letzten Bearbeiters sowie von Statusänderungen vorgenommen.

Konkrete Protokollierungen betreffen zum Beispiel:

- Eintragung beurteilungsrelevanter Inhalte für Auszubildende inkl. Eintragendem
- Abstimmungsworkflow bei Feedbackgesprächen
- Erstellung von Berichten

Ebenfalls ist an ausgewählten Stellen eine Protokollierung von Meta-Informationen und Hinweise zur Fehleranalyse von Im- und Exporten in der Anwendung vorgesehen.

3.2 Speicherort der Protokolldaten

Der Speicherort der fachlichen Protokolldaten ist die Anwendungsdatenbank bei Dataport im Rechenzentrum RZ².

3.3 Auswertungszweck und Rhythmus

Die Daten können im Rahmen der Analyse bedarfsorientiert ausgewertet werden. Eine regelmäßige Auswertung erfolgt nicht.

3.4 Ordnungsmäßigkeit der Auswertung

In den fachlichen Protokollen wird vor allem gespeichert, wer welche Änderungen durchgeführt hat. Wie die Authentifizierung durchgeführt wird, ist unter 4. Identitätsprüfung beschrieben.

Die Inhalte der Auswertungen sind initial unbearbeitet und weder pseudonymisiert noch anonymisiert.

3.5 Zugriff/Manipulation der Protokolldaten

Der Zugriff auf die Protokolldaten ist über die entsprechende Berechtigung möglich.
Änderungen der Protokolldaten sind über das IT-Verfahren nicht möglich.

4. Identitätsprüfung

Das Produkt Magellan bietet verschiedene Methoden an, den Anwendenden zu authentifizieren. Beim Thema Authentifizierung fällt oft der Begriff des Identity Providers. Damit ist ein Service gemeint, der die Identität eines Benutzers feststellen und dafür bürgen kann. Das kann auch die eigentliche Fachanwendung sein, muss aber nicht, es kann aber auch ein komplett getrennter Dienst sein, auf die die Anwendung verweist.

Im Sprachgebrauch werden außerdem oft die Begriffe Authentifizierung, Authentisierung und Autorisierung durcheinandergeworfen. Damit sind aber unterschiedliche Sachverhalte gemeint:

	Beschreibung	Beispiel
Authentisierung	„Ich bin Max Mustermann“ Der Anwender beweist seine Identität gegenüber des Identity Providers, er authentisiert sich.	Er gibt ein Passwort ein, das nur er kennt. Er lässt seinen Fingerabdruck scannen.
Authentifizierung	„Ich glaube dir, dass du Max Mustermann bist“ Der Identity Provider bestätigt den Identitätsbeweis des Anwenders, er authentifiziert den Anwender.	Das Passwort oder der Fingerabdruck werden mit einer Datenbank abgeglichen.
Autorisierung	„Du darfst diese Aktion durchführen“ Die Anwendung (nicht der Identity Provider) erlaubt oder verbietet Aktionen je nach Berechtigung des Anwenders, sie autorisiert ihn.	Er darf die Liste an Anmeldungen anzeigen. Er darf nicht Anwendungseinstellungen ändern.

Für das IT-Verfahren AMS kommen die zwei nachstehenden Authentifizierungsmethoden zum Tragen.

4.1 Form-Login

Der Anwender loggt sich über eine von der Anwendung bereitgestellte Loginmaske ein und wird von der Anwendung als Identity Provider authentifiziert. Dazu muss das AMS alle Benutzer in einer Datenbank vorhalten und hat keine Abhängigkeit auf ein weiteres System. Für den Start des AMS wird diese Variante eingesetzt.

4.2 Kerberos / Integrated Windows Authentication

Der Browser des Anwenders und die Anwendung handeln einen Authentifizierungsmechanismus aus, der auf der Windows-Domäne basiert. Über diesen Weg wird für das AMS die Nutzung von Single-Sign-On ermöglicht. Da zunächst Erfahrungswerte gesammelt werden müssen, ob für alle Kennungen Single-Sing-On händelbar ist, wird diese Variante in einem zweiten Schritt umgesetzt.

