

Vereinbarung

nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG)

über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens
Bewerbungsmanagementsystem (BMS)

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 strebt in Hamburg ein Innovationsklima an, das die Entwicklung moderner digitaler Anwendungen und Applikationen befördert und die Vernetzung zwischen den daran Beteiligten fördert. Dabei zeichnet sich die Freie und Hansestadt Hamburg (FHH) bereits heute durch verschiedene digitale Verwaltungsangebote und die zunehmende Digitalisierung interner Prozesse aus. In Anbetracht dieser Entwicklungen wächst der Bedarf an einer IT-Lösung zur Unterstützung von Personalauswahl- und Personalrekrutierungsprozessen sowie an digitaler Vernetzung der daran beteiligten Akteurinnen und Akteure. In Ermangelung einer FHH-weit einheitlichen IT-Lösung entwickelten die verschiedenen Dienststellen bislang zahlreiche Individuallösungen zur analogen oder digitalen Umsetzung von weitestgehend standardisierten Prozessen.

Eine gemeinsame, integrierte Lösung für ein FHH-weit einheitliches, digitales Bewerbungsmanagementsystem (BMS) in den zahlreichen Personaldienststellen der FHH fördert eine technische Vereinfachung der Beteiligung der verschiedenen Akteurinnen und Akteure, transparente Datenbearbeitung und -verarbeitung sowie eine medienbruchfreie Zusammenarbeit aller Beteiligten im weiteren Verlauf des Verfahrens. Die Einführung eines neuen und modernen Stellenportals ermöglicht es den Bewerberinnen und Bewerbern, sich unkompliziert online zu bewerben und ihre Bewerbungen(en) komfortabel über ein persönliches Benutzerkonto zu verwalten.

Nr. 1

Gegenstand der Vereinbarung

Gegenstand der Vereinbarung sind die Einführung, der Betrieb, die Nutzung und die Weiterentwicklung des neuen IT-Verfahrens Bewerbungsmanagementsystem (BMS).

Zweck und Ziel des IT-Verfahrens sind in der Beschreibung der Verarbeitungstätigkeit (Anlage 1) und der Datenschutzfolgeabschätzung* (Anlage 2) näher beschrieben. Die Anlagen sind Bestandteil der vorliegenden Vereinbarung.

Nr. 2

Geltungsbereich

Die Vereinbarung gilt für alle Verwaltungseinheiten der FHH, für die der Senat oberste Dienstbehörde ist und die gleichzeitig das digitale Bewerbungsmanagementsystem BMS eingeführt haben.

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

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.

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 erfüllen¹.

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.

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 oder ** Abweichung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

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, Schutz vor Leistungs- und Verhaltenskontrolle

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.

Die erforderlichen personenbezogenen Daten der Anwenderinnen und Anwender des BMS werden zu folgenden Zwecken genutzt:*

- Identifikation und Aufruf des Verfahrens,
- Aufzeichnung der Zugriffe und Veränderungen,
- Aufzeichnung von Kommentaren zu Veränderungen sowie
- die revisionssichere Identifikation und dauerhafte Speicherung erfassender und den Workflow durchführender Personen sowie der das Verfahren administrierenden Personen.

Im Einzelnen handelt es sich um folgende personenbezogene Daten der Beschäftigten:*

- Name, Vorname
- Funktionsbezeichnung (optional)
- Benutzer-Kennung
- dienstliche E-Mail-Adresse
- dienstliche Anschrift (optional)
- dienstliches Telefon sowie Fax (optional)
- Organisationseinheit
- Benutzergruppe

Die Erteilung von Berechtigungen erfolgt auf der Grundlage eines Berechtigungs- und Rollenkonzepts, in dem die für die verschiedenen Funktionen/Mitarbeitergruppen erforderliche Berechtigungen festgelegt werden um mandantenspezifische (d. h. separat für jede Organisationsstruktur geltende) Berechtigungsstrukturen abzubilden. Es wird gewährleistet, dass auftragsverarbeitende Stellen ausschließlich anlassbezogen auf Bewerbungsunterlagen zugreifen können.* Das Rechte- und Rollenkonzept wird in der Anlage 3 näher beschrieben.

Eine revisionssichere Protokollierung wird wie folgt sichergestellt:*

Jedes Objekt (Vakanz, Bewerbung) hat eine Änderungshistorie, die sämtliche Veränderungen von Daten, Hinzufügen oder Löschen von Dateien und Änderungen am Status der Prozessierung mit Zeitstempel und einer verantwortlichen Person für die betreffende Änderung dokumentiert. Jeder Nutzer hat einen eindeutigen persönlichen Zugriff auf das BMS und kann nur

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

gemäß vorgegebener Berechtigungen auf die Anwendung selbst und auf Objekte darin zugreifen. Nicht jeder Nutzer hat Änderungsrechte.² Die Historie eines Objektes wird nicht gelöscht. Datenänderungen werden nicht im Detail protokolliert.*

Die serverseitige Archivierung (Backup, Logging) erfolgt gemäß der vom Betreiber Dataport standardmäßig zur Verfügung gestellten, BSI-zertifizierten RZ2-Infrastruktur. Die entsprechende Dokumentation ist nur über den InSiMa-Sharepoint der FHH einsehbar. Ansprechpartner ist der InSiBe des Personalamts.*

Das Löschkonzept ist als Anlage 4 beigefügt. Schnittstellen zu anderen Systemen (Datenimport, Datenexport) werden in einem Katalog zusammengefasst und beschrieben (Anlage 5).^{*} In der Entwicklung des Verfahrens ist die Einbindung von weiteren Schnittstellen zu anderen Verfahren geplant. Hierzu wird die Anlage (Nr. 5) laufend aktualisiert.

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 zur 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 möglichst³ 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.

Nr. 6

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 Qualifizierungsmaßnahmen erfolgen zeitnah vor Einführung des IT-Verfahrens. Im Zuge der Einführung wird der Erfolg der Qualifizierungsmaßnahmen überprüft indem nach ca. 4 – 6 Monaten Arbeit mit dem IT-Verfahren wird den Anwenderinnen und Anwendern Gelegenheit gegeben wird, durch eine

² Vgl. dazu das Berechtigungskonzept als Anlage 3 zu dieser Vereinbarung.

³ 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 oder ** Abweichung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

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 oder 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, Personalräte und Schwerbehindertenvertretungen erhalten Gelegenheit an den Qualifizierungsmaßnahmen teilzunehmen.

Nr. 7

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.

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.

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

Nr. 8

Evaluation des Betriebs unter Beteiligung der Spitzenorganisationen

Zwei 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).

Soweit möglich werden bei der Evaluation alle Entwicklungsziele zu fachlichen Belangen, Datenschutz, Anwendungstauglichkeit (Gebrauchstauglichkeit), Barrierefreiheit 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. 9

Verfahren bei Änderungen

Das unter lfd. Nummer 1 beschriebene Verfahren wird bei Bedarf weiterentwickelt.

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

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

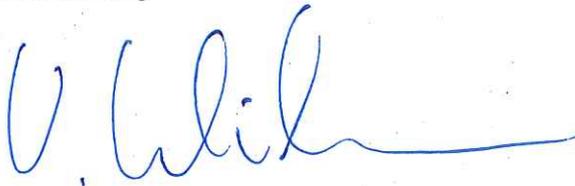
Schlussbestimmungen

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

Die Vereinbarung tritt am 1. April 2022 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 16. März 2022

Freie und Hansestadt Hamburg
für den Senat

Volker Wiedemann

dbb hamburg
beamtenbund und tarifunion

Rudolf Klüver

Deutscher Gewerkschaftsbund
-Bezirk Nord-

Olaf Schwede

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

Anlagen:

1. Beschreibung der Verarbeitungstätigkeit
2. Datenschutzfolgeabschätzung
3. Berechtigungskonzept
4. Löschkonzept
5. Schnittstellenkonzept
6. Qualifizierungskonzept

Beschreibung der Verarbeitungstätigkeit

(Bitte an die Verzeichnisführende Stelle absenden!)

Nur auszufüllen, wenn personenbezogene Daten verarbeitet werden!

Blatt-Nr.:

Von der Verzeichnisführenden Stelle auszufüllen!

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

| Allgemeines | | | |
|--|---|--|---------------------------------------|
| | Datum: | 15.07.2021 | |
| | Ausfüllende Personen: | Taylan Karakurt (externer Berater) | |
| | Bezeichnung des Verfahrens: | BMS - Bewerbungsmanagement System | |
| | Bezeichnung der Verarbeitung: | <input checked="" type="checkbox"/> Erheben <input checked="" type="checkbox"/> Erfassen <input checked="" type="checkbox"/> Organisieren <input checked="" type="checkbox"/> Ordnen <input checked="" type="checkbox"/> Speichern <input checked="" type="checkbox"/> Anpassen oder Verändern <input type="checkbox"/> Auslesen <input type="checkbox"/> Abfragen <input checked="" type="checkbox"/> Verwenden <input checked="" type="checkbox"/> Offenlegen durch Übermittlung, Verbreitung oder andere Form der Bereitstellung <input type="checkbox"/> Abgleichen oder Verknüpfen <input checked="" type="checkbox"/> Einschränken <input checked="" type="checkbox"/> Löschen <input checked="" type="checkbox"/> Vernichten | |
| | Beginn der Verarbeitung: | 01.04.2021 | |
| | Änderung bestehende Verarbeitung: | <input type="checkbox"/> ja | |
| | Überführung bestehende Verarbeitung in geltende Rechtslage nach DS-GVO: | <input type="checkbox"/> ja | |
| | Neue Verarbeitung: | <input checked="" type="checkbox"/> ja | |
| | Abmeldung bestehende Verarbeitung: | <input type="checkbox"/> ja | |
| 1. Grundsätzliche Angaben zur Verantwortlichkeit | | | |
| 1.1 | Verantwortliche Organisationseinheit (optional): | Gemeinsame Verantwortlichkeit aller das BMS nutzenden Organisationseinheiten und des ZPD gem. Art. 26 DSGVO | Vertrag gemeinsame Verantwortlichkeit |
| 1.2 | Vertreter der verantwortlichen Organisationseinheit (optional): | Herr Carsten Brucks | |
| 1.3 | Fachliche Leitstelle (bei IT-Verfahren) bzw. zuständige Stelle (bei nicht automatisierten Verfahren): Verantwortliche Führungskraft: Leitzeichen: | ZPD 3 Klicken Sie hier, um Text einzugeben. | |
| 1.4 | Ansprechpartner, sofern nicht verantwortliche Führungskraft: | Herr Stefan Kasimir Klicken Sie hier, um Text einzugeben. | |

| | | | |
|-----|---|--|--|
| 1.5 | Name des Datenschutzbeauftragten (optional): | Herr Ralf Napirata (ZPD) | |
| 1.6 | Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt: Auftragsnummer: | Dataport AöR Altenholzer Strasse 10-14 24161 Altenholz V15011/2141000 milch & zucker AG Friedrich-List-Straße 23 5398 Gießen | Clientenvereinbarung AVV Dataport AVV MZ |

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

| | | | |
|-------------------------------------|--|---|--|
| 2.1 | Beschreibung und Zweckbestimmung der Verarbeitung von Daten | Das BMS, dient der Erstellung und Online-Veröffentlichung von Stellenangeboten, sowie der Erfassung und Verwaltung eingehender Bewerbungen der FHH. Beschreibung der Zweckbestimmung: Bewerbungsverfahren | |
| 2.2 | Rechtsgrundlage (Zutreffendes bitte ankreuzen und ggf. erläutern): | | |
| <input type="checkbox"/> | Spezialgesetzliche Regelung außerhalb der DS-GVO | § 85 HmbBG, i.V.m. § 10 HmbDSG | |
| <input checked="" type="checkbox"/> | Einwilligung des Betroffenen (Art. 6 Abs. 1 a DS-GVO): | Ja | |
| <input checked="" type="checkbox"/> | Kollektivvereinbarung (z. B. Vereinbarung gem. HmbPersVG, Tarifvertrag) | Eine Kollektivvereinbarung gem. § 93 HmbPersVG wurde geschlossen. | |
| <input type="checkbox"/> | Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 4 HmbDSG n.F.) | Klicken Sie hier, um Text einzugeben. | |
| <input checked="" type="checkbox"/> | Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§ 10 HmbDSG n.F. und national geregelt im BDSG): | § 85 HmbBG i.V.m. § 10 HmbDSG Art. 6 Abs. 1, b; Art. 88 DS-GVO | |
| <input checked="" type="checkbox"/> | Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b DS-GVO) | Ja, Arbeitsverträge | |
| <input type="checkbox"/> | Interessenabwägung (Art. 6 Abs. 1 f DS-GVO) | Nein | |
| <input type="checkbox"/> | Weitere: | Klicken Sie hier, um Text einzugeben. | |

3. Beschreibung betroffener Personen- und Datenkategorien

| | | | |
|-----|---|---|--|
| 3.1 | Beschreibung der betroffenen Personengruppen: | Wählen Sie ein Element aus. interne und externe Bewerberinnen und Bewerber (externe Interessenten u. inte- | |
|-----|---|---|--|

| | | | |
|---|---|---|--|
| | | ressierte Beschäftigte), Recruiter, Fachbereiche, Personalratsmitglieder, Schwerbehindertenvertretung, Gleichstellungsbeauftragte | |
| 3.2 | Beschreibung der Art der Daten bzw. Datenkategorien | Identifikations- und Adressdaten Mitarbeiterdaten Gesundheitsdaten Kommentare der Prozessbeteiligten Lohn- / Besoldungsdaten Angaben zum beruflichen Werdegang und zur beruflichen Qualifikation Titel Lebenslauf Abschlüsse/ Beurteilungen Angaben zu familiären Verhältnissen | |
| 3.3 | Werden besondere Kategorien von Daten verarbeitet (Art. 9 Abs. 1 DS-GVO)? | <input checked="" type="checkbox"/> ja, welche? Gesundheitsdaten Wählen Sie ein Element aus. Wählen Sie ein Element aus. Wählen Sie ein Element aus. Bei allen Bewerbern wird erfasst, ob schwerbehindert/gleichgestellt oder nicht. Bei den sogenannten Mobilien Mitarbeitern der FHH gibt es die Kategorie der aus gesundheitlichen Gründen nicht mehr im ursprünglichen Beruf Befindlichen. Bestimmte Dienststellen (z.B. Polizei) verlangen ferner die Angabe der gesundheitlichen Eignung (im Pilotbetrieb nicht relevant). Daten zur Herkunft, sexuellen/religiösen Orientierung, Lebenspartnerschaft sowie biometrische Daten werden nicht abgefragt und nicht verarbeitet. Nicht verhindert werden kann, dass diese ex- oder implizit freiwillig oder versehentlich preisgegeben werden (z.B. im Lebenslauf). Die Bewerbenden im Bereich Trainees (P31) werden zur Vorbereitung späterer Verbeamtungen auch nach ihrer Staatsangehörigkeit gefragt. | |
| 4. Datenweitergabe und deren Empfänger | | | |
| 4.1 | Eine Datenübermittlung findet statt oder ist geplant. | <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein | |
| 4.2 | Interne Empfänger innerhalb der verantwortlichen Stelle | <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein | |
| | Interne Stelle (Organisationseinheit) | Sämtliche Personalabteilungen der Dienststellen und ihrer Gremien, die das BMS nutzen (siehe Berechtigungskonzept) Personalamt (P31, P34) Postfach der Personalsachbearbeitung der ausschreibenden Stelle | |

| | | | |
|--|----------------------------|--|--|
| | | <p>Personalrat der ausschreibenden Stelle (PR)</p> <p>Gleichstellungsbeauftragte der ausschreibenden Stelle (GB)</p> <p>Schwerbehindertenvertretung der ausschreibenden Stelle (SBV)</p> <p>Leitungskräfte der ausschreibenden Stelle</p> <p>Empfang der ausschreibenden Stelle</p> | |
| | Art der Daten | Jeweils aufgabenbezogen notwendige personenbezogene Daten – siehe 3.2 | |
| | Zweck der Daten-Mitteilung | <p>Alle nachfolgenden Organisationseinheiten erhalten die sie betreffenden Informationen über ihren eigenen Zugriff auf das BMS. Davon ausgenommen sind Leitungskräfte und Empfang. Der Empfang erhält personenbezogene Daten (Name des Bewerbers u. Termin des Vorstellungsgesprächs) per E-Mail aus dem BMS. Leitungskräften können per E-Mail Globalinformationen zum Stand von Stellenbesetzungsverfahren zugespielt werden.</p> <ul style="list-style-type: none"> • Personalamt (P31, P34) Die beiden Einheiten P31 und P34 des PA sind für die Steuerung der Personalgewinnung und -entwicklung der FHH zuständig und haben jeweils die gesamte Sicht auf laufende Stellenbesetzungsverfahren in ihrem Zuständigkeitsbereich. Zudem ist die Einheit P34 Empfänger der Daten aus der Webanalyse durch Matomo. • Dienststelle In den Dienststellen führen die Mitarbeitenden des Recruiting die Verwaltung und Bearbeitung von Bewerbungen aus • Postfach der Personalsachbearbeitung Nachdem die Recruiter ihren Teil des Bewerbungsprozesses abgeschlossen haben, werden alle relevanten Dokumente dem Postfach der Personalsachbearbeitung zur Verfügung gestellt. • Personalrat (PR) Im Rahmen der Beteiligungsrechte des Personalrats nach dem Hamburgischen Personalvertretungsgesetz (HmbPersVG) | |

| | | | |
|-----|------------------------------|---|--|
| | | <p>werden dem Personalrat die für die Wahrnehmung seiner Aufgaben erforderlichen personenbezogenen Daten übermittelt. Art und Umfang der Beteiligung ergeben sich aus dem HmbPersVG. Dort ist unter anderem auch geregelt, dass Unterlagen mit personenbezogene Daten nach Abschluss des Mitbestimmungsverfahrens zurückzugeben oder zu vernichten sind (§ 78 Abs. 5 HmbPersVG).</p> <ul style="list-style-type: none"> • Gleichstellungsbeauftragte (GB) Zur Wahrnehmung ihrer Aufgaben nach dem Hamburgischen Gleichstellungsgesetz (HmbGleiG) werden den Gleichstellungsbeauftragten der Dienststellen personenbezogene Daten offengelegt bzw. übermittelt. Die Gleichstellungsbeauftragten sind über alle anstehenden personellen, sozialen und organisatorischen Maßnahmen, die die Gleichstellung von Frauen und Männern und die Vereinbarkeit von Erwerbs- und Familienarbeit betreffen, zu unterrichten. • Schwerbehindertenvertretung (SBV) Die Schwerbehindertenvertretung ist in allen Angelegenheiten, die einen einzelnen oder die schwerbehinderten Menschen als Gruppe berühren, zu beteiligen. Daher werden ihr die zur Wahrnehmung ihrer Aufgaben benötigten personenbezogenen Daten übermittelt. Art und Umfang der Beteiligung ergeben sich aus § 178 Sozialgesetzbuch Neuntes Buch (SGB IX). • Leitungskräfte Im Laufe der Bewerbungsprozesse sind Leitungskräfte in Bereichen, in Stellen besetzt werden sollen, nachrichtlich zu involvieren. • Empfang Für die Organisation der Bewerbungstermine werden Namen an das Postfach des Empfangsbereichs versendet. Der Empfangsbereich verfügt nicht über einen eigenen Zugriff auf das BMS. | |
| 4.3 | Externe Empfänger und Dritte | <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein Dataport AöR (als Auftragsdatenverarbeiter gemäß Ziffer 1.6) milch & zucker AG (als Auftragsdatenverarbeiter gemäß Ziffer 1.6) | |
| | Externe Stelle | Dataport AöR (Adresse siehe Ziffer 1.6) | |

| | | | |
|---|---|--|---------------------------|
| | | milch & zucker AG (Adresse siehe Ziffer 1.6) | |
| | Art der Daten | Dataport u. milch & zucker: Anlassbezogen personenbezogene Daten gemäß Abschnitt 3 im Rahmen des Supports. | |
| | Zweck der Daten-Mitteilung | Dataport: Bereitstellung, Hosting u. Betrieb der Applikation auf der Infrastrukturmgebung des Rechenzentrums von Dataport. milch & zucker: Pflege und Wartung der gelieferten Software, fachliche und technische Betriebsunterstützung durch Supportleistungen für die Software und die Technische Dokumentation über Installation und Betrieb sowie Anwenderdokumentation. | |
| 4.4 | Geplante Datenübermittlung in Drittstaaten (außerhalb der EU) bzw. internationale Organisation | <input type="checkbox"/> ja <input checked="" type="checkbox"/> 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: <input type="checkbox"/> verbindliche interne Datenschutzvorschriften, <input type="checkbox"/> von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln <input type="checkbox"/> 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 | | | |
| | Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Lösungsfristen? | <input checked="" type="checkbox"/> ja, um eine Anfechtung u. a. für Beamte nach dem Bewerbungsverfahren zu ermöglichen, werden die erhobenen Daten 400 Tage aufbewahrt und dann für statistische Zwecke anonymisiert. <input type="checkbox"/> nein | |
| | Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden: | Die Daten werden gemäß Löschkonzept anonymisiert bzw. gelöscht. | Löschkonzept+Löschfristen |
| 6. Mittel der Verarbeitung (optional) Welche Software oder Systeme werden für diese Verarbeitung eingesetzt? | | | |
| | Bezeichnung: Hersteller: | BeeSite Recruiting Edition milch & zucker AG | |