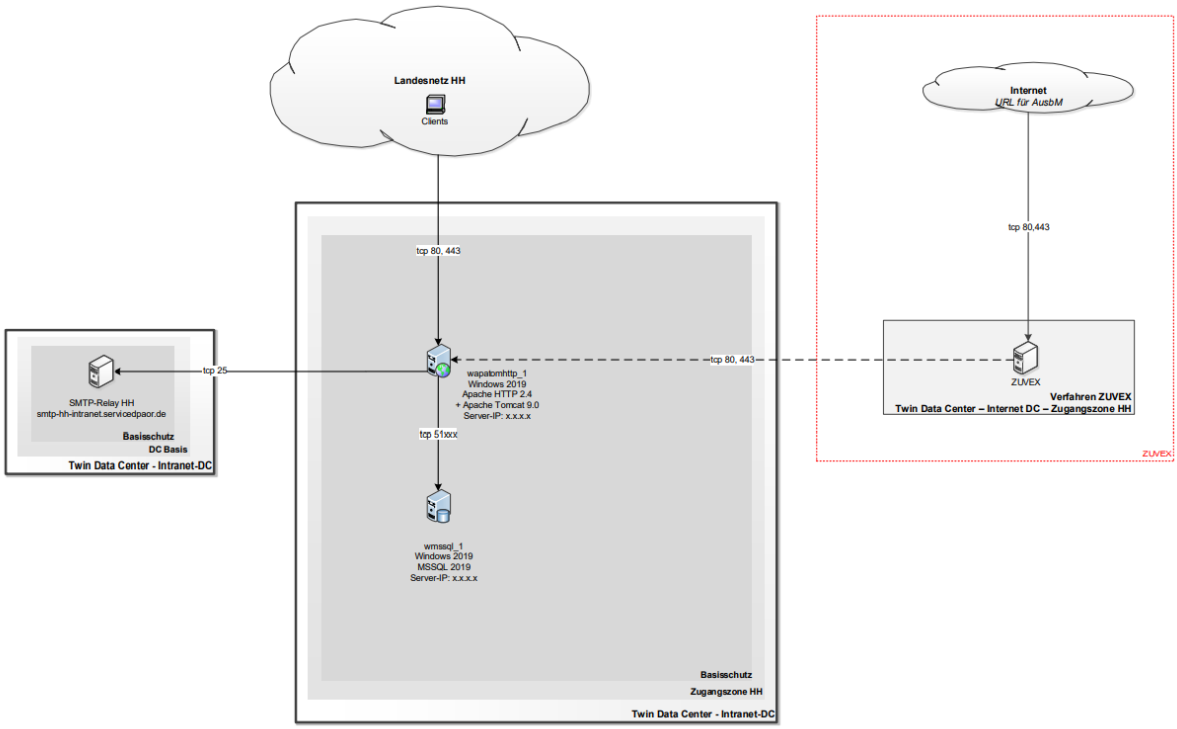
4.3 Automatische Abmeldung

Im Standard wird ein angemeldeter User nach 30 Min. Inaktivität ausgeloggt. Eine Sitzung endet auch immer dann, wenn der genutzte Browser vollständig geschlossen wird. Die Zeitspanne bis zur automatischen Abmeldung lässt sich individuell anpassen.

5. Infrastruktur

Beim IT-Verfahren AMS handelt es sich um eine Web-Anwendung, welche wie bereits zuvor erwähnt, in der von Dataport standardmäßig zur Verfügung gestellten, BSI-zertifizierten RZ2-Infrastruktur betrieben wird.

Der Aufbau der Infrastruktur der Produktivumgebung kann dem nachstehenden Schaubild entnommen werden – die Stageumgebung ist analog aufgesetzt:



Da sich der Anwenderkreis auf alle Behörden und Ämter der FHH erstrecken kann, kann das AMS generell aus dem gesamten FHHnet (Landesnetz HH) aufgerufen werden. Für den Zugriff ist die Eingabe einer Benutzerkennung erforderlich.