| | | | |
|--|--|--|-----------------------|
| | Funktionsbeschreibung: Bereitstellung: | Eine Software für das Bewerbermanagement. <input type="checkbox"/> Eigenentwickelte/ individuelle Software <input checked="" type="checkbox"/> Standard-Software Mit Anpassungen entsprechend den spezifischen Anforderungen der FHH. <input type="checkbox"/> Cloud-Services <input type="checkbox"/> Sonstige: Klicken Sie hier, um Text einzugeben. | |
| 7. Zugriffsberechtigte Personengruppen (vereinfachtes Berechtigungskonzept) | | | |
| | Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte Berechtigungskonzept: | Berechtigungskonzept Dieses beschreibt die Berechtigungsverfahren detailliert und listet die berechtigten Gruppen übersichtlich. | Berechtigungs-konzept |
| 8. Sicherheit der Verarbeitung (Risikoprüfung), Datenschutz-Folgenabschätzung und Technische und organisatorische Maßnahmen | | | |
| 8.1 | Hinsichtlich der Datensicherheitsmaßnahmen wurde der Bereich IT-Sicherheit (z. B. InSiBe der OE) eingebunden? | <input checked="" type="checkbox"/> ja, IT-SiBe des ZPD <input type="checkbox"/> nein | |
| 8.2 | Die allgemeine Zielsetzung aus dem Rahmensicherheitskonzept wurde sichergestellt. | <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein, Abweichungen erläutern: Klicken Sie hier, um Text einzugeben. | |
| 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? | <input checked="" type="checkbox"/> ja (ggf. Betriebs-/Herstellerkonzept beifügen) <input type="checkbox"/> 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. | <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein Bitte Ergebnis der Risikoprüfung als Anlage beifügen. | |
| 8.5 | Es wurden die Erforderlichkeitsprüfung („Schwellwertanalyse“) und ggf. die Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO durchgeführt. | <input checked="" type="checkbox"/> ja, Ergebnis der Erforderlichkeitsprüfung („Schwellwertanalyse“) als Anlage beifügen <input type="checkbox"/> nein | |
| 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). | <input checked="" type="checkbox"/> Es liegt ein Verfahren vor, das bei Dataport gehostet wird. | |
| 8.7 | Bei Verfahren, die <u>nicht</u> bei Dataport gehostet werden: | <input type="checkbox"/> Es liegt kein Verfahren vor, das bei Dataport gehostet wird. | |

| | | | |
|--|---|--|--|
| | Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMs laut Anlage 2 sichergestellt. | <input type="checkbox"/> Die Anlage 2 wurde ausgefüllt und liegt vor. | |
| 8.8 | Es liegen schriftlich vor | <input type="checkbox"/> interne Verhaltensregeln (wird Bestandteil des Verfahrens-betriebskonzepts sein) <input checked="" type="checkbox"/> DSFA <input checked="" type="checkbox"/> Risikoprüfung/ Schutzbedarfsfeststellung <input checked="" type="checkbox"/> allg. Datensicherheitsbeschreibung (siehe Folgepunkt) <input checked="" type="checkbox"/> umfassendes Datensicherheitskonzept (nur den IT-SiBe. des ZPD zugänglich) <input checked="" type="checkbox"/> Wiederanlauf- bzw. Notfallkonzept <input type="checkbox"/> Sonstiges: Klicken Sie hier, um Text einzugeben. | |
| 9. Datenübertragbarkeit (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? | <input type="checkbox"/> ja, Format: Klicken Sie hier, um Text einzugeben. <input type="checkbox"/> nein, Begründung: Klicken Sie hier, um Text einzugeben. | |
| 10. Informationen der Betroffenen | | | |
| | Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht? | Die Datenschutzhinweise sind den Nutzern des Stellenportals im Footerbereich zugänglich. Bei der Registrierung eines Accounts für das BMS muss die Kenntnisnahme der Datenschutzhinweise vom Nutzer bestätigt werden. | |
| 11. Sonstiges | | | |
| | Anmerkungen: | Klicken Sie hier, um Text einzugeben. | |

.....
Verantwortlicher

.....
Datum

.....
Unterschrift

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 |
|--|--|---|
| <p>Datenminimierung Art. 5 Abs. 1 lit.c DS-GVO</p> | - | <p>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)</p> |
| <p>Gewährleistung der Integrität Art. 32 Abs. 1 lit. b DS-GVO</p> | <p>Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BDSG)</p> | <p>Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (luK-Grundschutzkonzept) Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)</p> |
| | <p>Datenintegrität (§ 64 Abs. 3 Nr. 11 BDSG)</p> | <p>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)</p> |
| | <p>Datenträgerkontrolle (§ 64 Abs. 3 Nr. 2 BDSG)</p> | <p>Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im luK-Bereich Entsorgungs-Richtlinie</p> |
| | <p>Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)</p> | <p>Sicherheits- und Betriebskonzept Rechenzentrum Dataport Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden</p> |
| | <p>Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BDSG)</p> | <p>Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im luK-Bereich</p> |
| | <p>Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)</p> | <p>Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz</p> |

| | | |
|---|--|---|
| | | Geschäftsordnungsbestimmungen der Behörden |
| | Trennbarkeit (§ 64 Abs. 3 Nr. 14 BDSG) | 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 BDSG) | Sicherheits- und Betriebskonzept Rechenzentrum Dataport 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 BDSG) | 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 |

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

| | | |
|--|---|--|
| | | 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 Grundsatzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (luK-Grundsatzkonzept) Richtlinie zur Datensicherheit im luK-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 luK-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 luK-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 luK-Bereich |

| | | |
|--|---|--|
| | Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BDSG) | Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundsatzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundsatzkonzept) 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 BDSG) | 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 Grundsatzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundsatzkonzept) 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) |

Anlage 2 der Vereinbarung nach § 93 HmbPersVG Vereinbarung über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS)

| Risiko Nr. | Schutzleie (Grundsätze nach Art 5 DSGVO) | I. Risikoidentifikation | | | II. Risikokategorie | | | III. Risikobewertung | | | IV. Risiko inkl. Maßnahmen | | |
|------------|--|---|--|--|---|-------------------------------------|------------------------------|-------------------------|--|-------------------------------------|------------------------------|------------------------------|--|
| | | Risikquelle | Risikobeschreibung | Möglicher physischer, materieller oder immaterieller Schaden | Schadenskategorie (nach EnwGrV 75) | Eintrittswahrscheinlichkeit 1 bis 4 | Schwere des Schadens 1 bis 4 | Ergebnis 1 bis 3 | Mitigierende Abhilfemaßnahmen | Eintrittswahrscheinlichkeit 1 bis 4 | Schwere des Schadens 1 bis 4 | Mitigiertes Ergebnis 1 bis 3 | |
| 1 | Vertraulichkeit | Bewerberin Cyberkriminelle (Hacker / Schadsoftware) | nutzt ein kompromittiertes System zur Eingabe | führt zu Abfluss von Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | Risiko (4) | | Begrenzt (2) | Begrenzt (2) | Risiko (4) | |
| 2 | Vertraulichkeit | Mandant (Recruiter, Teledienst) | entwendet unbefugte Daten aus dem Datenbank/dem BMS | führt zu Abfluss von allen gespeicherten Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Passwortrichtlinie, Kennwortoffenheit | Begrenzt (2) | Begrenzt (2) | Risiko (4) | |
| 3 | Vertraulichkeit | Dienstleister Dataport | entwird unbefugte Daten aus der Datenbank/dem BMS | führt zu Abfluss von allen gespeicherten Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Berechtigungskonzept, Monitoring | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 4 | Vertraulichkeit | Dienstleister MAZ | entwird unbefugte Daten aus der Datenbank/dem BMS | führt zu Abfluss von allen gespeicherten Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Gewährleistung der Verschlüsselungsstärke | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 6 | Vertraulichkeit | Dienstleister MAZ | entwird unbefugte Daten aus der Datenbank/dem BMS | führt zu Abfluss von allen gespeicherten Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Testung | Begrenzt (2) | Begrenzt (2) | Risiko (4) | |
| 7 | Vertraulichkeit | Cyberkriminelle (Hacker / Schadsoftware) | schneidet Datenverkehr mit | führt zu Abfluss von Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Aufsucht durch Dataport und Logging der Aktionen | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 8 | Vertraulichkeit | Cyberkriminelle (Hacker / Schadsoftware) | schneidet Datenverkehr mit | führt zu Abfluss von Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Sichere Softwareentwicklung, Testing (App/HPI) | Begrenzt (2) | Maximal (4) | Risiko (6) | |
| 9 | Vertraulichkeit | Cyberkriminelle (Hacker / Schadsoftware) | schneidet Datenverkehr mit | führt zu Abfluss von Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Wesentlich (3) | Wesentlich (3) | Risiko (4) | Transportverschlüsselung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 10 | Vertraulichkeit | Cyberkriminelle (Hacker / Schadsoftware) | schneidet Datenverkehr mit | führt zu Abfluss von Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Gewährleistung der Verschlüsselungsstärke | Vernachlässigbar (1) | Begrenzt (2) | Risiko (4) | |
| 11 | Vertraulichkeit | Staatliche Institutionen (Nachrichtendienst) | schneidet Datenverkehr mit | führt zu Abfluss von Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Wesentlich (3) | Begrenzt (2) | Risiko (4) | Transportverschlüsselung | Wesentlich (3) | Vernachlässigbar (1) | Risiko (4) | |
| 12 | Vertraulichkeit | Softwarefehler | führt zu partieller Aufhebung der Mandatentrennung | führt zu Abfluss von Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Qualitätskontrolle durch Recruter | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 13 | Vertraulichkeit | Verantwortlicher (Fachliche Leitstelle/Admin) | weist falsche Berechtigungen zu | führt zu unbefugtem Zugriff | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Rechte- und Rollenkonzept, Plausibilitätsprüfung | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 14 | Vertraulichkeit | Verantwortlicher (Fachliche Leitstelle/Admin) | trägt absichtlich falsche Daten ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Prüfkript auf verwaiste Gruppen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 15 | Integrität | Bewerberin | trägt richtige Daten falsch ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Vernachlässigbar (1) | Begrenzt (2) | Risiko (4) | Qualitätskontrolle durch Betroffenen | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 16 | Integrität | Bewerberin | nutzt ein kompromittiertes System zur Eingabe | führt zu Abfluss der Daten ohne weitere Kontrolle | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 17 | Integrität | Mandant (Recruiter, Teledienst) | entwendet unbefugte Daten aus dem Datenbank/dem BMS | führt zu Abfluss von Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Backupsystem | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 18 | Integrität | Mandant (Recruiter, Teledienst) | entwendet unbefugte Daten aus dem Datenbank/dem BMS | führt zu Abfluss von Daten | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Qualitätskontrolle durch Betroffenen | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 19 | Integrität | Dienstleister Dataport | manipuliert Rohdaten | führt zu korruptierten Daten und zu Systemfehlern | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Backupsystem | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 20 | Integrität | Dienstleister MAZ | manipuliert Rohdaten | führt zu korruptierten Daten und zu Systemfehlern | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Backupsystem | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 21 | Integrität | Dienstleister MAZ | manipuliert Rohdaten | führt zu korruptierten Daten und zu Systemfehlern | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Mechanismen zur Recovery | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 22 | Integrität | Cyberkriminelle (Hacker / Schadsoftware) | schließt Schadcode direkt in die Anwendung (SQL etc.) | führt zu korruptierten Daten und zu Systemfehlern | Andere wirtschaftliche oder gesellschaftliche Nachteile | Wesentlich (3) | Maximal (4) | Risiko (6) | Sichere Softwareentwicklung, Testing (App/HPI) | Begrenzt (2) | Maximal (4) | Risiko (6) | |
| 23 | Integrität | Staatliche Institutionen (Nachrichtendienst) | manipuliert Rohdaten | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Vernachlässigbar (1) | Maximal (4) | Risiko (6) | Sichere Softwareentwicklung, Testing (App/HPI) | Begrenzt (2) | Maximal (4) | Risiko (6) | |
| 24 | Integrität | Hardwaredefekt (physikalisch) | führt zum Verlust von Datenpaketen | führt zu Betriebsfehlern während der Laufzeit | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | geringstes Risiko (2-3) | Sichere Softwareentwicklung, Testing (App/HPI) | Begrenzt (2) | Maximal (4) | Risiko (6) | |
| 26 | Integrität | Softwarefehler | führt zu korruptierten Daten | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | Sichere Softwareentwicklung, Testing (App/HPI) | Begrenzt (2) | Maximal (4) | Risiko (6) | |
| 27 | Integrität | Softwarefehler | führt zu korruptierten Daten im Backup | verhindert die Kontrolle der Betroffenen über eigene Daten | Hinderung der Kontrolle der Betroffenen über eigene Daten | Begrenzt (2) | Begrenzt (2) | geringstes Risiko (2-3) | Sichere Softwareentwicklung, Testing (App/HPI) | Begrenzt (2) | Maximal (4) | Risiko (6) | |
| 28 | Integrität | Nutzungen | lassen Datenpakete verschwinden | führt zu Betriebsfehlern während der Laufzeit | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | geringstes Risiko (2-3) | Sichere Softwareentwicklung, Testing (App/HPI) | Begrenzt (2) | Maximal (4) | Risiko (6) | |
| 29 | Integrität | Verantwortlicher (Superadministrator) | manipuliert Rohdaten | führt zu korruptierten Daten und zu Systemfehlern | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Begrenzt (2) | geringstes Risiko (2-3) | Sichere Softwareentwicklung, Testing (App/HPI) | Begrenzt (2) | Maximal (4) | Risiko (6) | |
| 30 | Verfügbarkeit | Bewerberin | trägt unbefugte Daten ein | keine weitere Verarbeitung mehr möglich, z. B. Nicht-Einstellung | Finanzieller Verlust | Begrenzt (2) | Vernachlässigbar (1) | Risiko (4) | Kontrollinformationen setzen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 31 | Verfügbarkeit | Mandant (Recruiter, Teledienst) | trägt absichtlich falsche Daten ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Kontrollinformationen setzen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 32 | Verfügbarkeit | Dienstleister Dataport | trägt absichtlich falsche Daten ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Kontrollinformationen setzen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 33 | Verfügbarkeit | Dienstleister Dataport | trägt absichtlich falsche Daten ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Kontrollinformationen setzen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 34 | Verfügbarkeit | Dienstleister Dataport | trägt absichtlich falsche Daten ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Kontrollinformationen setzen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 35 | Verfügbarkeit | Dienstleister Dataport | trägt absichtlich falsche Daten ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Kontrollinformationen setzen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 36 | Verfügbarkeit | Dienstleister MAZ | trägt absichtlich falsche Daten ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Kontrollinformationen setzen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 37 | Verfügbarkeit | Dienstleister MAZ | trägt absichtlich falsche Daten ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Kontrollinformationen setzen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 38 | Verfügbarkeit | Dienstleister MAZ | trägt absichtlich falsche Daten ein | Verarbeitung auf falschen Tatsachen, beeinflusst Auswahl | Finanzieller Verlust | Begrenzt (2) | Begrenzt (2) | Risiko (4) | Kontrollinformationen setzen | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | |
| 39 | Verfügbarkeit | Cyberkriminelle (Hacker / Schadsoftware) | erzeugen eine ungewöhnlich hohe Last (DoS) | führt zu Betriebsfehlern während der Laufzeit | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Anti DoS Recovery | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 40 | Verfügbarkeit | Cyberkriminelle (Hacker / Schadsoftware) | lassen Datenpakete verschwinden | führt zu Betriebsfehlern während der Laufzeit | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Fehlerrückmeldungen implementieren, Monitoring | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 41 | Verfügbarkeit | Cyberkriminelle (Hacker / Schadsoftware) | schneidet Daten des Betroffenen durch Schwachstelle | führt zu Betriebsfehlern während der Laufzeit | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Monitoring, revisionssichere Protokollierung | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 42 | Verfügbarkeit | Cyberkriminelle (Hacker / Schadsoftware) | schneidet Daten des Betroffenen durch Schwachstelle | führt zu Betriebsfehlern während der Laufzeit | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Monitoring, revisionssichere Protokollierung | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 43 | Verfügbarkeit | Hardwaredefekt (physikalisch) | führt zu Betriebsfehlern während der Laufzeit | führt zu Betriebsfehlern während der Laufzeit | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | Monitoring, revisionssichere Protokollierung | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 44 | Verfügbarkeit | Hardwaredefekt (physikalisch) | führt zu Betriebsfehlern während der Laufzeit | führt zu Betriebsfehlern während der Laufzeit | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Vernachlässigbar (1) | geringstes Risiko (2-3) | Monitoring, revisionssichere Protokollierung | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 45 | Verfügbarkeit | Softwarefehler | verhindert die Nutzung der Software | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Begrenzt (2) | Begrenzt (2) | geringstes Risiko (2-3) | Monitoring, revisionssichere Protokollierung | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 46 | Verfügbarkeit | Netzstörungen | führen zum Verlust von Datenpaketen | führt zu Betriebsfehlern während der Laufzeit | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | Mechanismen zur Recovery | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 47 | Verfügbarkeit | Verantwortlicher (Superadministrator) | wirken auf die Systeminfrastruktur | führt zu Betriebsfehlern während der Laufzeit | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Mechanismen zur Recovery | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 48 | Verfügbarkeit | Umwelteinflüsse (Naturgewalt) | wirken auf das Offsite-Backup | verhindert die interne Systemwiederherstellung | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | Mechanismen zur Recovery | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 49 | Verfügbarkeit | Umwelteinflüsse (Naturgewalt) | wirken auf das Offsite-Backup | verhindert die interne Systemwiederherstellung | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | Mechanismen zur Recovery | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 50 | Verfügbarkeit | Umwelteinflüsse (Naturgewalt) | wirken auf das Offsite-Backup | verhindert die interne Systemwiederherstellung | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | Mechanismen zur Recovery | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 51 | Datenspeicherung | Bewerberin | führt mehr Daten in das System ein als gefordert | Datenverarbeitung ohne Erforderlichkeit, Folgeverarbeitung mit Diskriminierung | Andere wirtschaftliche oder gesellschaftliche Nachteile | Wesentlich (3) | Begrenzt (2) | Risiko (5) | Kontrollieren vor Datenspeicherung | Begrenzt (2) | Begrenzt (2) | Risiko (4) | |
| 52 | Datenspeicherung | Mandant (Recruiter, Teledienst) | führt mehr Daten in das System ein als gefordert | Datenverarbeitung ohne Erforderlichkeit, Folgeverarbeitung mit Diskriminierung | Andere wirtschaftliche oder gesellschaftliche Nachteile | Wesentlich (3) | Begrenzt (2) | Risiko (5) | Kontrollieren vor Datenspeicherung | Begrenzt (2) | Begrenzt (2) | Risiko (4) | |
| 53 | Datenspeicherung | Dienstleister Dataport | führt mehr Daten in das System ein als gefordert | Datenverarbeitung ohne Erforderlichkeit, Folgeverarbeitung mit Diskriminierung | Andere wirtschaftliche oder gesellschaftliche Nachteile | Begrenzt (2) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 54 | Datenspeicherung | Dienstleister MAZ | führt mehr Daten in das System ein als gefordert | Datenverarbeitung ohne Erforderlichkeit, Folgeverarbeitung mit Diskriminierung | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 55 | Datenspeicherung | Softwarefehler | führt mehr Daten in das System ein als gefordert | Datenverarbeitung ohne Erforderlichkeit, Folgeverarbeitung mit Diskriminierung | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 56 | Datenspeicherung | Verantwortlicher (Superadministrator) | führt mehr Daten in das System ein als gefordert | Datenverarbeitung ohne Erforderlichkeit, Folgeverarbeitung mit Diskriminierung | Andere wirtschaftliche oder gesellschaftliche Nachteile | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 57 | Nichtverketzung (Zweckbind.) | Mandant (Recruiter, Teledienst) | verwendet Daten für andere Zwecke | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 58 | Nichtverketzung (Zweckbind.) | Dienstleister Dataport | verwendet Daten für andere Zwecke | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 59 | Nichtverketzung (Zweckbind.) | Dienstleister MAZ | verwendet Daten für andere Zwecke | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 60 | Nichtverketzung (Zweckbind.) | Cyberkriminelle (Hacker / Schadsoftware) | verwendet Daten für andere Zwecke | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 61 | Nichtverketzung (Zweckbind.) | Staatliche Institutionen (Nachrichtendienst) | verwendet Daten für andere Zwecke | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 62 | Nichtverketzung (Zweckbind.) | Staatliche Institutionen (Strafverfolgung) | verwendet Daten für andere Zwecke | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 63 | Nichtverketzung (Zweckbind.) | Gesetzestützungen | verwendet Daten für andere Zwecke | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 64 | Nichtverketzung (Zweckbind.) | Verantwortlicher (Superadministrator) | verwendet Daten für andere Zwecke | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 65 | Nichtverketzung (Zweckbind.) | Verantwortlicher (Superadministrator) | verwendet Daten für andere Zwecke | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 66 | Transparenz | Bewerberin | speichert die Protokolle fehlerhaft ab | speichert die Protokolle fehlerhaft ab | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 67 | Transparenz | Dienstleister Dataport | speichert die Protokolle fehlerhaft ab | speichert die Protokolle fehlerhaft ab | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 68 | Transparenz | Dienstleister Dataport | speichert die Protokolle fehlerhaft ab | speichert die Protokolle fehlerhaft ab | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 69 | Transparenz | Cyberkriminelle (Hacker / Schadsoftware) | speichert die Protokolle fehlerhaft ab | speichert die Protokolle fehlerhaft ab | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 70 | Transparenz | Softwarefehler | speichert die Protokolle fehlerhaft ab | speichert die Protokolle fehlerhaft ab | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 71 | Transparenz | Gesetzestützungen | speichert die Protokolle fehlerhaft ab | speichert die Protokolle fehlerhaft ab | Hinderung der Kontrolle der Betroffenen über eigene Daten | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | Kontrollieren vor Datenspeicherung | Vernachlässigbar (1) | Wesentlich (3) | Risiko (4) | |
| 72 | Intervenierbarkeit | Bewerberin | fordert Auskunft, aber der Prozess fehlt | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Begrenzt (2) | Wesentlich (3) | Risiko (4) | in Datenschutzmanagement integrieren | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 73 | Intervenierbarkeit | Mandant (Recruiter, Teledienst) | fordert Auskunft, aber der Prozess fehlt | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Begrenzt (2) | Wesentlich (3) | Risiko (4) | in Datenschutzmanagement integrieren | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 74 | Intervenierbarkeit | Dienstleister MAZ | fordert Auskunft, aber der Prozess fehlt | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Begrenzt (2) | Wesentlich (3) | Risiko (4) | in Datenschutzmanagement integrieren | Vernachlässigbar (1) | Begrenzt (2) | geringstes Risiko (2-3) | |
| 75 | Intervenierbarkeit | Cyberkriminelle (Hacker / Schadsoftware) | schließt Schadcode direkt in die Anwendung (SQL, etc.) | führt zu unvorhergesehenen Systemfehlern | Hinderung der Kontrolle der Betroffenen über eigene Daten | Wesentlich (3) | Maximal (4) | Risiko (6) | Sichere Softwareentwicklung, Testing | Begrenzt (2) | Maximal (4) | Risiko (6) | |
| 76 | Intervenierbarkeit | Verantwortlicher (Superadministrator) | schließt Schadcode direkt in die Anwendung (SQL, etc.) | führt zu unvorhergesehenen Systemfehlern | Hinderung | | | | | | | | |



Projekt

“Bewerbungsmanagementsystem Einführung“

Berechtigungskonzept

Projektleitung Zentrum für Personaldienste Hamburg

Friederike Vieth

ZPD 21 HR Digital 040 42805-2596

friederike.vieth@zpd.hamburg.de

Jannes Süpke

SK-ITD 42 (IT-Projektpool) 0176 42860979

jannes.suepke@sk.hamburg.de

Version: 1.6

Änderungshistorie

| Version | Datum | Änderung | Autor |
|---------|----------|---|---------------------|
| 0.1 | 02.04.20 | Ersterstellung | Selina Tong |
| 0.2 | 21.04.20 | Kapitel 3 Berechtigungssteuerung erstellt | Manfred Book |
| 0.5 | 07.05.20 | Einarbeitung von Anmerkungen des BMS-Teams | Manfred Book |
| 0.7 | 12.05.20 | Einarbeitung von Anmerkungen von milch & zucker | Manfred Book |
| 0.8 | 19.05.20 | Einarbeitung von Anmerkungen des BMS-Teams | Manfred Book |
| 0.9 | 15.06.20 | Inhaltliche Überarbeitung der Kapitel 4, 5 und 6 | Manfred Book |
| 1.0 | 19.06.20 | QS-Version | Manfred Book |
| 1.1 | 25.06.20 | Anmerkungen von Detlef Weber ZPD2 eingearbeitet | Manfred Book |
| 1.2 | 19.08.20 | Anmerkungen von Renate Pläßmann und Ralf Napijata (Datenschutzbeauftragter ZPD) eingearbeitet | Dr. Tobias Knobloch |
| 1.3 | 18.09.20 | Anmerkungen von Eicke Eddicks (Datenschutzbeauftragter PA) eingearbeitet | Dr. Tobias Knobloch |
| 1.4 | 03.12.20 | Ergänzungen der Rollen | Taylan Karakurt |
| 1.6 | 18.12.20 | Kapitel: 2.3 / 4.7 / 6.3 / 6.4 überarbeitet | Manfred Book |

Inhalt

| | | |
|----------|--|-----------|
| 1 | Glossar und Abbildungsverzeichnis | 4 |
| 2 | Einleitung | 6 |
| 2.1 | Projekthintergrund und Zielsetzung | 6 |
| 2.2 | Aufbau des Dokumentes | 6 |
| 2.3 | Zur Verwendung des Begriffs „Dienststelle“ | 6 |
| 3 | Administrative Zuständigkeiten | 7 |
| 3.1 | Administrative Trennung | 7 |
| 3.2 | Fachliche Leitstelle | 7 |
| 3.3 | FHH-Dienststellen | 8 |
| 3.4 | Interne BMS-Nutzende | 9 |
| 4 | Berechtigungssteuerung | 10 |
| 4.1 | BMS-Zugangsarten | 10 |
| 4.2 | Übersicht BMS-Benutzerverwaltung | 11 |
| 4.3 | Mandanten | 12 |
| 4.3.1 | Namenskonvention für Projekte | 12 |
| 4.3.2 | Projekte und Zuständigkeiten | 14 |
| 4.3.3 | Mandantenfähigkeit | 15 |
| 4.4 | Zugriffssteuerung auf Vakanzen | 15 |
| 4.5 | Fachliche Benutzergruppen | 17 |
| 4.6 | BMS-Benutzergruppen | 19 |
| 4.7 | Rolle Super-Administrator | 23 |
| 4.8 | Basis-Rollen | 24 |
| 4.8.1 | Basis-Rollen und Basis-Rechte | 24 |
| 4.8.2 | Neue Basis-Rollen anlegen | 26 |
| 5 | Administrative Prozesse | 27 |
| 5.1 | Einrichtung und Änderung von Benutzergruppen | 27 |
| 5.2 | Dokumentation der Berechtigungen | 27 |
| 5.3 | Interne Benutzer | 27 |
| 5.4 | Ändern der Zugriffsberechtigungen | 28 |
| 5.5 | Umgang mit internen Bewerbungen durch Verfahrensbeteiligte | 29 |
| 6 | Sicherheitskonzept BMS | 30 |
| 6.1 | Kennwortregeln | 30 |
| 6.2 | Sperrung von Kennungen nach langer Inaktivität | 30 |
| 6.3 | BMS-Datenbank | 30 |
| 7 | Anlagen zum Berechtigungskonzept | 31 |

1 Glossar und Abbildungsverzeichnis

Glossar

| Begriffe/ Abkürzung | Erläuterung |
|-----------------------|--|
| AD | Active Directory |
| Benutzergruppe | Über die Zugehörigkeit zu Benutzergruppen sind die Zugriffsrechte und Sichten in der BMS-Backend-Anwendung definiert. |
| Bewerbungsportal | Internetportal, in dem der Bewerber seine Daten und Bewerbungen ansehen und verwalten kann. |
| BMS | Bewerbermanagementsystem |
| BMS-Anwendung | Gesamtes BSM-System, umfasst die Backend-Anwendung und die Stellenportale (Frontend). |
| BMS-Backend-Anwendung | Bezeichnet den Teil der BMS-Anwendung, die von den internen Benutzern verwendet werden. |
| BMS-Sollprozess | Bezeichnet den neuen Bewerbungsprozess der FHH, der für angebundene Dienststellen mit BMS abgebildet wird. Technisch der Workflow im BMS |
| BMS-Stellenportale | Im Internet frei verfügbare Portale zur Darstellung der internen und externen Stellenanzeigen. |
| DSGVO | Datenschutzgrundverordnung |
| FB | Fachbereich |
| FHH | Freie und Hansestadt Hamburg |
| FL | Fachliche Leitstelle |
| ggf. | Gegebenenfalls |
| GSB | Gleichstellungsbeauftragte |
| KPT/HaSi | Kontenpflegetool / Hamburger Informationssysteme |
| HmbDSG | Hamburgisches Datenschutzgesetz |
| i.d.R. | in der Regel |
| OE | Organisationseinheit |
| PR | Personalrat |
| Projekt | Ein Ordnungsbegriff im BMS, der zur Strukturierung der Dienststellen und Zuständigkeiten verwendet wird. |
| PSB | Personalsachbearbeitung |
| Recruiter (R) | „Hüter des Verfahrens“, steuert federführend den gesamten Recruiting-Prozess. |
| SBV | Schwerbehindertenvertretung |
| SSO | Single Sign On |
| SteA | Stellenausschreibung |
| z.B. | zum Beispiel |

| Begriffe/ Abkürzung | Erläuterung |
|----------------------------|--|
| Vakanzen | Vakanzen sind in BMS ein übergreifendes Datenobjekt, zu dem der Recruiter Stellenanzeigen anlegt und zuständige Personen und Personengruppen zuordnet. |

Abbildungsverzeichnis

| | |
|--|----|
| Abbildung 1 BMS-Anwendung..... | 11 |
| Abbildung 2 Projekteintrag | 14 |
| Abbildung 3 Relationen einer Vakanz..... | 16 |

Hinweis: Alle Abbildungen wurden vom Autor für das Berechtigungskonzept erstellt.

2 Einleitung

2.1 Projekthintergrund und Zielsetzung

Für die Freie und Hansestadt Hamburg (FHH) soll eine integrierte und einheitliche Lösung für ein digitales Bewerbungsmanagementsystem (BMS) geschaffen werden. Hierzu wurde vom 02.01.2019 bis zum 31.10.2019 das „Projekt zur Vorbereitung und Durchführung eines Vergabeverfahrens zum Erwerb eines Bewerbungsmanagementsystems für die FHH“ (Projekt-ID: P0000901) umgesetzt. Dieses Projekt endete mit der Beschaffung der Software „BeeSite Recruiting Edition“ der Firma „milch & zucker AG“. Das am 01.06.2019 gestartete Einführungsprojekt zielt darauf ab, bis zum Projektende am 31.12.2021 für alle potenziellen Personal-Dienststellen die eingekaufte Software einzuführen.

Die BMS-Anwendung wird in der FHH von mehreren Behörden und Nutzern mit verschiedenen fachlichen Aufgaben genutzt. Das Berechtigungskonzept hat das zentrale Ziel einen reibungslosen, beherrschbaren und zugriffsgesteuerten Betrieb der BMS-Anwendung sicherzustellen und dabei gewährleisten, dass Nutzende ausschließlich Zugriff auf Daten haben, die für die Erledigung der ihr übertragenen Aufgaben benötigt werden. Die Umsetzung und Dokumentation des Berechtigungskonzeptes stellen sicher, dass

- die Administrierbarkeit der Benutzergruppen und Berechtigungen dauerhaft und praktikabel gegeben ist,
- das Minimalitätsprinzip gewahrt ist,
- ein hoher Wiederverwendbarkeitsgrad der einzelnen Benutzergruppen erreicht wird und
- eine hinreichende Dokumentation garantiert ist.

Dieses Dokument regelt nicht die Verwaltung von Berechtigungen der Entwicklungsumgebung oder Berechtigungen, die zur Installation des Systems benötigt werden. Weitere Ausführungen sind in dem Konzept zum Verfahrensbetrieb enthalten.

2.2 Aufbau des Dokumentes

Dieses Berechtigungskonzept wurde im Rahmen des Projekts Bewerbungsmanagement - Einführung (Projekt-ID: P0000936) erstellt und beschreibt die Verwaltung von Zugriffsrechten für das Produktivsystem des Bewerbungsmanagementsystems (BMS). Die wesentlichen Themenbereiche sind in drei Hauptkapitel gegliedert:

1. Im Kapitel 3 werden die fachlichen Zuständigkeiten aufgezeigt, die zur Umsetzung des Berechtigungskonzeptes notwendig sind.
2. Kapitel 4 beschreibt, wie Berechtigungen in der BMS-Anwendung definiert und administriert werden.
3. Kapitel 5 fasst Prozesse zusammen, durch die sich Auswirkungen auf die Benutzerrechte ergeben.

2.3 Zur Verwendung des Begriffs „Dienststelle“

In diesem Dokument wird der Begriff „Dienststelle“ allgemein für Verwaltungseinheiten mit eigener Personalverwaltung i.S. des § 6 Hamburgisches Personalvertretungsgesetz verwendet, die einen Bewerbungsprozess durchführen. Eine fachliche Differenzierung in Fachbehörden, Ämter, Gerichte, Landesbetriebe oder weitere Dienststellen ist für das Berechtigungskonzept nicht relevant. Ist es notwendig, Abhängigkeiten zwischen Dienststellen zu benennen, werden die Beziehungen als nachgeordnete Verwaltungseinheit oder weisungsbefugte Dienststelle gekennzeichnet.

Jede Dienststelle ist i.d.R. für ihre Bewerbungsprozesse eigenständig verantwortlich. Es sind auch organisatorische Ausnahmen möglich, in denen eine Dienststelle für sich selbst und für weitere nachgeordnete Verwaltungseinheiten die Bewerbungsverfahren durchführt.

Beispiel: Dem Personalamt sind die Landesbetriebe Zentrum für Personaldienste und ZAF/AMD nachgeordnet. Das Personalamt führt für sich selbst und den Landesbetrieb ZAF/AMD den Bewerbungsprozess durch.

In Kapitel 4.3.2 wird erläutert, wie die Berechtigungen und Zugriffe der BMS-Nutzenden auf die Vakanzen und Stellenanzeigen sowohl für einzelne Dienststelle als auch nachgeordneten Verwaltungseinheiten abgebildet werden können.

3 Administrative Zuständigkeiten

3.1 Administrative Trennung

Die Verwaltung und Pflege von Benutzerkonten in den Dienststellen und die Steuerung der Berechtigungen in der BMS-Anwendung durch die Fachliche Leitstelle sind getrennt organisiert. In diesem Kapitel werden die administrativen Zuständigkeiten aufgezeigt, die von den Dienststellen sowie der Fachlichen Leitstelle zur Umsetzung des Berechtigungskonzeptes zu beachten sind.

Die technische Umsetzung basiert auf dem Einsatz des länderübergreifenden Kontenpflege-tools (KPT) der FHH, umgangssprachlich auch „HaSi“ genannt (für Hamburger Informationssystem). KPT ist ein System zur Verwaltung von Benutzerkonten und Gruppenobjekten im Active Directory (AD). Zusätzlich werden im KPT die Organisationseinheiten der Dienststellen verwaltet, siehe Konzept „Länderübergreifendes Kontenpflege-tool“ von Dataport.¹

3.2 Fachliche Leitstelle

Für die Wahrnehmung einer übergreifenden Verantwortung zur Erfüllung fachlicher Aufgaben oder für Verfahren von besonderer Bedeutung soll eine Fachliche Leitstelle (FL) eingesetzt werden. Der Fachlichen Leitstelle obliegt entsprechend der Freigaberichtlinie der FHH insbesondere die Entwicklungsplanung, die fachliche, organisatorische Steuerung, auch der technischen Dienstleister, die Festlegung fachlicher Anforderungen, die Dokumentation, die Freigabe der Software und DV²-Verfahren sowie die Autorisierung und fortlaufende Qualifizierung der anwendenden Stelle(n) und Benutzenden. Die Fachliche Leitstelle hat die Rechte eines fachlichen Administrators und somit keinen Zugriff auf die Datenbank. Die Fachliche Leitstelle kann korrigierend auf Benutzerrechte eingreifen. Welcher Nutzende mit welcher Benutzergruppe in den Dienststellen auf das System zugreift, wird über die KPT Kontenpflegenden in den Behörden gesteuert (siehe 3.3). Die Fachliche Leitstelle ist somit nur unterstützendes Organ bei der Fehlerbehebung. Die Fachliche Leitstelle kann Bewerbungsvorgänge einsehen und darauf zugreifen. Dies ist erforderlich, um auftauchende Probleme im Prozessablauf zu analysieren und Maßnahmen einleiten zu können. Technisch wird das BMS auf der Ebene der Infrastruktur durch Dataport administriert, auf der Ebene der Datenbanken unter der Aufsicht von Dataport durch den Hersteller Milch und Zucker.

¹ Dateilink zum Konzept „[Länderübergreifendes Kontenpflege-tool](#)“ von Dataport

² Datenverarbeitung

Mit Bezug auf die BMS-Berechtigungsverwaltung führt die Fachliche Leitstelle folgende Aufgaben durch:

- Problemanalyse im Fall von Inkonsistenzen der Berechtigungen von BMS-Nutzern
- Entfernen der Zugriffsberechtigung einzelner Nutzer im Fehlerfall
- Hinzufügen oder Entfernen von Benutzergruppen und Berechtigungen
- Anpassung von Berechtigungen in bestehenden Benutzergruppen
- Korrektur fehlerhafter Organisationsstammdaten im BMS
- Administration und Konfiguration der BMS-Anwendung im laufenden Verfahrensbetrieb durch die Administratorberechtigung

Die Fachliche Leitstelle überprüft den Import von Daten aus dem übergreifenden Kontenpflegetool (siehe dazu den folgenden Abschnitt) und leitet, wenn notwendig, Maßnahmen zur Fehlerbehebung ein. Weitere Einzelheiten werden im Konzept zum Verfahrensbetrieb der Fachlichen Leitstelle festgelegt.

3.3 FHH-Dienststellen

Im Zuge der BMS-Anbindung einer Dienststelle werden die Mitarbeitenden, die das BMS nutzen, gemäß ihrer Funktion ermittelt. Die Mitarbeitenden werden einer oder mehreren BMS-Benutzergruppen zugeteilt. Die Zuordnung der Mitarbeitenden zu den jeweiligen BMS-Benutzergruppen wird in dem übergreifenden Kontenpflegetool (KPT) hinterlegt. Die Kontenpflegenden der FHH-Dienststellen ordnen die Mitarbeitenden der jeweiligen Dienststelle zu den im KPT hinterlegten AD-Gruppen, wie folgt zu:

| BMS-Benutzergruppe | KPT/AD-Gruppe (Beispiel) | Kommentar |
|-----------------------------|--|-----------------|
| Recruiter | ZPD BMS Recruiting (ROL-ZPD-BMS-R) | |
| Fachbereich | ZPD BMS Fachbereich (ROL-ZPD-BMS-FB) | |
| Personalsachbearbeitung | ZPD BMS Fachbereich (ROL-ZPD-BMS-PSB) | |
| Gleichstellungsbeauftragte | ZPD BMS Fachbereich (ROL-ZPD-BMS-GSB) | |
| Schwerbehindertenvertretung | ZPD BMS Fachbereich (ROL-ZPD-BMS-SBV) | |
| Personalrat | ZPD BMS Fachbereich (ROL-ZPD-BMS-PR) | |
| PA Fachkräfte | PA BMS Fachkräfte (ROL-PA-BMS-P34) | Nur Personalamt |
| PA Führungskräfte | PA BMS Führungskräfte (ROL-PA-BMS-P31) | Nur Personalamt |

Die Dateneingabe und -pflege im KPT wird dezentral in den Dienststellen wahrgenommen. Personendaten und Organisationsdaten können nur von den für diesen Bereich zuständigen Mitarbeitenden gepflegt werden. KPT ist für die BMS Anwendung das führende System zur Verwaltung folgender Daten:

- Organisationsdaten der Dienststelle
- Zuordnung der Dienststelle in die Organisationshierarchie
- Kennzeichnung der Mitarbeitenden, die Zugriff auf das BMS benötigen
- Zuordnung der Berechtigungsgruppen im Active Directory zu den BMS-Nutzenden

Im Active Directory (AD) werden AD-Benutzergruppen angelegt und durch die Datenpflegenden in den Dienststellen den BMS-Nutzenden, abhängig von deren Aufgaben im Bewerbungsprozess, zugeordnet. Die AD-Benutzergruppen bestehen aus Texteinträgen (Zeichenketten), die so aufgebaut sind, dass sie eindeutig einer Benutzergruppe in BMS zugeordnet werden können, siehe Tabelle: KPT/AD-Gruppe.

Die Definition der AD-Benutzergruppen wird zwischen der Fachlichen Leitstelle (FL) und den Dienststellen abgestimmt und dokumentiert. Die Anlage der AD-Benutzergruppen im Active Directory erfolgt dann durch die FL. Die Texteinträge der AD-Benutzergruppen definieren keine Berechtigungen, sondern sind nur Referenzen auf BMS-Benutzergruppen. Die Berechtigungen, die ein Nutzender in der BMS-Anwendung hat, werden ausschließlich durch die Benutzergruppe im BMS festgelegt. Kann, im Fehlerfall, eine AD-Benutzergruppe keiner BMS-Benutzergruppe zugeordnet werden, fehlen dem Nutzenden diese Berechtigungsgruppe und somit auch die dazugehörigen Berechtigungen in BMS.

Im Rahmen der BMS-Projekteinführung wird eine technische Schnittstelle vom KPT zur BMS-Anwendung erstellt. Über diese Schnittstelle werden die Organisationseinheiten und BMS-Nutzerstammdaten aus dem KPT ausgelesen und automatisiert in das BMS übertragen. Die Aktualisierung der Benutzerstammdaten erfolgt täglich. Die Qualitätssicherung koordiniert die Fachliche Leitstelle, die Dienststellen müssen im Zuge ihrer Zuständigkeit bei der Zuordnung der Mitarbeitenden zu den jeweiligen AD-Gruppen dabei mitwirken.

Änderungen bei den Mitarbeitenden, die Auswirkungen auf die Nutzung der BMS-Anwendung haben, können so von den Dienststellen gepflegt und hinterlegt werden. Ohne Anspruch auf Vollständigkeit führen folgende Ereignisse zu einer Änderung der Berechtigungen in der Backend-Anwendung des BMS:

- Neue Mitarbeitende in der Dienststelle benötigen einen BMS-Zugang
- Der BMS-Benutzende wechselt von einer Dienststelle zu einer anderen
- Der Benutzende wechselt, ändert oder verliert seine aktuelle BMS-Benutzergruppe

3.4 Interne BMS-Nutzende³

Die FHH-internen Mitarbeitenden melden sich in dem FHH-Netzwerk über Single-Sign-On (SSO) an und werden ohne Eingabe der Zugangsdaten authentifiziert.