Zusätzlich soll das Verfahren ZUVEX den Zugriff von extern auf das AMS ermöglichen. Dieser ist zum einen für an der Ausbildung beteiligte Beschäftigte erforderlich, deren Dienststellen aus organisatorischen Gründen nicht an das FHHnet angebunden sind (z.B. Jobcenter team.arbeit.hamburg). Zum anderen müssen die Nachwuchskräfte von verschiedenen Örtlichkeiten und Geräten auf das IT-Verfahren zugreifen können, da zwischen den Theorie- und Praxisphasen gewechselt wird und somit während der Ausbildungs- und Studienzeit verschiedene Benutzerkonten angelegt werden.

Aus diesem Grund kommt nicht nur ein Web- und Datenbank-Server zum Einsatz, sondern auch das Verfahren ZUVEX. Der SMTP-Server wickelt die E-Mail-Kommunikation ab.

Qualifizierungskonzept zur Schulung der Anwenderinnen und Anwender des IT-Verfahrens „Ausbildungsmanagement-System (AMS)“

Für die Einführung des IT-Verfahrens AMS ist ein mehrstufiges Qualifizierungskonzept vorgesehen. Die Notwendigkeit der jeweiligen Stufe sowie der dann vorliegende Projektfortschritt werden nachstehend zur jeweiligen Stufe beschrieben:

Ausgangslage
Durch den Betrieb des IT-Verfahrens im Rechenzentrum von Dataport ist der Betriebsbereitschaft des IT-Verfahrens der sog. EHdB-Prozess vorgeschaltet – die erstmalige Herstellung des Betriebs. In dieser Zeit stellt Dataport die entsprechenden Server bereit und installiert die Software. Das Projektteam hatte in dieser Zeit keinen Zugriff auf die Anwendung, sodass zu diesem Zeitpunkt noch keine Test-/Qualifizierungsmaßnahmen in geeigneter Form erfolgen konnten. Gemeinsam mit dem Hersteller GuideCom bereitete das Projektteam jedoch bereits in dieser Zeit das auf die FHH angepasste Grundgerüst im Rahmen einer Installationstabelle vor (z.B. Aufbau der Ausbildungs- und Studiengänge, Notenskalen, Behördenstruktur).

Nach erfolgter Installation im Rechenzentrum erfolgte die sog. Kundenabnahme. Dies bedeutet, dass die Installation gegenüber Dataport im Rahmen abgenommen werden muss. Die Kundenabnahme ist am 11.04.2022 gestartet und damit starteten auch die Qualifizierungsmaßnahmen:

Kundenabnahme und Konfigurations-Vorbereitung: 12. und 13.04.2022
Um die Kundenabnahme durchführen und um die weitere Konfiguration der Anwendung abstimmen zu können, wurde der die Ausbildungen steuernde Anwenderkreis* im Rahmen einer schulungsähnlichen Veranstaltung in die Lage versetzt, die Logik und Aufbau der Software nachzuvollziehen und auf die eigenen Prozesse zu übertragen.

*10 Personen bestehend aus Projektteam sowie weitere Kolleginnen und Kollegen des LB ZAF/AMD, Bereich Personal-Center und Qualitätsmanagement / spätere Fachliche Leitstelle.

Vertiefung zur Kundenabnahme und Konfigurations-Vorbereitung:
Da die vorgenannte Veranstaltung vorrangig die Softwarestruktur und Funktionen fokussierte, die für die Kundenabnahme und die Konfiguration der Anwendung erforderlich sind, erfolgt anschließend eine tiefergehende fachliche Schulung, auch mit Blick auf administrative Einstellungsmöglichkeiten für die spätere Fachliche Leitstelle. Der Kreis der Schulungsteilnehmenden entspricht denen der vorgenannten Veranstaltung mit Ausnahme der Projektleitung.