Während des Anmeldevorgangs werden die AD-Benutzergruppen an das BMS übergeben und mit dem im BMS definierten Benutzergruppen abgeglichen. Die Autorisierung erfolgt über die Auswertung der AD-Benutzergruppen, die einem BMS-Nutzenden im KPT zugeordnet wurden. Kann eine AD-Benutzergruppe nicht eindeutig einer BMS-Benutzergruppe zugeordnet werden, wird diese ignoriert. Weichen die übermittelten AD-Benutzergruppen von den aktuellen Benutzergruppen im BMS ab, wird die Zuordnung der Benutzergruppen im BMS

³ Vgl. hierzu auch die Übersicht in Abschnitt 4.2 unten.

angepasst. Nach erfolgreicher Anmeldung sind dem Nutzenden somit immer die Benutzergruppen zugeordnet, wie sie der Benutzergruppenzuordnung im Active Directory entsprechen. Als Folge dieser Logik sieht ein Recruiter ausschließlich Verfahren, auf die er berechtigt ist. Verfahren - inklusive der dazugehörigen Daten, auf die er nicht berechtigt ist, sind somit für diesen Recruiter, nicht sichtbar. Organisatorisch wird zudem geregelt welcher Recruiter für welche Verfahren (Vakanzen) zuständig ist.

Sollten BMS-Nutzende nach der Anmeldung im BMS feststellen, dass sie nicht über ihre erforderlichen Berechtigungen verfügen, müssen sie sich an den First-level-Support oder den zuständigen KPT-Datenpflegenden ihrer Dienststelle wenden. Jeder BMS-Nutzende kann anhand der Inhalte seiner Cockpit-Ansicht im BMS erkennen, ob er über die erforderlichen Berechtigungen verfügt. In Kapitel 4.6. sind zu jeder BMS-Benutzergruppe die Inhalte der Cockpit-Ansichten aufgeführt.

4 Berechtigungssteuerung

4.1 BMS-Zugangsarten

Die BMS-Anwendung ist eine Lösung für den gesamten Bewerbungsprozess. Dies umfasst die Internetpräsenz mit den internen und externen Stellenportalen und dem Bewerbungsportal, in dem Bewerbende ihre persönlichen Daten und Bewerbungen verwalten können. Zur Durchführung der BMS-Sollprozesse verfügt die BMS-Backend-Anwendung über eine browserbasierte Benutzeroberfläche, die von den Mitarbeitenden der FHH genutzt wird. In den Stellenportalen werden die internen oder externen Stelleanzeigen (SteA) angezeigt.

Aus Sicht der Benutzenden besteht die gesamte BMS-Anwendung somit aus zwei Komponenten, den Internetportalen inklusive Benutzerportal (Frontend) und der Bewerbungsverwaltung, der sogenannten BMS-Backend-Anwendung. IT-Technisch⁴ handelt es sich bei der BMS-Anwendung um ein integriertes Softwaresystem. Die logische Benutzerperspektive ist in der folgenden Abbildung dargestellt.

⁴ Die IT-Infrastruktur ist im Sollkonzept/Betriebshandbuch zur EHdB beschrieben.

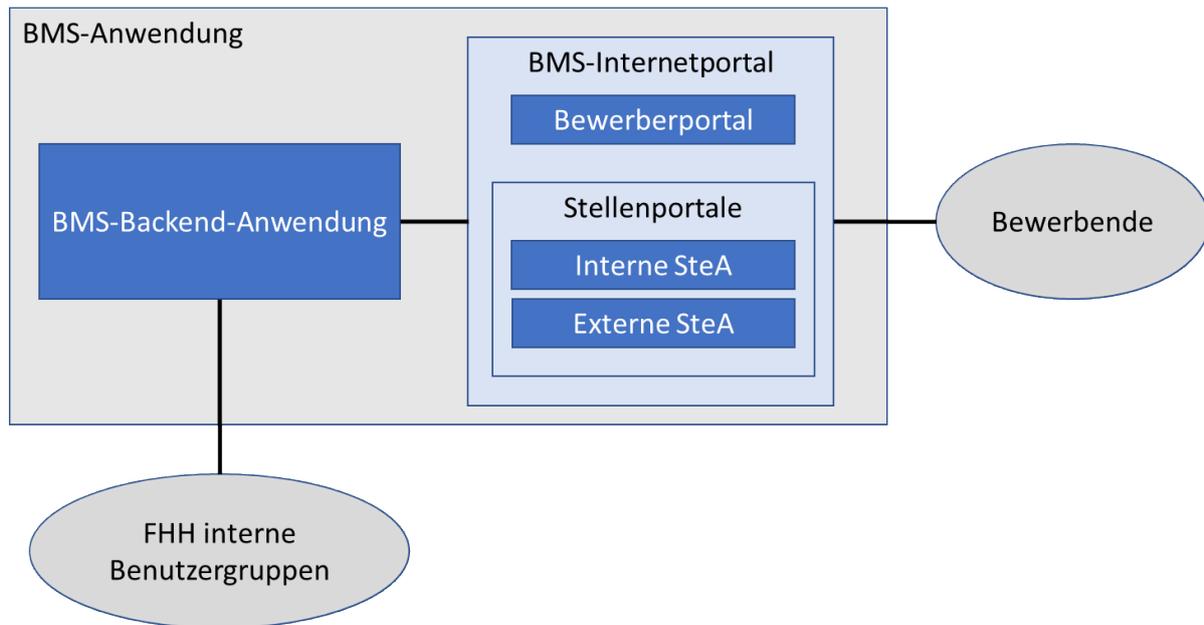


Abbildung 1 BMS-Anwendung

Die BMS-Backend-Anwendung umfasst die Speicherung der Daten und steuert den Bewerbungsprozess. Die Mitarbeitenden der FHH-Dienststellen werden über Single-Sign-On (SSO) ohne erneute Eingabe der Zugangsdaten an die BSM-Backendanwendung angemeldet, wenn sie sich im FHH-internen Netzwerk befinden. Damit FHH-Benutzende, wie in Kapitel 3.4 beschrieben, sich in der BMS-Backend-Anwendung anmelden können, müssen sie für die Nutzung der Anwendung im KPT registriert sein. Die Berechtigungen der Benutzenden werden über die Benutzerverwaltung der BMS-Backend-Anwendung definiert, siehe dazu Kapitel 4.2 bis 4.8.

Bewerbende können beispielsweise über das Karriereportal von hamburg.de auf das interne oder externe Stellenportal zugreifen. Initiativbewerbungen werden im BMS aktuell weder gespeichert noch bearbeitet. Ein Überblick über den Aufbau der Stellenportale wird in Kapitel III. des Fachkonzepts gegeben. Bewerbende können sich optional registrieren und erhalten somit Zugang zum Bewerbungsportal, wo Stellenanzeigen, Favoriten und persönliche Daten angezeigt und bearbeitet werden können.

Die Berechtigungen für den Zugang zum Bewerbungsportal und der BMS-Backend-Anwendung sind systemtechnisch strikt getrennt. Dadurch ist sichergestellt, dass Bewerbende nur Zugriff auf die Stellenportale und nach erfolgreicher Registrierung auf die Funktionen im Bewerbungsportal erhalten.

4.2 Übersicht BMS-Benutzerverwaltung

In der BMS-Backend-Anwendung können die Berechtigungen von BMS-Benutzenden von der Fachlichen Leitstelle (FL) eingesehen und verwaltet werden. Dazu werden die zuständigen Mitarbeitenden der FL im BMS der Administratorengruppe zugeordnet.

Mit der BMS-Oberfläche des Administrators können interne und externe Benutzende, Benutzergruppen und Anmelde- und Passwortregeln verwaltet werden. In der BMS-Anwendung werden folgende Kategorien verwendet:

| Kategorie | Beschreibung |
|-------------------------|--|
| Interne Benutzer | Wie in Abschnitt 4.1 eingeführt, haben interne Benutzende Zugriff auf die BMS-Backend-Anwendung. Im FHH-Netzwerk werden interne Benutzende (FHH Nutzende) über Single-Sign-On (SSO) angemeldet. |
| Interne Benutzergruppen | Eine Benutzergruppe fasst identische Aufgaben, Zugriffsrechte und Spracheinstellungen zusammen. Benutzende sind mindestens einer Benutzergruppe zugeordnet. Die FL kann neue Benutzergruppen anlegen und deren Berechtigungen und Zugriffe administrieren. |
| Externe Benutzer | Externe Benutzende der BMS-Anwendung sind Bewerbende, die das BMS-Frontend (internes oder externes Stellenportal) nutzen. |
| Externe Benutzergruppen | In der BMS-Backend-Anwendung können externe Benutzergruppen für externe Benutzende angelegt werden. In der FHH werden keine externen Benutzergruppen benötigt und somit auch nicht verwaltet. |
| Administrator | In der FHH erhält nur die Fachliche Leitstelle Administratorrechte. Außer der FL erhalten Service-Mitarbeitende der Firma milch & zucker personalisierte Zugänge mit Administratorberechtigung, um Fehlerbehebungen und Systemaktualisierungen vorzunehmen. ⁵ Die Zugriffe von milch & zucker auf die BMS Anwendung erfolgt unter strikter Kontrolle durch Dataport und nur auf Auftrag durch die FL. Die Zusammenarbeit zw. Dataport und milch & zucker ist in einer Clientvereinbarung geregelt. Falls milch & zucker auf die Produktions- oder Pre-Produktions-Umgebung zugreifen muss, erfolgt dies unter Kontrolle von Dataport (4-Augen Prinzip). Der Zugriff erfolgt nur für die Analyse von schwerwiegenden Problemen in der Produktion. |

4.3 Mandanten

4.3.1 Namenskonvention für Projekte

Die Trennung der Zugriffsrechte zwischen den Dienststellen und den einzelnen Mitarbeitenden erfolgt durch die Steuerung der Zugriffsberechtigung in der BMS-Anwendung. Alle FHH-Dienststellen, die die BMS-Anwendung nutzen, verwenden dieselbe technische IT-Infrastruktur.

Die Mandantentrennung stellt sicher, dass BMS-Benutzende, siehe Kapitel 4.5, nur auf die Daten ihrer zugeordneten Dienststellen zugreifen können. In der BMS-Backend-Anwendung erfolgt die Abbildung unterschiedlicher Dienststellen und Zuständigkeiten durch den sogenannten „Projektstrukturbaum“. Der Terminus „Projekt“ ist ein Begriff in der BMS-Anwendung und kann hier im Sinne von Bewerbungsverfahren interpretiert werden. Projekte werden dazu verwendet, um den Bewerbungsprozess mit den dazugehörigen Vakanzen,

⁵ Nach aktuellem Stand erhalten die 3rd-Level Service-Mitarbeitenden die gleichen Administratorberechtigungen wie die FL. Wenn erforderlich, kann eine zusätzliche Benutzergruppe „M+Z Administrator“ für die Service-Mitarbeitenden in Abstimmung mit der FL erstellt werden.

Stellenanzeigen und Bewerbungen auf Dienststellen und Personalamtsbereiche einzugrenzen und zu strukturieren.

In der BMS-Backend-Anwendung ist die FL zuständig für die Verwaltung des Projektstrukturbaums. Der Projektstrukturbaum bildet im BMS eine Logik ab, nach welcher für jedes Projekt individuelle Zugriffsrechte gesteuert werden. Durch das Projekt wird auch die Beteiligung des Personalamtes festgelegt. Das bedeutet, dass die fachliche Zuteilung der Vakanzen bereits mit deren Anlage im BMS erfolgt und nicht intern in Abstimmung zwischen den Abteilungen P 31 und P 34. Auf Grund der spezifischen Zuständigkeiten im Personalamt werden für jede Behörde drei Projekteinträge angelegt:

| Projektbezeichnung | Erläuterung |
|---|---|
| <Behörde ⁶ > Stellen bis A/E14 | <p>Die zuständigen Mitarbeitenden aus P 34 werden im BMS- Prozess eingebunden für Stellen der Wertigkeit bis A/E14, für die Qualitätssicherung der Stellenanzeigen und der Kandidatenprüfung. In P 34 gibt es zwei Teams:</p> <ul style="list-style-type: none"> • P 342 übernimmt die Eingabe und die Veröffentlichung der Stellenanzeigen für Dienststellen, die nicht an BMS angebunden sind. P 341 verantwortet die QS der Stellenanzeigen und die Prüfung und das Vorschlagswesen der intern kandidierenden Personen. |
| <Behörde> Stellen ab A/E15 | <p>Die zuständigen Mitarbeitenden aus P 31 haben Zugriffsrechte auf die Vakanzen und ab Bewerbungseingang ein Sichtrecht auf das gesamte Ausschreibungsverfahren für Stellen der Wertigkeit ab A/E15.</p> <p>Die zuständigen Mitarbeitenden aus P 31 werden im BMS- Sollprozess eingebunden für Stellen der Wertigkeit ab A/E15, für die Qualitätssicherung der Stellenanzeigen und der Kandidatenprüfung.</p> |
| <Behörde> Stellen Ärzte | <p>Die zuständigen Mitarbeitenden aus P 31 werden im BMS- Sollprozess eingebunden für Stellen der Ärzte, für die Qualitätssicherung der Stellenanzeigen und der Kandidatenprüfung.</p> |

Damit eine möglichst hohe Transparenz für die Benennung der Projekte besteht, wird nach der Behördenbezeichnung ein konstanter Zusatz, wie in der obigen Tabelle beschrieben, angefügt, die genaue Bezeichnung ist zu klären.

Im Zuge der Projekteinführung wird dieser Strukturbaum initial mit Daten befüllt. Die Bezeichnung der Projekte kann vom BMS-Administrator auch zu einem späteren Zeitpunkt geändert werden. Ebenso können manuell neue Projekte angelegt werden.

⁶ Platzhalter für die genaue Bezeichnung der personalverwaltenden Dienststelle, z.B. BA Nord, BIS (für die Kernverwaltung) bzw. Polizei Hamburg oder Feuerwehr Hamburg mit eigener Personalverwaltung.

4.3.2 Projekte und Zuständigkeiten

Damit ein Projekteintrag die Zuständigkeiten erhält, die er gemäß seiner Namensgebung erhalten soll, muss das Projekt entsprechend aufgesetzt werden. Dazu werden dem Projekt eine Organisationseinheit und die zuständigen Personen zugeordnet.

Zur Veranschaulichung zeigt die nachfolgende Abbildung einen Ausschnitt aus einem möglichen Projektbaum für das Personalamt mit den drei Kombinationen der Projekte, wie in Abschnitt 4.3.1 beschrieben.

Wie in der Abbildung 2 dargestellt, ist dem Projekt „PA – Stellen bis A/E14“ eine Organisationsstruktur zugeordnet. Mittels Auswahllisten werden das zuständigen Recruiting und Mitarbeitenden aus dem Personalamt zugeordnet. Zusätzlich wird ein verantwortlicher für das Recruiting, der der Benutzergruppe Recruiter angehört, für das jeweilige Projekt festgelegt.

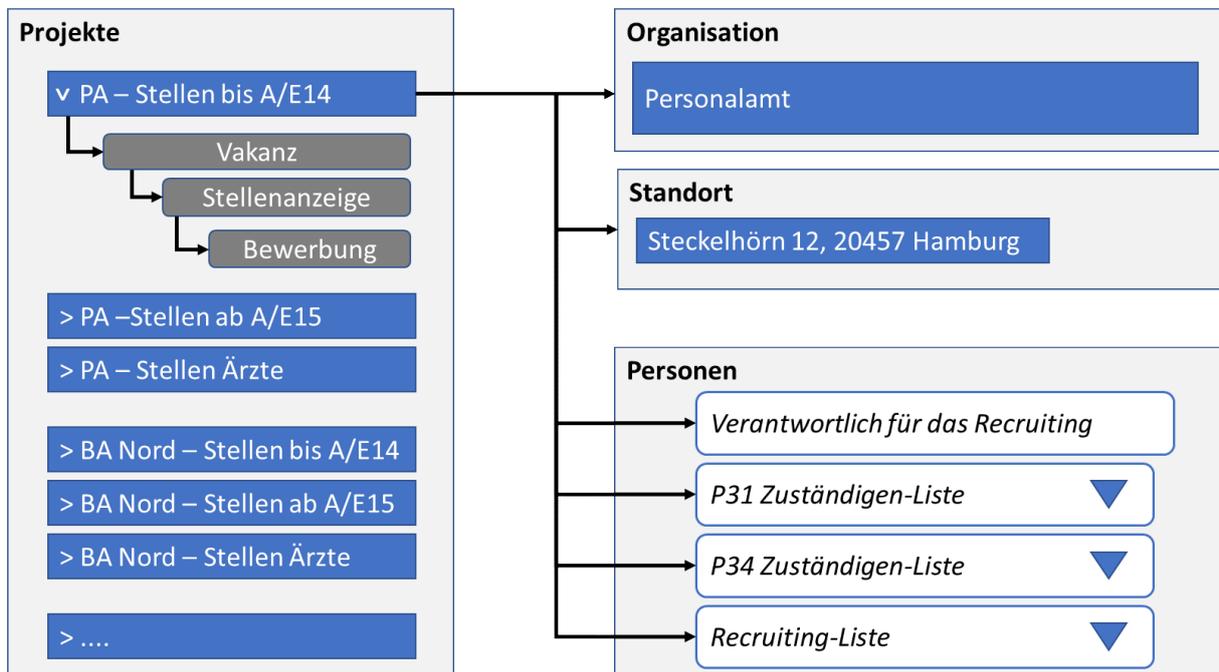


Abbildung 2 Projekteintrag

Auswahl Gesellschaft und Standorte

Die Zuordnung einer Dienststelle zu einem Projekteintrag wird durch die zugeordnete Organisationseinheit im BMS definiert. In dem Beispiel (siehe Abbildung 2) handelt es sich dabei um das Personalamt. Jeder Vakanz wird auch einer Standortadresse zugeordnet.

Somit definiert ein Projekt eine FHH Behörde oder Dienststelle für die Bewerbungsverfahren durchgeführt werden. Für jedes Bewerbungsverfahren wird eine Vakanz zu diesem Projekt (FHH Behörde oder Dienststelle) angelegt.

Nicht jede FHH Dienststelle oder auch Behörde führt ihre Bewerbungsverfahren in Personalunion selber durch. Zum Beispiel führt das Personalamt die Bewerbungsverfahren für sich selbst und nachgeordneten Verwaltungseinheiten durch. Damit auch hier die richtigen Zuständigkeiten abgebildet werden, werden für jede nachgeordnete Verwaltungseinheit eigene Projekte angelegt und den zuständigen Recruiting Personen aus dem Personalamt zugeordnet.

Auswahllisten Personen

Im Menü zur Konfiguration der Projekte stehen mehrere Auswahllisten zur Verfügung, um Personen einem Projekteintrag zuzuordnen. Jede Auswahlliste repräsentiert eine bestimmte Personengruppe. Jede Person in der Auswahlliste ist auch gleichzeitig BMS-Backend-Nutzender. Folgende Auswahllisten stehen zur Verfügung:

| Personengruppe | Beschreibung |
|------------------------------------|---|
| Verantwortliche für das Recruiting | Auswahl einer Person als Hauptverantwortlicher des Projektes (Hüter des Verfahrens), die der Benutzergruppe Recruiting zugeordnet ist. |
| P 31 Zuständige | Multiselektionsauswahl ⁷ , angezeigt werden alle Personen, die der Benutzergruppe Personalamt Führungskräfte (P 31) zugeordnet sind. |
| P 34 Zuständige | Multiselektionsauswahl, angezeigt werden alle Personen, die der Benutzergruppe Personalamt Fachkräfte (P 34) zugeordnet sind. |
| Recruiting | Multiselektionsauswahl, angezeigt werden alle Personen, die der Benutzergruppe Recruiting zugeordnet sind. |

Wird ein neues Projekt eingerichtet muß mit der Fachlichen Leitstelle vereinbart werden, wer die führenden Recruiting Personen und die zuständigen Personen aus dem Personalamt sind, die für die zugeordnete FHH Dienststelle (= Gesellschaft) zuständig sind.

4.3.3 Mandantenfähigkeit

Die Pflege der Projektbaumstruktur mit der Zuordnung zu den Organisationen und Personengruppen erfolgt durch die Fachliche Leitstelle. Zur Verwaltung in der BMS-Backend-Anwendung sind Administratorrechte erforderlich.

Das Recruiting kann nur zu den Projekteinträgen, denen es zugeordnet sind, Vakanzen anlegen, diese einsehen und den Recruiting-Prozess anstoßen. Analoges gilt für die Zuordnung der Mitarbeitenden aus dem Personalamt. Mitarbeitende aus den Referaten P 31 und P 34 sind nur an Recruiting-Prozessen beteiligt, wenn sie den entsprechenden Projekten zugeordnet wurden. Um die geforderte Trennung der Zuständigkeiten von P 31 und P 34 zu erreichen, werden den Projekten jeweils nur Personen aus dem Bereich P 31 oder P 34 zugeordnet.

4.4 Zugriffssteuerung auf Vakanzen

Vakanzen sind in der BMS-Anwendung die Datenobjekte, an denen die Stellenausschreibungen verankert sind. Zu einer Vakanz können interne und externe Stellenausschreibungen (SteA) erstellt werden.

Eine Vakanz ist in der BMS-Anwendung das zentrale Datenobjekt, dem alle relevanten Informationen zugeordnet werden. Das folgende Diagramm veranschaulicht die berechtigungsrelevanten Relationen mit der Vakanz als zentralem Datenobjekt.

⁷ Erläuterung des Begriffs „Multiselektionsauswahl“ (gilt auch für die folgenden Zeilen): Die Zuständigkeit von P31 u. P34 erstreckt sich auf die Stellenbesetzungsverfahren aller FHH-Dienststellen für Führungskräfte bzw. Fachkräfte. Das Recruiting hat eine fachliche Zuordnung zu einer bestimmten Dienststelle („Gesellschaft“). Einem Projekt können jeweils mehrere zuständige Personen zugeordnet werden.

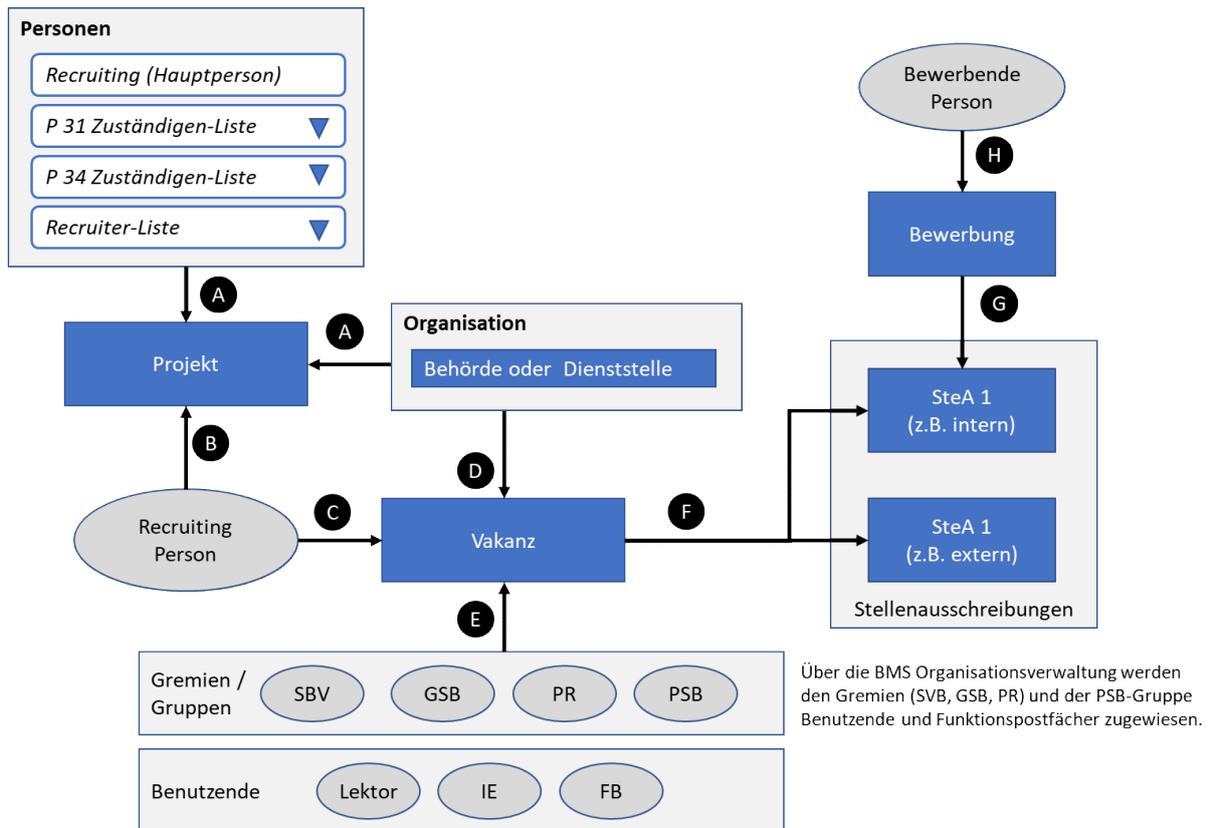


Abbildung 3 Relationen einer Vakanz

Wie in Abschnitt 4.3 ausgeführt, werden Projekte auf Dienststellen und bestimmte Benutzergruppen (Recruiting, Personalamt P 31 oder P 34) eingeschränkt. Vakanz werden durch Benutzende mit Recruiting-Berechtigungen angelegt.

Die folgende Tabelle beschreibt die Relationen zwischen wesentlichen Datenobjekten, Personen und Personengruppen, die im Diagramm als Pfeile dargestellt sind. Durch diese Beziehungen ergeben sich Zuständigkeiten und Abhängigkeiten.

| Relation | Beschreibung |
|----------|---|
| (A) | Bei der Projektanlage wird dem betreffenden Projekt genau eine Behörde zugeordnet. Wie in Kapitel 4.3 erläutert, werden zusätzlich Recruiting und Personen aus dem Personalamt zugeordnet. |
| (B) | Recruiting kann eine Vakanz nur zu einem Projekt anlegen, dem es als Recruiting zugeordnet wurde, siehe Relation (A). Recruiting arbeiten somit immer nur auf Projekten, denen es zugeordnet ist.. |
| (C) | Recruiting legt im BMS eine Vakanz an. Eine Vakanz ist immer genau mit einem Projekt verknüpft. |
| (D) | Der Vakanz kann nur die Organisationsstruktur, die auf Grund der Relation (A) zum Projekt hinterlegt wurde, zugeordnet werden. Durch das BMS-Datenfeld „Gesellschaft“ ist die zuständige Dienststelle eindeutig festgelegt. |
| (E) | Das Recruiting ordnet der Vakanz Gremien zu: Schwerbehindertenvertretung (SBV), Gleichstellungsbeauftragte (GSB), Personalrat (PR), |

| Relation | Beschreibung |
|----------|---|
| | <p>Personalsachbearbeitung (PSB)-Gruppen. Des Weiteren können Personen für die Rolle Fachbereich (FB), Lektor (L) und Informationsempfänger (IE) ausgewählt werden.⁸</p> <p><u>Hinweis:</u> Die Gremien und PSB-Gruppe sind über die BMS-Organisationsverwaltung mit Personen (Benutzern) und einem Funktionspostfach verknüpft. In den Auswahllisten werden nur die Gruppen angezeigt, die zu der Behörde gehören, die in der Organisationseinheit „Gesellschaft“ steht.</p> <p>Für die Rolle Lektor und IE stehen alle BMS-Benutzende zur Auswahl. Für die Rolle Fachbereich stehen alle Benutzende zur Auswahl, die der BMS-Benutzergruppe Fachbereich angehören.</p> |
| (F) | <p>Auf Basis der Vakanz werden vom Recruiting Stellenausschreibungen erstellt. Die in der Vakanz zugeordnete Dienststelle (=Gesellschaft) wird als Dienststelle in der SteA in den Stellenportalen angezeigt. Wurde auch ein Standort zur Vakanz ausgewählt, wird diese als untergeordnete Verwaltungseinheit übernommen. Die Adresse der SteA wird durch die Auswahl des Standortes festgelegt.</p> <p><u>Hinweis:</u> In der SteA können die Textbausteine für die Dienststelle und der nachgeordneten Verwaltungseinheit überschrieben werden.</p> |
| (G) | <p>Der Stellenausschreibung wird eine Bewerbung zugeordnet, sobald sich Bewerbende auf diese bewerben.</p> |
| (H) | <p>Bewerbende erstellen eine Bewerbung.</p> <p><u>Hinweis:</u> Reichen Bewerbende mehrere Bewerbungen ein, die einer Dienststelle zugeordnet sind, so kann das Recruiting, dieser Dienststelle, die Mehrfachbewerbung einsehen. Bewirben sich Bewerbende bei unterschiedlichen Dienststellen, die im BMS verschiedenen Projekten zugeordnet sind, kann das Recruiting die Bewerbung aus dem anderen Projekt (Dienststelle) nicht einsehen, wenn es dem Projekt nicht zugeordnet ist. .</p> |

4.5 Fachliche Benutzergruppen

In Kapitel 2 des Fachkonzepts werden die fachlichen Benutzergruppen im BMS-Sollprozess beschrieben. Diesen fachlichen Benutzergruppen werden in der BMS-Anwendung durch die BMS-Benutzergruppen (vgl. Abschnitt 4.6) unterschiedliche Ansichten und Berechtigungen zugewiesen.

In diesem Abschnitt werden die fachlichen Benutzergruppen tabellarisch zusammengefasst. Weiterführende Informationen können dem Fachkonzept entnommen werden. In der Spalte Prozessbeteiligung wird gekennzeichnet, ob die Benutzergruppen aktiv oder passiv am BMS-Sollprozess beteiligt sind. In der Spalte Intern/Extern ist gekennzeichnet, ob die Rolle einer internen oder externen Benutzergruppe angehört (vgl. Abschnitt 4.2).

⁸ Die Funktionen dieser Rollen werden zusammenfassend in Abschnitt 4.5 unten erläutert.

| Fachliche Benutzergruppe | Aufgabe/Funktion im BMS-Prozess | Prozessbeteiligung | Intern / Extern |
|------------------------------|---|--------------------|-----------------|
| Recruiting | Fungiert gemäß Lenkungsgruppen-Entscheidung vom 13. Januar 2020 als „Hüter des Verfahrens“: Steuert federführend den gesamten Recruiting-Prozess, ist insbesondere verantwortlich für die Sichtung der Bewerbungen, die Prüfung der formalen Eignung der Bewerbung sowie die Erstellung des Bewerbungsvergleichs und die Dokumentation der Auswahlentscheidung. | Aktiv | Intern |
| Fachbereich | Ist auftraggebende Person für zu besetzende Stellen in seinem Bereich, trägt die fachliche Verantwortung für die Ausschreibung und die Besetzung der Vakanz. | Aktiv | Intern |
| PA Führungskräfte | P 31 (Führungskräftegewinnung und -entwicklung) verantwortet alle Ausschreibungen ab A/E15 und ist bei diesen Stellen auch an der Auswahl beteiligt. Benutzende erhalten Sichtrecht auf das gesamte Verfahren und verfügen über einen Zustimmungsvorbehalt. | Aktiv | Intern |
| PA Fachkräfte | P 34 (Personalgewinnung, Beratung und Controlling) teilt sich in zwei Teams auf. Verantwortet die Qualitätssicherung der Stellenanzeigen und die Kandidatenprüfung. | Aktiv | Intern |
| Personalrat | Die Einbindung des Personalrats erfolgt gemäß Hamburgischem Personalvertretungsgesetz. | Aktiv | Intern |
| Schwerbehinderte nvertretung | Die Einbindung der Schwerbehindertenvertretung erfolgt gemäß SGB IX. | Aktiv | Intern |
| Gleichstellungsbeauftragte | Die Einbindung der Gleichstellungsbeauftragten erfolgt gemäß Hamburger Gleichstellungsgesetz. | Aktiv | Intern |
| Informationsempfangende | Werden im Recruiting-Prozess über ausgewählte Prozessschritte per Mail informiert, eine aktive BMS-Nutzung ist nicht vorgesehen. ⁹ | Passiv | Intern |

⁹ Bei der Rolle „Informationsempfänger“ handelt es sich um eine Sonderrolle zur informativen Beteiligung höherer Hierarchieebenen. Personenbezogene Daten werden hier nur an einer Stelle übermittelt, nämlich bei der Benachrichtigung über die Zustimmung des Personalrats (Name der bewerbenden Person).

| Fachliche Benutzergruppe | Aufgabe/Funktion im BMS-Prozess | Prozessbeteiligung | Intern / Extern |
|--------------------------|--|--------------------|-----------------|
| Lektor | Die Lektorrolle ermöglicht das Lektorieren einer SteA im BMS in einem eigens dafür vorgesehenen Widget. Diese Rolle kann das Recruiting z.B. einer Führungskraft aus dem Fachbereich zuordnen. Außer der Stellenanzeige kann der Lektor nichts sehen oder verändern. | Aktiv | Intern |
| Personalsachbearbeitung | Verantwortet die Einstellung der bewerbenden Person nach der Auswahl und ist damit nicht Teil des Recruiting-Prozesses. Für den Zugriff auf die einstellungsrelevanten Unterlagen erhält die Personalsachbearbeitung Zugriff auf ein separates Cockpit im BMS. | Passiv | Intern |
| Fachliche Leitstelle | Die Fachliche Leitstelle ist zentrale Anlaufstelle für das BMS im laufenden Verfahrensbetrieb. | Passiv | Intern |
| Bewerbende Person | Die bewerbende Person ist Teil des Recruiting-Prozesses und erhält Informationen über das BMS-Portal (intern oder extern). Im Portal kann sie ihre Daten aktualisieren. | Aktiv | Extern |

4.6 BMS-Benutzergruppen

Die Abbildung der unterschiedlichen Benutzerprofile und die benötigten Rollen in der BMS-Anwendung erfolgt durch die Definition von Benutzergruppen. Im BMS können nach Bedarf weitere Benutzergruppen durch die Fachliche Leitstelle angelegt werden.

Im BMS ist jeder Benutzergruppe genau einer BMS-Basisrolle zugewiesen. Eine Benutzergruppe hat häufig den gleichen Namen wie die dazugehörige Basisrolle. Die Bezeichnungen der Benutzergruppen können von der Administration geändert werden. Anpassungen in den Bezeichnungen sind also möglich, ändern aber nichts an ihrer Bedeutung. Die Basisrollen definieren im BMS eine bestimmte Obermenge an Basisberechtigungen und wurden in der Projekteinführung an die Anforderungen der FHH angepasst.¹⁰

Im Folgenden werden für jede BMS-Benutzergruppe die BMS-Module und -Widgets in der Cockpit-Ansicht aufgeführt. Im BMS ist ein Widget eine kleine Komponente in der grafischen Ansicht (Cockpit), die Informationen anzeigt und Aktionen zur Verfügung stellt. Widgets basieren auf einem vorhandenen elementaren Datenobjekt (Widget Typ) im BMS und werden für die Cockpit-Ansichten und benötigten Verwendungszwecke der jeweiligen Benutzergruppe konfiguriert. Welche Aktionen (Lesen, Schreiben, Ausführen) ein Nutzer in einem Widget ausführen kann, wird durch seine Basisrollen definiert, die seiner Benutzergruppe zugeordnet

¹⁰ Da Doppelrollen technisch nicht ausgeschlossen sind, muss die Fachliche Leitstelle vor allem darauf achten, dass die fachlichen Dienststellen keine Administratorenrechte besitzen.

ist. Die Cockpit-Ansichten, d. h. Zusammenstellung der Widgets, werden pro BMS-Benutzergruppe konfiguriert.

Hat eine Benutzergruppe Zugriff auf bestimmte Module im BMS, werden diese genannt. BMS-Module sind getrennte Benutzeransichten mit einem speziellen erweiterten Funktionsumfang. Module stellen erweiterte Funktionen zur Verfügung, weshalb nur bestimmte Benutzergruppen Zugriff auf einzelne Module haben.

Benutzergruppe: Administrator

| | Beschreibung |
|--|--|
| BMS-Basisrolle | Administrator |
| BMS-Module | Projekte, Bewerbungssuche, Talentpools, Terminplaner, Fragebögen |
| Administration | Benutzer, Cockpit-Manager, Auswahllisten, Pools, Organisation, Reminder, Masterfragebögen, Medienbibliothek |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Nicht zuordbare E-Mails <widgetEmailJunk> - Zuletzt bearbeitet <widgetLastUpdate> |

Benutzergruppe: Recruiter

| | Beschreibung |
|--|---|
| BMS-Basis-Rolle | Recruiter |
| BMS-Module | Projekte, Bewerbersuche, Talentpools ¹¹ , Terminplaner |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Hilfe <QuickHelp> - Suche < widgetSearchResult> - E-Mails < widgetEmailInbox> - Aufgaben: Bewerber <GenericReminder> - Aufgaben: Vakanzen <GenericReminder> - Aufgaben: Stellenanzeigen <GenericReminder> - Terminübersicht <AppointmentWidget> - Meine Vakanzen <widgetMyVacancy> - Zuletzt bearbeitet <widgetLastUpdate> - Daten-Matrix <widgetDataMatrix> |

¹¹ Dieses Modul wird zum Start der Piloten nicht genutzt werden.

Benutzergruppe: Fachbereich (Führungskräfte)¹²

| | Beschreibung |
|--|---|
| BMS-Basis-Rolle | Fachbereich |
| BMS-Module | <i>keine</i> |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Hilfe <QuickHelp> - Bewerbung zur formalen Prüfung <ExtendedCandidate> - Nicht zur Einladung empfohlene Bewerbungen (B-Kandidaten) <ExtendedCandidate> - Bewerbungsvergleich <ExtendedCandidateWidget> - Bewerbungen im Einstellungsprozess <ExtendedCandidate> - Bewerbungen zur formalen Prüfung <ExtendedCandidate> - Meine Vakanzen <widgetMyVacancy> |

Benutzergruppe: Lektor

| | Beschreibung |
|--|--|
| BMS-Basis-Rolle | Lektor |
| BMS-Module | <i>keine</i> |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Hilfe <QuickHelp> - Weitergeleitete Stellenanzeigen <LectorJobadWidget> |

Benutzergruppe: PA Führungskräfte (P31)

| | Beschreibung |
|--|---|
| BMS-Basis-Rolle | PA Führungskräfte |
| BMS-Module | <i>keine</i> |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Suche <widgetSearchResult> - Hilfe <QuickHelp> - Aktive Stellenanzeigen <GenericJobadWidget> - Einzustellende Bewerbungen <ExtendedCandidate> - Bewerbungen zur Stellungnahme <ExtendedCandidate> - Vakanzen <widgetMyVacancy> |

¹² Hierzu zählen alle Führungskräfte, die im KPT als solche hinterlegt sind. Zusätzlich können Dienststellen über einen Genehmigungsprozess weitere Personen (z.B. Vertreter) bei der Fachlichen Leitstelle anmelden.

Benutzergruppe: PA Fachkräfte (P34)

| | Beschreibung |
|--|--|
| BMS-Basis-Rolle | PA Fachkräfte |
| BMS-Module | <i>keine</i> |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Hilfe <QuickHelp> - Stellenanzeigen zur Bearbeitung <GenericJobadWidget> - Aktive Stellenanzeigen <GenericJobadWidget> - Vakanzen <widgetMyVacancy> |

Benutzergruppe: PR

| | Beschreibung |
|--|--|
| BMS-Basis-Rolle | PR |
| BMS-Module | <i>keine</i> |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Hilfe <QuickHelp> - Bewerbungen im Einstellungsprozess <ExtendedCandidate> - Nicht zur Einladung empfohlene Bewerbungen (B-Kandidaten) <ExtendedCandidate> - Bewerbungsvergleich <ExtendedCandidateWidget> - Stellenanzeigen zur Stellungnahme <GenericJobadWidget> - Aktive Stellenanzeigen <GenericJobadWidget> - Vakanzen <widgetMyVacancy> |

Benutzergruppe: SBV

| | Beschreibung |
|--|--|
| BMS-Basis-Rolle | SBV |
| BMS-Module | <i>keine</i> |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Hilfe <QuickHelp> - Bewerbungen von Schwerbehinderten <ExtendedCandidate> - Nicht zur Einladung empfohlene Bewerbungen (B-Kandidaten) <ExtendedCandidate> - Bewerbungen im Einstellungsprozess <ExtendedCandidate> - Bewerbungsvergleich <ExtendedCandidateWidget> - Bewerbungen im Prozess <ExtendedCandidate> |

Benutzergruppe: GSB

| | Beschreibung |
|--|---|
| BMS-Basis-Rolle | GSB |
| BMS-Module | <i>keine</i> |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Hilfe <QuickHelp> - Bewerbungen im Einstellungsprozess <ExtendedCandidate> - Nicht zur Einladung empfohlene Bewerbungen (B-Kandidaten) <ExtendedCandidate> - Bewerbungsvergleich <ExtendedCandidateWidget> - Stellenanzeigen <GenericJobadWidget> - Vakanzen <widgetMyVacancy> |

Benutzergruppe: PSB

| | Beschreibung |
|--|---|
| BMS-Basis-Rolle | PSB |
| BMS-Module | <i>keine</i> |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Hilfe <QuickHelp> - Einzustellende Bewerbungen <ExtendedCandidate> |

Benutzergruppe: IE

| | Beschreibung |
|--|---|
| BMS-Basis-Rolle | Informationsempfänger |
| BMS-Module | <i>Keine</i> |
| Widgets im Cockpit Name + <Widget Typ> | <ul style="list-style-type: none"> - Hilfe <QuickHelp> |

4.7 Rolle Super-Administrator

Die technische Rolle Super-Administrator wird in der Produktionsumgebung keinem Anwender zugeordnet. Sie kann für Notfalleingriffe bei Gefährdung des Produktionsbetriebs verwendet werden. Über den Einsatz entscheidet die Fachliche Leitstelle. Die Entscheidung ist schriftlich zu begründen und die Vergabe und Verwendung schriftlich zu dokumentieren.

Die Rolle Super-Administrator wird dazu verwendet, um die BMS-Anwendung aufzusetzen und nach der Installation die ersten Konfigurationen, wie z. B. dem Aufsetzen der Standard Benutzergruppen und um die Administratoren anzulegen. Kapitel 6.3 beschreibt, wie diese Rolle im laufenden Verfahrensbetrieb genutzt wird.