Schulung der Ausbildungsleitungen und Vertretungen sowie der Ausbilderinnen und Ausbilder in der Fachrichtung Allgemeine Verwaltung:
Da die Anwenderschulungen möglichst zeitnah zum Produktivbetrieb erfolgen sollen, dieser aber noch vom Abschluss der §93-Vereinbarung abhängig ist, wurden mehrere Terminblocker im 4. Quartal 2022 bzw. Anfang des 1. Quartals 2023 geplant, sodass je nach Abschlussdatum auf den passendsten Termin zurückgegriffen werden kann.

Die Anwenderschulungen für die Ausbildungsleitungen und ihre Vertretungen erfolgen durch den Hersteller und in Ergänzung durch die Fachliche Leitstelle und Beschäftigte, die für die Ausbildungssteuerung verantwortlich sind. Die Ausbildungsleitungen und ihre Vertretungen sollen dann als Multiplikatoren die Schulung ihrer Ausbilderinnen und Ausbilder in den

Behörden und Bezirksämtern übernehmen und werden im Rahmen der Schulung auf diese Aufgaben entsprechend vorbereitet und mit geeigneten Schulungsunterlagen ausgestattet.

Im Nachgang erfolgt dann in den Behörden und Bezirksämtern in eigener Zeitplanung die Multiplikatorenschulung.

Schulung der Koordinatorinnen und Koordinatoren sowie der Ausbilderinnen und Ausbilder in der Fachrichtung Soziale Arbeit:
Die Anwenderschulungen für die Koordinatorinnen und Koordinatoren erfolgt durch den Hersteller und in Ergänzung durch die Fachliche Leitstelle und Beschäftigte, die für die Ausbildungssteuerung verantwortlich sind.

Die Ausbilderinnen und Ausbilder werden durch die Fachliche Leitstelle und Beschäftigte, die für die Ausbildungssteuerung verantwortlich sind geschult.

Die Schulungen sollen im 1. Quartal 2023 stattfinden.

Schulungen im laufenden Betrieb:
Zum Ausbildungsstart eines jeden neuen Jahrgangs der vom Personalamt angebotenen Ausbildungen erfolgt im Rahmen der Einführungstage die Schulung der Nachwuchskräfte durch die spätere Fachliche Leitstelle und Beschäftigte, die für die Ausbildungssteuerung verantwortlich sind. Die erste Schulung in dieser Form wird mit dem Studiengang 2023 der Sozialen Arbeit ab dem 01.08.2023 stattfinden.

Daneben werden im laufenden Betrieb nach Bedarf Qualifizierungsmaßnahmen angeboten.
Auf die Benutzergruppen angepasste Handbücher werden u.a. direkt im AMS zur Verfügung gestellt und sind somit jederzeit für die Anwendenden zugänglich.

Anlage 7 – Umsetzungsplanung Barrierefreiheit und Softwareergonomie

Dieses Dokument enthält die Planung zur Umsetzung von Anpassungs- und Änderungsbedarfen („Umsetzungsplanung“). Die Anpassungs- und Änderungsbedarfe ergeben sich aus dem Prüfbericht Dataports zur Software-Ergonomie und dem Testat zur Barrierefreiheit auf Basis der WCAG.

Die detaillierte Auswertung Dataports wurde vom Hersteller positiv aufgenommen und eine kurzfristige Behebung der Bedarfe in Aussicht gestellt. Diverse Anpassungsbedarfe (vornehmlich bzgl. Kontraste, Tastatursteuerung und Feld-Beschriftungen) sind bereits in kürzlich entwickelten Updates umgesetzt.

Die übrigen Anpassungsbedarfe werden in zwei Schritten umgesetzt:

- Bedarfe, die unter die „Zentrale Umsetzung“ seitens GuideCom fallen, werden bereits in einer aktualisierten Version der Software enthalten sein, die bis zum 30.09.2022 bereitgestellt wird.
- Die unter "Umsetzung in der Fachabteilung" einsortierten Punkte werden in einer weiteren Iteration behoben und bis zum 30.11.2022 von GuideCom zur Verfügung gestellt.