4.8 Basis-Rollen

4.8.1 Basis-Rollen und Basis-Rechte

Wie bereits im Kapitel 4.6 erläutert, benötigen alle Benutzergruppen eine Basis-Rolle. Die Bezeichnung der Basis-Rollen erfolgt nach dem Verwendungszweck, weshalb die Bezeichnung ähnlich der zugehörigen Benutzergruppe ist. Die Basis-Rechte beziehen sich jeweils auf die Objekte **Projekt**, **Vakanz**, **Stellanzeige**, **Bewerbung**. Zur besseren Übersicht in den Tabellen, werden die Benutzergruppen abgekürzt. Die Rolle **Informationsempfänger** besitzt keine Rechte für diese Objekte und wird hier nicht näher beschrieben.

| Benutzergruppe | Abk. |
|-------------------------------------|------|
| Administrator | FL |
| Recruiter | R |
| Fachbereich | FB |
| Lektor | L |
| PA Führungskräfte | P 31 |
| PA Fachkräfte | P 34 |
| Personalrat | PR |
| Schwerbehindertenvertretung | SBV |
| Gleichstellungsbeauftragte | GSB |
| Personalsachbearbeitung | PSB |
| Informationsempfänger ¹³ | IE |

Die Basis-Rechte für jedes Objekt, inklusive der Zuordnung zu einer Benutzergruppe, werden auf einer Metaebene beschrieben. Für jedes Objekt werden in der Tabelle zu den Benutzergruppen die Basis-Rechte markiert. Ein „X“ bedeutet, dass Benutzende, mit der Berechtigung in einer Benutzergruppe, dieses Basis-Recht ausführen können.

In der BMS-Backend-Anwendung werden die Basis-Rechte durch Konstanten dargestellt. Beispielsweise bedeuten die Markierungen „X“ in der Tabelle „Vakanz für das Basis-Recht „OBJECT_ACTION_VACANCY_EDIT“, dass die Fachliche Leitstelle und Recruiting eine Vakanz bearbeiten und somit editieren können. Ein äquivalenter Begriff in Deutsch ist in der Spalte „Recht“ genannt. Die Auswertung der Berechtigungen erfolgt im Nutzungskontext der BMS-Anwendung, d. h. ein Basis-Recht kann nur ausgeübt werden, wenn Nutzende in der Benutzergruppe auf diesen Datenobjekt arbeiten können. Die Ausgestaltung der Rechte erfolgt dabei streng nach dem Prinzip der Notwendigkeit und orientiert sich an den zu erledigenden Aufgaben des Nutzenden.

Ob Nutzende auf ein bestimmtes Objekt zugreifen können, hängt zusätzlich davon ab, ob sie im BMS-Prozess Zugriff auf dieses Objekt erhalten. Das bedeutet, Nutzende können z. B. das Basis-Recht „OBJECT_ACTION_VACANCY_EDIT“ für eine bestimmte Vakanz nur ausüben, wenn im Laufe des BMS-Sollprozesses diese Vakanz für sie angezeigt werden. Die Details der Rechte, die ein Spiegelbild der Zuständigkeiten darstellen, werden im Folgenden beschrieben.

¹³ Die Rolle **Informationsempfänger** besitzt keine Rechte für diese Objekte und wird hier nicht näher beschrieben, vgl. die vorangehende Fußnote.

Objekt: Projekt

| Recht | Konstante | FL | R | FB | L | P31 | P34 | PR | SBV | GSB | PSB |
|----------------|---------------------------------------|----|---|----|---|-----|-----|----|-----|-----|-----|
| Anlegen | OBJECT_ACTION_PROJECT_NEW | X | | | | | | | | | |
| Einsehen | OBJECT_ACTION_PROJECT_READ | X | X | X | | X | X | | | | |
| Bearbeiten | OBJECT_ACTION_PROJECT_EDIT | X | | | | | | | | | |
| Auflisten | OBJECT_ACTION_PROJECT_LIST_VIEW | X | X | X | | X | X | | | | |
| Vakanz anlegen | OBJECT_ACTION_PROJECT_VACANCY_CREATE | X | X | | | | | | | | |
| Vakanz-Desktop | OBJECT_ACTION_PROJECT_VACANCY_DESKTOP | X | X | | | | | | | | |

Objekt: Vakanz

| Recht | Konstante | FL | R | FB | L | P31 | P34 | PR | SBV | GSB | PSB |
|-------------------------|--|----|---|----|---|-----|-----|----|-----|-----|-----|
| Anlegen | OBJECT_ACTION_VACANCY_NEW | X | X | | | | | | | | |
| Einsehen | OBJECT_ACTION_VACANCY_READ | X | X | X | X | X | X | X | X | X | x |
| Bearbeiten | OBJECT_ACTION_VACANCY_EDIT | X | X | | | | | | | | |
| Weiterleiten | OBJECT_ACTION_VACANCY_FORWARD | X | X | | | | | | | | |
| Als Vorlage speichern | OBJECT_ACTION_VACANCY_SET_TEMPLATE | X | X | | | | | | | | |
| Als Vorlage benutzen | OBJECT_ACTION_VACANCY_USE_TEMPLATE | X | X | | | | | | | | |
| Verschieben | OBJECT_ACTION_VACANCY_CHANGE_RELATED_PROJECT | X | X | | | | | | | | |
| Besitzer ändern | OBJECT_ACTION_VACANCY_CHANGE_OWNER | X | X | | | | | | | | |
| Auflisten | OBJECT_ACTION_VACANCY_LIST_VIEW | X | X | X | X | X | X | X | X | X | x |
| Stellenanzeigen-Desktop | OBJECT_ACTION_VACANCY_JOBAD_DESKTOP | X | X | | | | | | | | |
| Kandidaten-Desktop | OBJECT_ACTION_VACANCY_CANDIDATE_DESKTOP | X | X | | | | | | | | |
| Bewerbung anlegen | OBJECT_ACTION_VACANCY_CANDIDATE_CREATE | X | X | | | | | | | | |
| Stellenanzeige anlegen | OBJECT_ACTION_VACANCY_JOBAD_CREATE | X | X | | | | | | | | |
| Erinnerung hinzufügen | OBJECT_ACTION_VACANCY_REMINDER_CREATE | X | X | | | | | | | | |

Objekt: Stellenanzeigen

| Recht | Konstante | FL | R | FB | L | P31 | P34 | PR | SBV | GSB | PSB |
|-----------------------|-------------------------------------|----|---|----|---|-----|-----|----|-----|-----|-----|
| Anlegen | OBJECT_ACTION_JOBAD_NEW | X | X | | | | | | | | |
| Einsehen | OBJECT_ACTION_JOBAD_READ | X | X | X | X | X | X | X | X | X | X |
| Bearbeiten | OBJECT_ACTION_JOBAD_EDIT | X | X | | X | | | | | | |
| Weiterleiten | OBJECT_ACTION_JOBAD_FORWARD | X | X | | X | X | X | | | | |
| Als Vorlage speichern | OBJECT_ACTION_JOBAD_SET_TEMPLATE | X | X | | | | | | | | |
| Als Vorlage benutzen | OBJECT_ACTION_JOBAD_USE_TEMPLATE | X | X | | | | | | | | |
| Auflisten | OBJECT_ACTION_JOBAD_LIST_VIEW | X | X | X | X | X | X | X | X | X | X |
| Erinnerung hinzufügen | OBJECT_ACTION_JOBAD_REMINDER_CREATE | X | X | | | | | | | | |
| Vergleichen | OBJECT_ACTION_JOBAD_COMPARE | X | X | | | | | | | | |

Objekt: Bewerbung

| Recht | Konstante | FL | R | FB | L | P31 | P34 | PR | SBV | GSB | PSB |
|---|--|----|---|----|---|-----|-----|----|-----|-----|-----|
| Einsehen | OBJECT_ACTION_CANDIDATE_READ | X | X | X | | X | X | X | X | X | X |
| Bearbeiten | OBJECT_ACTION_CANDIDATE_EDIT | X | X | | | | | | | | |
| Weiterleiten¹⁴ | OBJECT_ACTION_CANDIDATE_FORWARD | X | X | X | | X | X | X | X | X | X |
| Kontaktieren | OBJECT_ACTION_CANDIDATE_CONTACT | X | X | | | X | X | | | | |
| HR-Ranking | OBJECT_ACTION_CANDIDATE_RANKING_HR | X | X | | | | | | | | |
| Vakanz ändern | OBJECT_ACTION_CANDIDATE_CHANGE_RELATED_VACANCY | X | X | | | X | X | | | | |
| Auflisten | OBJECT_ACTION_CANDIDATE_LIST_VIEW | X | X | X | | X | X | X | X | X | X |
| Sichtbar in Bewerbersuche¹⁵ | OBJECT_ACTION_CANDIDATE_GREATGROUPS | X | X | | | X | X | | | | |
| Bewerbung kopieren¹⁶ | OBJECT_ACTION_CANDIDATE_COPY | X | X | | | X | X | | | | |
| FE-Account anlegen | OBJECT_ACTION_CANDIDATE_CREATE_ACCOUNT | X | X | | | X | X | | | | |
| Kommentar löschen | OBJECT_ACTION_CANDIDATE_COMMENT_DELETE | X | X | X | | X | X | | | | |
| Kommentar einsehen | OBJECT_ACTION_CANDIDATE_COMMENT_READ | X | X | X | | X | X | X | X | X | |
| Kommentar anlegen | OBJECT_ACTION_CANDIDATE_COMMENT_NEW | X | X | X | | X | X | X | X | X | X |
| Stellenanzeige ändern | OBJECT_ACTION_CANDIDATE_CHANGE_RELATED_JOBAD | X | X | | | | | | | | |
| Vollständige Doublettenliste | OBJECT_ACTION_CANDIDATE_DOUBLETLIST_SHOWALL | X | | | | | | | | | |
| Junkmail lesen | OBJECT_ACTION_CANDIDATE_JUNKMAIL_READ | X | X | | | X | X | | | | |
| Historie ansehen | OBJECT_ACTION_CANDIDATE_OVERALL_HISTORY_READ | X | X | | | X | X | X | X | X | |
| Termin vereinbaren | OBJECT_ACTION_CANDIDATE_EVENT_INVITATION | X | X | | | | | | | | |
| Anhangstyp ändern | OBJECT_ACTION_CANDIDATE_FILE_CHANGE_ATTACHMENT_TYPE | X | X | | | | | | | | |
| Dossier¹⁷ öffnen | OBJECT_ACTION_OPEN_DOSSIER | X | X | X | | X | X | X | X | X | X |
| Datei hochladen | OBJECT_ACTION_CANDIDATE_EVENT_INVITATION_FILE_UPLOAD | X | X | | | | | | | | |
| Erinnerung hinzufügen¹⁸ | OBJECT_ACTION_CANDIDATE_REMINDER_CREATE | X | X | | | | | | | | |

4.8.2 Neue Basis-Rollen anlegen

Sollten, aufgrund zusätzlicher oder geänderter Anforderungen, neue Basis-Rollen benötigt werden, können diese mit geringem Programmieraufwand in der BMS-Backend-Anwendung

¹⁴ Weitergeleitet werden kann nur an interne Personen, die entsprechend diesem Konzept berechtigt sind (per Dropdown-Auswahl). Es wird lediglich ein Link zum Datensatz im System per Mail versendet, keinerlei personenbezogenes Datum.

¹⁵ Dies bedeutet, dass alle Bewerbungen im jeweils berechtigten Bereich (Projekt) im Modul „Bewerbersuche“ sichtbar sind für die Rollen Admin (FL), Recruiting, P31, P34.

¹⁶ Vakanz für mobile Mitarbeiter muss kopiert werden, sobald ein MA prozessiert wird, damit im Nicht-Erfolgsfall das Profil noch vorhanden ist.

¹⁷ Das Dossier umfasst die Eckdaten der Stelle sowie die gesamten Bewerbungsunterlagen (Daten Masterfragebogen u. Anhänge) als PDF-Dokument.

¹⁸ Mittels dieser Funktion können Bewerbenden Erinnerungen bzgl. der Vervollständigung ihrer Bewerbungsdaten zugestellt werden.

bereitgestellt werden. Die dafür notwendigen Einstellungen in BMS werden vom Produkt-hersteller milch & zucker durchgeführt.

Im BMS-Einführungsprojekt wurden bestehende Basis-Rollen verwendet und auch neue Basis-Rollen eingeführt, z. B. für das Personalamt zur Differenzierung der unterschiedlichen Rechte für P 31 und P 34. Nach Anlage der Basis-Rollen können Änderungen an den Basis-Rechten durch die BMS-Administration durchgeführt werden.

Für das Erstellen neuer Basis-Rollen und auch die Änderung der Konfiguration sind ein tiefgehendes Verständnis der internen BMS-Berechtigungsregeln erforderlich, um die Auswirkungen der Änderungen richtig einschätzen zu können. Im Betrieb ist hier eine Vereinbarung mit der BMS-Anwendungsbetreuung durch milch & zucker zu vereinbaren. Änderungen an den Basis-Rollen sollten nur in einer kontrollierten Umgebung durchgeführt und getestet werden, bevor diese produktiv gesetzt werden.

5 Administrative Prozesse

In diesem Kapitel werden einige administrative Prozesse zur Verwaltung von Berechtigungen aufgezeigt. Eine genaue Festlegung erfolgt im Rahmen des Konzeptes zum Verfahrensbetrieb.

5.1 Einrichtung und Änderung von Benutzergruppen

Im Projekt Bewerbungsmanagement - Einführung (Projekt-ID: P0000936) werden alle benötigten Basis-Rollen und Benutzergruppen aufgesetzt und in der BMS-Backend-Anwendung hinterlegt. Die BMS-Administration kann die Berechtigungen der Benutzergruppen anpassen. Das Aufsetzen neuer Benutzergruppen oder Basis-Rollen ist im laufenden Verfahren nur erforderlich, wenn neue Prozesse oder Benutzergruppen mit speziellen Rechten benötigt werden, siehe hierzu Kapitel 4.8.2.

5.2 Dokumentation der Berechtigungen

Die aktuellen Berechtigungen von Nutzenden können aus der BMS-Backend-Anwendung von der Fachlichen Leitstelle eingesehen werden. Nutzende sind mindestens einer oder mehreren Benutzergruppen zugeordnet.

Die fachliche Dokumentation der BMS-Berechtigungen von Mitarbeitenden in den Behörden wird, wie in Kapitel 3.2 und 3.4 beschrieben, im Kontenpfegetool (KPT) hinterlegt. Aus dem KPT können Berichte mit den Berechtigungen (AD-Gruppen) und organisatorischen Zugehörigkeiten der Nutzer erstellt werden. Die Verwaltung der AD-Gruppen erfolgt durch die Kontenpflegern in den Behörden.

Benötigen Mitarbeitende einer Dienststelle eine Berechtigung auf die BMS-Software, stellt der Anwendungsberatende¹⁹ oder die Führungskraft einen schriftlichen Antrag an die Kontenpflegenden der Behörde. Der Antrag wird von den Kontenpflegenden geprüft und revisionssicher außerhalb des BMS gespeichert.

5.3 Interne Benutzer

Die Mitarbeitenden der FHH gehören zur Kategorie der internen Benutzenden, siehe Kapitel 4.2, und melden sich via SSO an die BMS-Backend-Anwendung an. Die Regeln zur Vergabe

¹⁹ Als Anwendungsberatende werden Anwendende der Rolle Recruiting bezeichnet, die über zusätzliches Know-how der Anwendung verfügen und als Ansprechpartner für die FL in den Dienststellen fungieren.

und Änderung der Passwörter wird durch SSO gesteuert und entspricht den Vorgaben der FHH IT.

Die Service-Mitarbeitenden der Firma milch & zucker gehören ebenfalls der Kategorie interne Benutzende an. Die Anmeldung erfolgt durch Eingabe der persönlichen Zugangsdaten, ohne SSO. Die Service-Mitarbeitenden der Firma milch & zucker erhalten personalisierte Zugriffsrechte, damit nachvollzogen werden kann, welcher Service-Mitarbeitende auf das System zugegriffen hat und identifiziert werden kann. Die Passwortregeln werden durch die BMS-Backend-Anwendung festgelegt, Vorgaben werden hierzu in Kapitel 6 beschrieben.

Für die Vergabe und Dokumentation der Berechtigungen der externen Service-Mitarbeitenden ist die Fachliche Leitstelle verantwortlich. Die Zugänge sind personalisiert, Anträge auf Zugänge müssen von milch & zucker schriftlich angefordert werden. Werden Zugänge nicht mehr benötigt, ist dies schriftlich von milch & zucker der FL anzuzeigen.

5.4 Ändern der Zugriffsberechtigungen

Wie in Kapitel 3 ausgeführt, werden die Daten von den Behörden und Ämtern gepflegt und zentral im Kontenpflegetool gespeichert. Das Hinzufügen von neuen Mitarbeiterenden oder das Ändern von Berechtigungen für die BMS-Anwendung erfolgt durch die Kontenpfleger der Dienststelle.

Bei der Vergabe von Berechtigungen gilt das Minimalitäts-Prinzip („need-know-Prinzip“). Daraus folgend muss insbesondere gewährleistet sein, dass Benutzende lediglich aufgabenbezogene Daten einsehen können und Berechtigungen nicht behalten, wenn sie diese für die Erledigung einer übertragenen Aufgabe nicht mehr benötigen. Durch die tägliche Aktualisierung über den KPT Import werden Benutzenden im BMS Berechtigungen entzogen, die sie nicht mehr benötigen.

Die Dienststellen überwachen den Umfang der eingeräumten Zugriffsrechte ihrer Beschäftigten selbst. Bei jeder dauerhaften Veränderung von Zuständigkeiten, Aufgabenwechseln oder Aufgabenentfall hat eine Gegenprüfung gegen die erteilten Rechte zu erfolgen. Relevante Änderungen werden über den KPT Import, derzeit täglich, in BMS aktualisiert. Im Fehlerfall oder bei Unstimmigkeiten ist die Fachliche Leitstelle von der datenverarbeitenden Dienststelle schriftlich zu informieren.

Für die in der Fachlichen Leitstelle beschäftigten Personen trifft die Fachliche Leitstelle organisatorische Regelungen²⁰, so dass bei berechtigungsrelevanten Veränderungen eine Überprüfung und Anpassung der Berechtigungen erfolgt. Alle Änderungen sind durch schriftliche Aufträge zu dokumentieren. Dies betrifft die FL sowie externe Personen, die zur Systempflege auf die BMS-Anwendung zugreifen.

Es ist organisatorisch ausgeschlossen, dass auftragsberechtigte Personen aus den Fachbereichen selbst Berechtigungsadministratoren sind.

Die Umsetzung der Aufträge wird von der Fachlichen Leitstelle mit geeigneten Mitteln dokumentiert. Als geeignet gelten alle Mittel, die nachvollziehbar beschreiben, wer (Person) welche Änderungen (Einstellungen im System) wann (Datum, keine Uhrzeit) vorgenommen hat. In der BMS-Backend-Anwendung wird protokolliert, welcher Nutzer wann eingerichtet wurde und welche Berechtigungen ihm eingeräumt bzw. entzogen wurden. Die Protokollierung der Zugriffe, d. h. welcher Nutzer sich wann angemeldet und auf welche Datenobjekte schreibend zugegriffen hat, wird in BMS gespeichert. Die schriftlichen Aufträge sind abzulegen

²⁰ Diese werden im Verfahrensbetriebskonzept näher beschrieben.

und für Revisionszwecke nach Abschluss des Kalenderjahres der Wirksamkeit der Änderung gem. § 76 BDSG für ein Jahr aufzubewahren.

5.5 Umgang mit internen Bewerbungen durch Verfahrensbeteiligte

Sind im einem laufenden Bewerbungsverfahren Personen beteiligt (als Bewerbende oder sonstig Beteiligte Person), die nach § 20 Hamburgisches Verwaltungsverfahrensgesetz (HmbVwVfG)²¹ nicht tätig werden dürfen, werden diese Personen von dem laufenden Bewerbungsverfahren ausgeschlossen. Gemäß § 21 HmbVwVfG (Besorgnis der Befangenheit) müssen die Personen, die von der Misstrauen gegen eine unparteiische Amtsausübung Kenntnis erlangen, die zuständigen Verantwortlichen in ihrer Dienststelle informieren. Das Vorliegen eines solchen Falls kann entweder von der betreffenden Person selbst angezeigt oder von den anderen Verfahrensbeteiligten erkannt werden.

Ein solcher Fall kann u.a. eintreten, wenn Verfahrensbeteiligte (z.B. Recruiting, Mitarbeitende aus P31/34, Personalratsmitglieder) sich auf ausgeschriebene Stellen bewerben, an denen sie selber mitwirken.

Die in der Dienststelle zuständigen BMS Anwendungsbetreuende, informieren die Fachliche Leitstelle mit Angabe des Bewerbungsverfahrens und der betroffenen Person. Die Fachliche Leitstelle leitet die notwendigen Maßnahmen ein und teilt diese dem betroffenen Personenkreis (Anwendungsbetreuende der Dienststelle) mit.

Kann die betroffene Person nicht durch Entzug der Berechtigungen aus einem Bewerbungsverfahren ausgeschlossen werden, wird für diese Dienststelle ein Sonderprojekt angelegt, in welchem nur die zulässigen Personen berechtigt werden. Somit kann sichergestellt werden, dass Personen mit herausgehobenen Sicht- und Schreibrechten in laufenden Bewerbungsverfahren nicht gleichzeitig Bewerbende in eben diesen Verfahren sind.

Interne Bewerbende, die sonst eine nominelle Verfahrensbeteiligung hätten, bewerben sich somit auf ein Bewerbungsverfahren (in BMS eine Vakanz) in einem Sonderprojekt, in dem die betroffenen Bewerbende keine Sicht- und Schreibrechte haben.

²¹ HmbVwVfG im FHH Intranet:

https://fhhportal.ondataport.de/websites/bac_729/Fachverfahren/Forms/Susanne.aspx?RootFolder=%2fwebsites%2fbac%5f729%2fFachverfahren%2fNutzungen%2fRechtsgrundlagen%2fHamburgisches%20Verwaltungsverfahrensgesetz%20%2d%20HambVwVfG&FolderCTID=0x01200010AC373295A7D946A1E063DF7D1A9ED8

6 Sicherheitskonzept BMS

6.1 Kennwortregeln²²

Die Service Mitarbeiter der Firma milch & zucker AG melden sich ohne SSO an die BMS-Backend-Anwendung an. In diesem Fall werden die Passwortregeln von der BMS-Anwendung festgelegt. Für die Vergabe der Passwörter gilt die Passwort-Richtlinie der FHH²³. Zusammengefasst gelten folgende Grundsätze:

- Passwörter sind, unbeschadet notwendiger Vertretungsregelungen, geheim zu halten. Sie sind verdeckt einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt werden.
- Die Länge der Passwörter beträgt mindestens 8 Zeichen. Dabei ist eine Mischung aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen zu verwenden. Bei der Vergabe von Passwörtern wird die Komplexität automatisch geprüft. Nicht den Vorgaben entsprechende Passwörter können nicht vergeben werden.
- Passwörter sind spätestens nach 45 Tagen zu wechseln. Die Restlaufzeit wird vom System überprüft und die Benutzer nach Ablauf des Kennworts automatisch zu einer Kennwortänderung aufgefordert.
- Passwörter dürfen in der Regel höchstens einmal am Tag gewechselt werden. Sie sind jedoch unverzüglich zu wechseln, wenn der Verdacht besteht, dass sie Dritten bekannt geworden sein könnten.
- Übergangspasswörter sind unverzüglich durch eigene Passwörter zu ersetzen.

6.2 Sperrung von Kennungen nach langer Inaktivität

Für FHH Nutzende erfolgt der Anmeldevorgang über SSO, dadurch werden die Kennungen nach den Vorgaben der FHH IT gesperrt. Bei den Service Mitarbeiterenden der Firma milch & zucker sollen die Kennungen nach einer definierbaren Dauer der Inaktivität aus Sicherheitsgründen gesperrt werden. Die BMS-Anwendung unterstützt eine automatische Sperrung, die Zeitspanne wird von der FL auf 90 Tage festgelegt. Aus Transparenzgründen sind nicht mehr benötigte Kennungen nicht zu löschen, sondern nur zu sperren.²⁴

6.3 BMS-Datenbank

Im Verfahrensbetrieb wird die gesamte BMS-Anwendung auf Dataport-Servern in einer gesicherten Umgebung betrieben und technisch überwacht. Die Firma milch & zucker und die FL verfügen über keinen direkten Zugriff, weder lesend noch schreibend, auf die von Dataport betriebenen BMS-Datenbanken.

Müssen Daten aus der BMS-Datenbank gelesen oder verändert werden, erfolgt dies in einer streng durch Dataport TVM kontrollierten und gesteuerten Art und Weise. Die Datenextraktion und auch Datenänderung in der BMS-Datenbank erfolgt durch Dataport Techniker in Abstimmung und auf Anforderung durch die FL. Dabei wird durch das Dataport TVM sichergestellt, dass keine personenbezogenen Daten an milch & zucker übermittelt werden. Weitere Einzelheiten sind im Verfahrensbetrieb zwischen milch & zucker, Dataport und der FL festzulegen.

²² Gilt nur Fälle, in denen keine single-sign-on-Anmeldung erfolgt

²³ Die Richtlinie zur Verwaltung von Passwörtern ist im FHH-Portal im Bereich Downloads unter dem Link [11.650 - Passwort-Richtlinie](#) zu finden.

²⁴ Aus KPT werden täglich diejenigen Mitarbeiter geliefert, die das BMS nutzen dürfen. Zugriffsberechtigungen all derjenigen, die in den KPT-Daten nicht enthalten sind, werden direkt gelöscht.

7 Anlagen zum Berechtigungskonzept

Die folgenden aufgelisteten Anlagen werden dem Berechtigungskonzept separat beigelegt:

| ID | Dokument |
|------------|---|
| Anhang-1 | Fachkonzept zum Projekt Bewerbermanagement Einführung |
| Anhang-2 | BMS-Sollprozess Diagramm |
| Anhang-3 | Konzept zum Verfahrensbetrieb (<i>*** noch in Erstellung ***</i>) |
| Anhang-4.1 | EHdB - RZ Betriebshandbuch Kundenversion |
| Anhang-4.2 | EHdB - Diagramm Systeminfrastruktur Kundenversion |



Anonymisierungs- und Löschkonzept



BeeSite Recruiting Edition

(Release Version 8.0)

Für:



Projektleitung Freie und Hansestadt Hamburg

Friederike Vieth

ZPD 21 HR Digital

040 42805-2596

Friederike.Vieth@zpd.hamburg.de

Stefanie Liebner Freter

Personalamt

040 42831-1698

stefanie.liebner@personalamt.hamburg.de

Projektleitung milch & zucker AG

Verena Schwarz

0641 – 300 20 643

v.schwarz@milchundzucker.de

1 Inhalt

| | | |
|----------|--|-----------|
| 2 | Änderungsverzeichnis..... | 6 |
| 3 | Erläuterung..... | 7 |
| 3.1 | Allgemeines..... | 7 |
| 3.2 | Urheber und Kennzeichenrecht..... | 7 |
| 3.3 | Zweck und Abgrenzung..... | 7 |
| 3.4 | Rechtlicher Rahmen..... | 8 |
| 3.5 | Haftungsausschluss:..... | 8 |
| 3.6 | Überblick Objekte..... | 8 |
| 3.7 | Datenarten..... | 9 |
| 3.7.1 | Grad der Sensibilität von Daten..... | 9 |
| 3.7.2 | Liste der Datenarten..... | 9 |
| 3.7.3 | Datenfelder beispielhaft..... | 9 |
| 3.7.4 | Freitextfelder..... | 9 |
| 3.7.5 | Referenzieren/Verknüpfungen, Pseudonymisierung..... | 9 |
| 3.8 | Allgemeine Begriffs-Definition Aktion / Zustand..... | 9 |
| 4 | Webserver – Bereitstellung der Webseite..... | 13 |
| 4.1 | Beschreibung..... | 13 |
| 4.2 | Beinhaltete Daten..... | 13 |
| 4.3 | Aktionen..... | 13 |
| 5 | Objekt „Projekt“..... | 14 |
| 5.1 | Beschreibung..... | 14 |
| 5.2 | Beinhaltete Daten..... | 14 |
| 5.3 | Mögliche Änderung des Objekt-Zustands - Überblick..... | 14 |
| 5.3.1 | Archivieren..... | 14 |
| 5.3.2 | Sperren..... | 15 |
| 5.3.3 | Pseudonymisieren..... | 15 |
| 5.3.4 | Anonymisieren..... | 15 |
| 5.3.5 | Löschen..... | 15 |
| 6 | Objekt „Personalanforderung“..... | 16 |
| 6.1 | Beschreibung..... | 16 |
| 6.2 | Beinhaltete Daten..... | 16 |
| 6.3 | Mögliche Änderung des Objekt-Zustands - Überblick..... | 16 |
| 6.3.1 | Archivieren..... | 16 |
| 6.3.2 | Sperren..... | 17 |
| 6.3.3 | Pseudonymisieren..... | 17 |
| 6.3.4 | Anonymisieren..... | 17 |

| | | |
|-----------|---|-----------|
| 6.3.5 | Löschen | 17 |
| 7 | Objekt „Vakanz“ | 18 |
| 7.1 | Beschreibung..... | 18 |
| 7.2 | Beinhaltete Daten | 18 |
| 7.3 | Mögliche Änderung des Objekt-Zustands - Überblick..... | 18 |
| 7.3.1 | Archivieren..... | 18 |
| 7.3.2 | Sperren..... | 19 |
| 7.3.3 | Pseudonymisieren | 19 |
| 7.3.4 | Anonymisieren | 19 |
| 7.3.5 | Löschen | 19 |
| 8 | Objekt „Stellenanzeige“ | 20 |
| 8.1 | Beschreibung..... | 20 |
| 8.2 | Beinhaltete Daten | 20 |
| 8.3 | Mögliche Änderung des Objekt-Zustands - Überblick..... | 20 |
| 8.3.1 | Archivieren..... | 21 |
| 8.3.2 | Sperren..... | 21 |
| 8.3.3 | Pseudonymisieren | 21 |
| 8.3.4 | Anonymisieren | 21 |
| 8.3.5 | Löschen | 21 |
| 9 | Objekt „Frontend Account (Bewerber-Account)“ | 22 |
| 9.1 | Beschreibung..... | 22 |
| 9.2 | Beinhaltete Daten | 22 |
| 9.3 | Bewerber-Account für das Frontend erstellen | 22 |
| 9.3.1 | Registrierung durch den Kandidaten | 22 |
| 9.4 | Bewerbung ohne vorherige Registrierung | 23 |
| 9.5 | Frontend-Account läuft ab | 24 |
| 9.6 | Mögliche Änderung des Objekt-Zustands - Überblick..... | 25 |
| 9.6.1 | Archivieren..... | 25 |
| 9.6.2 | Sperren..... | 25 |
| 9.6.3 | Pseudonymisieren | 25 |
| 9.6.4 | Anonymisieren | 25 |
| 9.6.5 | Löschen | 25 |
| 10 | Objekt "Jobmerker" | 28 |
| 10.1 | Beschreibung..... | 28 |
| 10.2 | Beinhaltete Daten | 28 |
| 10.3 | Mögliche Änderung des Objekt-Zustands - Überblick..... | 28 |
| 11 | Objekt „Job-Abo“ | 29 |
| 11.1 | Beschreibung..... | 29 |

| | | |
|-----------|---|-----------|
| 11.2 | Beinhaltete Daten | 29 |
| 11.3 | Mögliche Änderung des Objekt-Zustands - Überblick | 29 |
| 11.3.1 | Archivieren | 29 |
| 11.3.2 | Sperren | 29 |
| 11.3.3 | Pseudonymisieren | 29 |
| 11.3.4 | Anonymisieren | 29 |
| 11.3.5 | Löschen | 29 |
| 12 | Objekt „Bewerbung“ | 30 |
| 12.1 | Beschreibung | 30 |
| 12.2 | Beinhaltete Daten | 30 |
| 12.3 | Mögliche Änderung des Objekt-Zustands - Überblick | 31 |
| 12.3.1 | Archivieren | 31 |
| 12.3.2 | Sperren | 32 |
| 12.3.3 | Pseudonymisieren | 32 |
| 12.3.4 | Anonymisieren | 32 |
| 12.3.5 | Löschen | 33 |
| 13 | Objekt „Backend-Account“ (BeeSite-Anwender / BeeSite-User) | 34 |
| 13.1 | Beschreibung | 34 |
| 13.2 | Nicht Bestandteil dieses Dokuments | 34 |
| 13.3 | Beinhaltete Daten | 34 |
| 13.4 | Mögliche Änderung des Objekt-Zustands - Überblick | 35 |
| 13.4.1 | Archivieren | 35 |
| 13.4.2 | Sperren | 35 |
| 13.4.3 | Pseudonymisieren | 36 |
| 13.4.4 | Anonymisieren | 36 |
| 13.4.5 | Löschen | 37 |
| 14 | Objekt „Termin“ | 38 |
| 14.1 | Beschreibung | 38 |
| 14.2 | Beinhaltete Daten | 38 |
| 14.3 | Mögliche Änderung des Objekt-Zustands - Überblick | 38 |
| 14.3.1 | Archivieren | 38 |
| 14.3.2 | Sperren | 39 |
| 14.3.3 | Pseudonymisieren | 39 |
| 14.3.4 | Anonymisieren | 39 |
| 14.3.5 | Löschen | 39 |
| 15 | Objekt „Poolprofil“ | 40 |
| 15.1 | Beschreibung | 40 |

| | | |
|-----------|--|-----------|
| 15.2 | Beinhaltete Daten | 40 |
| 15.3 | Mögliche Änderung des Objekt-Zustands – Überblick | 40 |
| 15.3.1 | Archivieren..... | 40 |
| 15.3.2 | Sperren..... | 41 |
| 15.3.3 | Pseudonymisieren | 41 |
| 15.3.4 | Anonymisieren | 41 |
| | Talentprofil bei Einstellung..... | 41 |
| 15.3.5 | Löschen | 41 |
| 16 | Anhang -Fristen | 42 |
| 16.1 | Schaubild Überblick Vorhalte- und Regellöschfrist am Beispiel der Bewerbung..... | 42 |
| 16.2 | Konfigurierte Fristen | 42 |

2 Änderungsverzeichnis

hat formatiert: Nicht Hervorheben

| Datum | Autor | Beschreibung | Version |
|-------------------|-----------------------|--------------------------------------|---------|
| 16.09.2019 | Yvo Freund | Freigabe Anonymisierungskonzept | 3.0 |
| <u>09.03.2020</u> | <u>Verena Schwarz</u> | <u>Bereitstellung für FHH-19-002</u> | |
| | | | |
| | | | |
| | | | |

3 Erläuterung

3.1 Allgemeines

Aus Gründen der besseren Lesbarkeit wird die männliche Formulierung (generisches Maskulinum) verwendet. Alle Beschreibungen gelten jedoch für alle Geschlechter.

3.2 Urheber und Kennzeichenrecht

Sämtliche Informationen und gegebenenfalls beigelegte Unterlagen sind zeitlich unbegrenzt als vertraulich zu behandeln. Eine Weitergabe der Informationen zu einem anderen Zweck als der Prüfung der Eignung für diese Aufgabe bedarf der schriftlichen Genehmigung von milch & zucker Talent Acquisition & Talent Management Company AG.

Innerhalb dieser Beschreibung genannte und ggf. durch Dritte geschützte Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer.

BeeSite® ist ein eingetragenes Warenzeichen von milch & zucker Talent Acquisition & Talent Management Company AG.

3.3 Zweck und Abgrenzung

Das Konzept dient dazu, gesetzliche Vorgaben, Normforderungen oder Kundenforderungen zu erfüllen, hier: dem Schutz von persönlichen Daten.

Soweit für milch & zucker praktikabel, orientiert sich das Konzept an der **DIN 66398** (Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschrufen für personenbezogene Daten).

Das Konzept beschreibt die Objekte im Recruiting-Vorgang und den möglichen Zustand eines Objektes, zum Beispiel archiviert, anonymisiert, gelöscht sowie deren Auswirkungen auf die enthaltenen Daten. **Die Begriffe beschreiben die Änderung des Zustands eines Objektes. Workflow-Status/Prozess-Schritte/Status-Namen eines Objektes sind hier nicht gemeint.** Die Definition eines Zustands erfolgt sowohl allgemeingültig für alle Objekte, als auch detailliert pro Objekt, da es hier Unterschiede gibt.

Das Konzept beschreibt, welche Daten im System verarbeitet werden, wie die Daten verwendet werden und wie sie geschützt werden.

Das Konzept bezieht sich auf Daten, die in der Software „BeeSite Recruiting Edition“ im Rahmen von Recruiting- und Talentpool-Prozessen verarbeitet werden.

Sicherungs-Zyklen und die Aufbewahrungsdauer von Backups im Rahmen der Ausfallsicherung sind im IT-Sicherheitskonzept beschrieben.

Konfigurierte Regeln und Fristen sind im Abschnitt X. Bewerberfristen in KON_FHH-19-002_Dokumentation.docx dargestellt. Die Anonymisierungs- und Löschrufen sind durch milch & zucker kundenindividuell parametrisierbar. Die beschriebenen Regeln sind die im Standard vorkonfigurierten Werte.

3.4 Rechtlicher Rahmen

Die Erhebung, Verarbeitung und Speicherung personenbezogener Daten unterliegt den datenschutzrechtlichen Vorgaben der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG). milch & zucker wählt in den Standardeinstellungen und Funktionen stets datenschutzfreundliche Voreinstellungen im Sinne des Art. 25 DSGVO.

Es obliegt dem Auftraggeber diese Voreinstellungen und etwaige Änderungen innerhalb des Unternehmens mit dem zuständigen Datenschutzbeauftragten und den Rechtsbereichen zu überprüfen, zu definieren und festzulegen.

milch & zucker übernimmt keine Gewährleistung dafür, dass die konkrete Umsetzung dieses Konzepts den rechtlichen Anforderungen genügt.

3.5 Haftungsausschluss:

Die von uns bereitgestellten Inhalte dienen ausschließlich Informationszwecken und stellen keine rechtliche Beratungsdienstleistung dar. Wir übernehmen daher keine Haftung für ihre Richtigkeit, Vollständigkeit und Aktualität. Zur Lösung konkreter Rechtsfälle empfehlen wir, zwingend einen Rechtsanwalt zu konsultieren.

3.6 Überblick Objekte

Innerhalb der BeeSite gibt es verschiedene Objekte, zu denen Daten gespeichert werden. Diese Objekte sind:

- Projekt
- Personalanforderung
- Vakanz
- Stellenanzeige
- Frontend-Account (Bewerber-Account, externes und internes Portal)
- Jobmerker
- Jobabo
- Bewerbung
- Backend-Account (BeeSite-Anwender)
- Termin
- Talentprofil / Poolprofil
- Talent-Community-Profil

Die Funktion der Objekte ist in den folgenden Kapiteln kurz beschrieben. Detaillierte Informationen finden sich in der Funktionsbeschreibung (Benutzerhandbuch) der BeeSite Recruiting Edition.

3.7 Datenarten

3.7.1 Grad der Sensibilität von Daten

Abhängig von der Einrichtung des Systems können in jedem dieser Objekte unterschiedlich sensible Daten gespeichert sein.

3.7.2 Liste der Datenarten

Die relevanten Datenarten sind im Abschnitt X. Bewerberfristen in KON_FHH-19-002_Dokumentation.docx dargestellt.

3.7.3 Datenfelder beispielhaft

Es wird der Umgang mit den Objekten beschrieben, allerdings werden nicht alle Datenfelder der Objekte aufgeführt. Falls hilfreich, werden Beispiele für Datenfelder angeführt.

Eine genaue Auflistung aller Datenfelder ist nicht Bestandteil dieses Dokuments, sondern der aktuelle Stand kann aus dem Live-System exportiert werden.

3.7.4 Freitextfelder

milch & zucker weist darauf hin, dass es innerhalb der BeeSite an verschiedenen Stellen **Freitextfelder** gibt.

Wenn diese Freitextfelder im Objekt „Bewerbung“ genutzt und personenbezogene Daten gespeichert werden, ist eine fristgemäße automatisierte Anonymisierung und/oder Löschung sichergestellt. Wenn Freitextfelder in anderen Objekten, z.B. „Vakanz“, „Stellenanzeige“ o.ä. genutzt und personenbezogene Daten gespeichert werden, kann eine fristgemäße automatisierte Anonymisierung und/oder Löschung nicht sichergestellt werden, da für diese Objekte keine Fristen vorkonfiguriert ausgeliefert werden.

3.7.5 Referenzieren/Verknüpfungen, Pseudonymisierung

Wenn Daten zu Anwendern nicht direkt im Objekt gespeichert werden, wird der Begriff „referenzieren“ verwendet. Damit ist gemeint, dass **nur Verknüpfungen (IDs) von Anwenderdaten** in den Datenbanktabellen von Objekten (z.B. Vakanz, Stellenanzeigen, etc.) gespeichert werden. Die eigentlichen Daten (z.B. Name, Adresse, etc.) zu den Anwendern liegen getrennt vor und werden in der Benutzerverwaltung verwaltet.

Bei der Verknüpfung handelt es sich somit um pseudonymisierte Daten.

Sobald also die Speicherung von persönlichen Daten im Rahmen eines Benutzer-Accounts nicht mehr erwünscht ist, greifen die zum jeweiligen Account gehörenden Regeln. Damit werden auch die persönlichen Daten in den jeweiligen Objekten nicht mehr angezeigt. Die dort noch vorhandene ID führt auf einen anonymen Datensatz, der keinerlei persönliche Informationen mehr enthält. Ein komplettes Löschen ist aufgrund der Integrität der erfassten Daten (Konsistenz der Datenbank) nicht möglich.