Zentrale Umsetzung *erfolgt zum 30.09.2022*

- 9.1.1.1a
  - Die Titel der Schaltflächen zum Ein- und Ausklappen von Gruppenboxen ("Akkordeonpfeile") wird GuideCom dynamisch aus dem Titel der Gruppenbox ableiten.
- 9.1.3.1b
  - GuideCom prüft, ob Listenstrukturen in der Navigation eingesetzt werden können.
- 9.1.3.1d
  - GuideCom wird im Modulwechsler die Texte in p-Tags darstellen.
- 9.3.1.2
  - GuideCom wird einzelne englische Texte in einen passenden sprachlichen Kontext setzen.
- 9.2.4.2
  - GuideCom wird einen Schalter implementieren, um wahlweise, den Seitentitel dynamisch abhängig von der aktuellen Position innerhalb der Anwendung anzupassen.

Umsetzung in der Fachabteilung *erfolgt zum 30.11.2022*

- 9.1.1.1b
  - GuideCom wird das Diagramm im Dashboard ausblenden.
- 9.1.1.1a
  - GuideCom wird die Alternativtitel der Icons in Tabellen prüfen und bei Bedarf anpassen.
  - GuideCom wird die unsichtbare Schaltfläche "Anlage herunterladen" passend konfigurieren.

- 9.1.3.1b
  - GuideCom wird prüfen, ob Listenstrukturen in einzelnen fachlichen Komponenten eingesetzt werden können.
- 9.1.3.1d
  - GuideCom wird prüfen, ob die fachliche Implementierung eine Umstellung der Gestaltung auf aussagekräftiges Markup ermöglicht.

Im Folgenden hat der Hersteller zu den offenen Punkten des Prüfberichts Stellung genommen:

9.1.3.1a: HTML-Strukturelemente für Überschriften

Aufgrund des dynamischen Aufbaus der GuideCom Anwendungen kann nicht immer eine numerisch sinnvolle Reihenfolge der *h1-h6*-Elemente sicherstellen. Um diesem Umstand zu begegnen, macht GuideCom intensiv Gebrauch von *„regions“*, die mit den jeweiligen Überschriften betitelt sind. Nutzerinnen und Nutzer von Assistenztechnologien können auf diese Weise genauso schnell durch die Anwendung navigieren, ohne durch eine möglicherweise inkonsistente Überschriftenstruktur verwirrt zu werden.

9.1.4.10: Mobile Ansicht

Die mobile Ansicht der Anwendung wird nur auf Mobiltelefonen (nicht auf Desktop-Systemen) angezeigt. Auf Desktop-Systemen und Tablets wird immer eine für größere Fenster optimierte Darstellung verwendet.

Die mobile Darstellung auf einem Mobiltelefon ist hinsichtlich der Barrierefreiheit von Dataport nicht gesondert betrachtet worden.

9.4.1.1: Korrekte Syntax

Die angemerkten ungültigen Elemente haben zum Teil technische Gründe (*style* als Kind von *custom-style*). Guidecom sieht in den angemerkten Fehlern keine Beeinträchtigung für Assistenztechnologien, da die erwähnten Punkte nicht im sichtbaren Bereich der Anwendung vorliegen. Die duplizierten IDs beziehen sich alle auf Elemente in SVG-Definitionen. Auch hier sind deshalb keine Probleme mit Assistenztechnologien zu erwarten. GuideCom wird diese IDs aber eindeutig machen bzw. entfernen.

9.1.4.12: Textabstände anpassbar

GuideCom wird prüfen, ob in Einzelfällen flexibler auf dynamische Textabstände reagiert werden kann. Diese Anpassungen haben aber möglicherweise Einfluss auf das „Look & Feel“ von Komponenten, sodass GuideCom noch nicht abschließend bewerten kann, wie mit der aufgezeigten Situation umgegangen werden kann.

9.3.3.1: Fehlerhervorhebung

Eine Überarbeitung der Formularkomponenten ist mittelfristig geplant. In diesem Zusammenhang wird auch die Darstellung von Fehleingaben betrachtet. Kurzfristig ist keine Anpassung geplant.