3.8 Allgemeine Begriffs-Definition Aktion / Zustand

Bei den Aktionen handelt es sich um die Änderung des Zustands eines Objektes. Workflow-Status eines Objektes sind hier **nicht** gemeint.

| Möglicher Zustand eines Objekts (NICHT Workflow-Status) | Erläuterung |
|--|--|
| Archivieren | <p>Allgemeine Definition</p> <hr/> <p>Umsetzung in der BeeSite Recruiting Edition</p> <hr/> <p>Wird ein Objekt archiviert, wird der Datensatz aus dem allgemeinen Bearbeitungsbereich in ein digitales Archiv innerhalb des Systems verschoben.</p> <hr/> <p>In der BeeSite Recruiting Edition bedeutet dies:</p> <p>Das Archiv dient der Aufbewahrung der Objekte Projekt, Vakanz, Stellenanzeige oder Bewerbung, die im täglichen Arbeiten nicht mehr benötigt werden, aber – sofern zutreffend – noch nicht anonymisiert oder gelöscht wurden.</p> <p>Das Objekt wird nur noch im Archiv angezeigt.</p> <p>Es ist nicht mehr im Navigationsbaum, in den Desktops oder – im Fall der Bewerbung – in der Bewerbersuche zu finden.</p> <p>Das Objekt ist nur für Personen einsehbar, die für das Archiv berechtigt sind.</p> <p>Das Objekt kann nicht bearbeitet werden. Das Objekt kann von berechtigten Personen re-archiviert werden.</p> <p><i>Zum Archivieren siehe auch die Anmerkung unterhalb dieser Tabelle.</i></p> |
| Sperren | <p>Sperrung ist das Verhindern einer weiteren Verarbeitung der Daten durch Anwender des Systems.</p> <hr/> <p>Der Datensatz wird in bestimmten Workflow-Schritten für bestimmte Anwendergruppen gesperrt.</p> <p>Der Datensatz ist damit für den Anwender (möglicherweise auch alle Anwender) nicht sichtbar.</p> <p>Wird ein Datensatz für alle Anwender gesperrt, wird dafür im Backend der Workflow-Status „gelöscht“ verwendet. Der Datensatz ist damit für den Anwender nicht länger sichtbar. Er kann ihn nicht mehr sehen oder bearbeiten, auch nicht zurückholen. Er ist aus der Backend-Oberfläche „gelöscht“.</p> <p>In der Datenbank ist der Datensatz noch vorhanden.</p> <p>Lediglich ein Datenbank-Administrator kann mittels Sonderberechtigung auf die Daten zugreifen.</p> |
| Anonymisieren | <p>Als Anonymisierung gilt die Veränderung personenbezogener Daten, die eine Zuordnung der erhobenen Einzelangaben zu einer Person nicht mehr oder nur noch mit einem erheblichen und unverhältnismäßig großen Aufwand an Zeit, Kosten und</p> |

| | |
|---------|---|
| | <p>Arbeitskraft möglich macht. Im Ergebnis wird ein personenbezogenes Datum so umgestaltet, dass kein Personenbezug mehr besteht und damit die Erhebung, Verarbeitung und Nutzung von Daten vermieden wird.</p> <hr/> <p>Anonymisierte Daten fallen nicht unter die DSGVO.</p> <hr/> <p>In der BeeSite Recruiting Edition bedeutet das:</p> <p>Das Objekt ist nicht einsehbar.</p> <p>Das Objekt ist nicht bearbeitbar.</p> <p>Es werden alle Datenfelder ersetzt, die einen Rückschluss auf eine Person ermöglichen würden (zum Beispiel * String = „Anonym.“, * Datum = „0000-00-00“).</p> <p>Das Objekt ist in anonymisierter Form in der Datenbank als Datensatz enthalten.</p> <p>Die anonymisierten Daten werden für statistische, NICHT personenbezogene Auswertungen verwendet.</p> |
| Löschen | <p>Die Datenschutz-Grundverordnung definiert den Begriff „Löschen“ nicht. Maßgeblich ist, dass im Ergebnis keine Möglichkeit mehr besteht, die Daten ohne unverhältnismäßigen Aufwand wahrzunehmen.</p> <hr/> <p>In der BeeSite bedeutet das:</p> <p>Die Daten werden vollständig gelöscht.</p> <p>Das Objekt ist nicht mehr in der Datenbank enthalten.</p> |

Anmerkung: Unterscheidung zwischen Archiv und Sicherungskopie

(Quelle: DIN Deutsches Institut für Normung e.V. "Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten", Version 1.0.3, Oktober 2015, Dr. Volker Hammer, Karin Schuler, Secorvo Security Consulting GmbH)

Archive dienen dazu, Daten langfristig vorzuhalten. Daten werden häufig in Archive verlegt, wenn an Datensätzen oder anderen Beständen keine Veränderungen mehr vorgenommen werden, sie jedoch aus zulässigen Gründen weiterhin aufbewahrt werden müssen. Ein Archiv kann unterschiedliche Datenarten mit unterschiedlichen Löschfristen enthalten.

Sicherungskopien (Backup) dürfen nicht als Archive verwendet werden, denn sie haben eine andere Funktion. Sie werden zur Wiederherstellung von Systemen und Datenbeständen nach Störungen benötigt. Sie dürfen daher nicht verändert werden. Sicherungskopien existieren in der Regel in verschiedenen Versionen oder Versionsketten. Jede der Versionen kann unterschiedlich alte Datenbestände der gleichen Datenart enthalten. Die einzelnen Instanzen von Datenobjekten erreichen daher ihre Löschfrist zu sehr unterschiedlichen Zeiten. Zur Einhaltung von Löschrregeln wären deshalb häufig einzelne Daten aus den Sicherungskopien zu löschen.

Zwischen Sicherungskopien und Archiven muss deshalb klar getrennt werden.

Die Daten in Archiven unterliegen den Löschrregeln der jeweiligen Datenarten und müssen nach diesen Regeln im Archiv gelöscht werden.

Für die Löschung von Sicherungskopien müssen dagegen eigene Fristen festgelegt werden, die bezüglich der Regellöschfristen der im Backup enthalten „gemischten“ Daten verhältnismäßig sind.

Die Löschung von Sicherungskopien (Backup) ist nicht Bestandteil dieses Dokuments, sondern im IT-Sicherheitskonzept beschreiben.

4 Webserver – Bereitstellung der Webseite

4.1 Beschreibung

Bei Aufruf des Webservers speichert der Webserver Log-Informationen.

4.2 Beinhaltete Daten

Welche Log-Informationen gespeichert werden, kann konfiguriert werden.

Normalerweise sind dies:

- IP-Adresse
- Datum, Uhrzeit (mit Zeitzone)
- angefragte Adresse
- Status Code
- übertragene Datenmenge

Im Auslieferungszustand werden die Log-Dateien rotiert.

Nach 7 Tagen werden die Daten überschrieben.

4.3 Aktionen

Die Log-Dateien des Webservers sind nicht Bestandteil der Anonymisierung. Sie werden regelmäßig rotiert und überschrieben.

Sämtliche zugrundeliegende Systemkomponenten werden im Folgenden nicht weiter berücksichtigt, da es dort an keiner Stelle eine dauerhafte Speicherung von personenbezogenen Daten gibt.

5 Objekt „Projekt“

5.1 Beschreibung

Ein Projekt dient als Ordnungsrahmen und kann beliebig viele Ausschreibungen beinhalten.

5.2 Beinhaltete Daten

- In einem Projekt werden keine personenbezogenen Daten von Kandidaten gespeichert.
- Von Backend-Anwendern, die in das Projekt involviert sind, wird lediglich eine Referenz-ID gespeichert, keine weiteren personenbezogenen Daten.

Alle weiteren Felder dienen der Information und/oder zur Prozesssteuerung. Eine detaillierte Auflistung der Felder findet sich im Dokument KON_FHH-19-002_Umsetzungsdokumentation.docx.

5.3 Mögliche Änderung des Objekt-Zustands - Überblick

| Aktion ¹ | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|---|
| Archivieren | Ja | Das Projekt wird im Archiv angezeigt. Es ist nicht mehr im Navigationsbaum und in den Desktops zu finden. Das Projekt ist ausschließlich für Personen einsehbar, die für das Archiv berechtigt sind. Das Projekt kann nicht bearbeitet werden. Das Projekt kann von berechtigten Personen re-archiviert werden. |
| Sperren | ja | Das Projekt ist für Backend-Anwender nicht einsehbar. Das Projekt ist mittels Sonderberechtigung von einem Datenbank-Administrator einsehbar. |
| Pseudonymisieren | nein | n. a. |
| Anonymisieren | nein | n. a. |
| Löschen | nein | n. a. |

5.3.1 Archivieren

5.3.1.1 Automatische Archivierung

Es wird keine automatische Archivierung durchgeführt.

¹ Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

5.3.1.2 Manuelle Archivierung

Um ein Projekt in das Archiv verschieben zu können, sind folgende Vorbedingungen notwendig:

- Das Projekt befindet sich im Status „inaktiv“.
Sollte diese Bedingung nicht erfüllt sein, wird die Aktion „Archivieren“ nicht zur Auswahl angeboten.
- Alle Vakanzen (damit auch indirekt alle Bewerbungen auf diese Vakanz und alle Stellenanzeigen), die unterhalb des Projekts liegen, befinden sich in einem finalen Status (z.B. „abgeschlossen“, „abgesagt“, „eingestellt“).

Sollte eine dieser Bedingung nicht erfüllt sein, wird durch das System eine entsprechende Fehlermeldung angezeigt:



5.3.2 Sperren

5.3.2.1 Automatische Sperrung

Es wird keine automatische Sperrung durchgeführt.

5.3.2.2 Manuelle Sperrung

Ein Projekt kann manuell für alle Anwender gesperrt werden, wenn es inaktiv ist und keine Objekte darunter existieren.

Das Projekt wird dafür in den Workflow-Status „gelöscht“ gesetzt.

5.3.3 Pseudonymisieren

Es wird keine Pseudonymisierung durchgeführt.

5.3.4 Anonymisieren

Es wird keine Anonymisierung durchgeführt.

5.3.5 Löschen

Es wird keine Löschung durchgeführt.

Ein Löschen ist aufgrund der Integrität der erfassten Daten (Konsistenz der Datenbank) nicht möglich.

6 Objekt „Personalanforderung“

6.1 Beschreibung

Mit einer Personalanforderung (PAF) meldet ein Fachbereich seinen Bedarf an einer Stellenbesetzung an die Personalabteilung. Aus einer Personalanforderung kann von berechtigten Personen eine Vakanz generiert werden.

6.2 Beinhaltete Daten

In der Personalanforderung wird ein Anforderungsprofil mit gesuchten Qualifikationen sowie Kopfdaten zur Stelle übermittelt.

- In einer Personalanforderung werden keine personenbezogenen Daten von Kandidaten gespeichert.
- Von Backend-Anwendern, die in die Personalanforderung involviert sind, wird lediglich eine Referenz-ID gespeichert, keine weiteren personenbezogenen Daten.

Alle weiteren Felder dienen der Information und/oder zur Prozesssteuerung. Eine detaillierte Auflistung der Felder findet sich im Dokument KON_FHH-19-002_Umsetzungs-Dokumentation.docx.

6.3 Mögliche Änderung des Objekt-Zustands - Überblick

| Aktion ² | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|---|
| Archivieren | ja | Die Personalanforderung ist nicht mehr auf dem Cockpit zu finden. Die Personalanforderung kann nicht bearbeitet werden. Die Personalanforderung ist für Backend-Anwender nicht einsehbar. |
| Sperren | ja | Die Personalanforderung ist für Backend-Anwender nicht einsehbar. |
| Pseudonymisieren | nein | n. a. |
| Anonymisieren | nein | n. a. |
| Löschen | nein | n. a. |

6.3.1 Archivieren

6.3.1.1 Automatische Archivierung

Es wird keine automatische Archivierung durchgeführt.

² Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

6.3.1.2 Manuelle Archivierung

Um eine Personalanforderung in den Status „archiviert“ zu setzen und damit aus dem Backend zu entfernen, sind folgende Vorbedingungen notwendig:

- Die Personalanforderung befindet sich im Status „inaktiv“.

Sollte diese Bedingung nicht erfüllt sein, wird die Aktion „Archivieren“ nicht zur Auswahl angeboten.

6.3.2 Sperren

Eine Personalanforderung kann manuell für alle Anwender gesperrt werden, wenn sie inaktiv ist und keine Objekte darunter existieren.

Die Personalanforderung wird dafür in den Workflow-Status „gelöscht“ gesetzt.

6.3.3 Pseudonymisieren

Es wird keine Pseudonymisierung durchgeführt.

6.3.4 Anonymisieren

Es wird keine Anonymisierung durchgeführt.

6.3.5 Löschen

Es wird keine Löschung durchgeführt.

Ein Löschen ist aufgrund der Integrität der erfassten Daten (Konsistenz der Datenbank) nicht möglich.

7 Objekt „Vakanz“

7.1 Beschreibung

Für jede zu besetzende Stelle wird eine Vakanz benötigt. Eine Vakanz enthält die strukturierten Daten einer Stellenausschreibung. Eine Vakanz ist Voraussetzung für die Erstellung einer Stellenanzeige und notwendig für die Erfassung von Bewerbungen.

7.2 Beinhaltete Daten

Eine Vakanz beinhaltet Informationen zur ausgeschriebenen Stelle (z.B. Art der Stelle, Zeitpunkt der Besetzung, am Prozess beteiligte Systemnutzer, Anforderungen an die Qualifikation des Kandidaten, Einsatzort).

In einer Vakanz werden keine personenbezogenen Daten von Kandidaten gespeichert.

- Von Backend-Anwendern, die in die Vakanz involviert sind, wird lediglich eine Referenz-ID gespeichert, keine weiteren personenbezogenen Daten.

Alle weiteren Felder dienen der Information und/oder zur Prozesssteuerung. Eine detaillierte Auflistung der Felder findet sich im Dokument KON_FHH-19-002_Umsetzungs-Dokumentation.docx.

7.3 Mögliche Änderung des Objekt-Zustands - Überblick

| Aktion ¹ | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|--|
| Archivieren | ja | Die Vakanz wird im Archiv angezeigt. Sie ist nicht mehr im Navigationsbaum und in den Desktops zu finden. Die Vakanz ist ausschließlich für Personen einsehbar, die für das Archiv berechtigt sind. Die Vakanz kann nicht bearbeitet werden. Die Vakanz kann von berechtigten Personen re-archiviert werden. |
| Sperren | ja | Die Vakanz ist für Backend-Anwender nicht einsehbar. Die Vakanz ist mittels Sonderberechtigung von einem Datenbank-Administrator einsehbar. |
| Pseudonymisieren | nein | n. a. |
| Anonymisieren | nein | n. a. |
| Löschen | nein | n. a. |

7.3.1 Archivieren

7.3.1.1 Automatische Archivierung

Es wird keine automatische Archivierung durchgeführt.

7.3.1.2 Manuelle Archivierung

Um eine Vakanz in das Archiv verschieben zu können, sind folgende Vorbedingungen notwendig:

- Alle Stellenanzeigen befinden sich in einem finalen Status (z.B. „abgeschlossen“)
- Alle Bewerbungen befinden sich in einem finalen Status (z.B. „eingestellt“, „abgesagt“)

Sollte eine dieser Bedingungen nicht erfüllt sein, wird durch das System eine Fehlermeldung angezeigt:



7.3.2 Sperren

7.3.2.1 Automatische Sperrung

Es wird keine automatische Sperrung durchgeführt.

7.3.2.2 Manuelle Sperrung

Eine Vakanz kann manuell für alle Anwender gesperrt werden, wenn sie inaktiv ist und keine Objekte darunter existieren.

Die Vakanz wird dafür in den Workflow-Status „gelöscht“ gesetzt.

7.3.3 Pseudonymisieren

Es wird keine Pseudonymisierung durchgeführt.

7.3.4 Anonymisieren

Es wird keine Anonymisierung durchgeführt.

7.3.5 Löschen

Es wird keine Löschung durchgeführt.

Ein Löschen ist aufgrund der Integrität der erfassten Daten (Konsistenz der Datenbank) nicht möglich.

8 Objekt „Stellenanzeige“

8.1 Beschreibung

Damit Kandidaten sich online bewerben können, wird mindestens eine Stellenanzeige benötigt. Eine Stellenanzeige stellt den Marketing-Layer einer Stellenausschreibung dar.

8.2 Beinhaltete Daten

Eine Stellenanzeige beinhaltet die zu veröffentlichenden Informationstexte (z.B. Titel, Aufgabenbeschreibung, etc.), Unternehmensbilder sowie Veröffentlichungskanäle und Gültigkeitsdauer.

In einer Stellenanzeige werden keine personenbezogenen Daten von Kandidaten gespeichert.

Von Backend-Anwendern, die in die Stellenanzeige involviert sind, werden im Rahmen der HTML-Generierung gespeichert:

- Vorname
- Nachname
- ggf.-falls Kontaktdaten (z.B. Unternehmensanschrift), sofern angegeben

Weiterhin können sich sowohl im Anzeigentext (Freitext) als auch in individuell angepassten Abschnitten der Stellenanzeige (z.B. Links zu Social-Network-Profil des Ansprechpartners) zusätzliche personenbezogene Daten befinden.

Alle weiteren Felder dienen der Information und/oder zur Prozesssteuerung. Eine detaillierte Auflistung der Felder findet sich im Dokument KON_FHH-19-002_Umsetzungs-Dokumentation.docx.

8.3 Mögliche Änderung des Objekt-Zustands - Überblick

| Aktion ³ | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|--|
| Archivieren | Ja | Die Stellenanzeige wird im Archiv angezeigt. Sie ist nicht mehr im Navigationsbaum und in den Desktops zu finden. Die Stellenanzeige ist ausschließlich für Personen einsehbar, die für das Archiv berechtigt sind. Die Stellenanzeige kann nicht bearbeitet werden. Die Stellenanzeige kann von berechtigten Personen re-archiviert werden. |
| Sperrern | Ja | Die Stellenanzeige ist für Backend Anwender nicht einsehbar. Die Stellenanzeige ist mittels Sonderberechtigung von einem Datenbank-Administrator einsehbar. |

³ Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

| | | |
|------------------|------|-------|
| Sperren | Nein | n. a. |
| Pseudonymisieren | Nein | n. a. |
| Anonymisieren | Nein | n. a. |
| Löschen | Nein | n. a. |

8.3.1 Archivieren

8.3.1.1 Automatische Archivierung

Es wird keine automatische Archivierung durchgeführt.

8.3.1.2 Manuelle Archivierung

Um eine Stellenanzeige in das Archiv verschieben zu können (setzen des Status „archiviert“), ist folgende Vorbedingung notwendig:

- Die Stellenanzeige ist im Status „inaktiv“.

Sollte diese Bedingung nicht erfüllt sein, wird durch das System die Aktion „archivieren“ nicht zur Auswahl angeboten.

8.3.2 Sperren

8.3.2.1 Automatische Sperrung

Es wird keine automatische Sperrung durchgeführt.

8.3.2.2 Manuelle Sperrung

Eine Stellenanzeige kann manuell für alle Anwender gesperrt werden, wenn sie inaktiv ist und keine Bewerbungen auf diese Stellenanzeige eingegangen sind.

Die Stellenanzeige wird dafür in den Workflow-Status „gelöscht“ gesetzt.

8.3.3 Pseudonymisieren

Es wird keine Pseudonymisierung durchgeführt.

8.3.4 Anonymisieren

Es wird keine Anonymisierung durchgeführt.

8.3.5 Löschen

Es wird keine Löschung durchgeführt.

Ein Löschen ist aufgrund der Integrität der erfassten Daten (Konsistenz der Datenbank) nicht möglich.

9 Objekt „Frontend Account (Bewerber-Account)“

9.1 Beschreibung

Wenn der Kunde ein Karriereportal (Frontend) von milch & zucker einsetzt, wird pro Kandidat ein Frontend-Account, also ein Benutzerkonto für den Kandidaten erstellt, wenn der Kandidat sich bewirbt, oder wenn er eine andere Funktion nutzt, für die ein Account erforderlich ist, zum Beispiel die Funktion „Jobmerker“.

Mit dem Frontend-Account erhält der Kandidat Zugang zu seinem persönlichen Karrierebereich, in dem er seine eingereichten Bewerbungen und deren Status, seine E-Mail-Korrespondenz sowie seine gemerkten Jobs einsehen kann. Er kann dort seine Job Abos und gegebenenfalls sein Talentpool-Profil verwalten.

9.2 Beinhaltete Daten

Ein Frontend Account beinhaltet

- Anrede,
- Vorname,
- Nachname,
- E-Mail-Adresse,
- Nutzernamen und
- Passwort (Hash)
- Passworthistorie

eines Kandidaten.

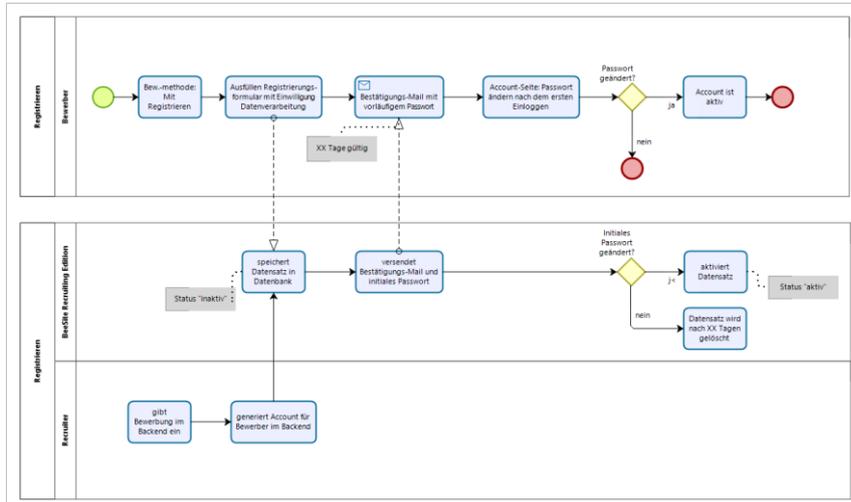
9.3 Bewerber-Account für das Frontend erstellen

Es gibt zwei Möglichkeiten, wie ein Kandidat ein Benutzerkonto erhält.

9.3.1 Registrierung durch den Kandidaten

Der Kandidat füllt ein Registrierungsformular aus, um sich einen Account anzulegen. Nach Absenden des Formulars werden die Account-Daten in der Datenbank gespeichert. Das Anlegen des Accounts erfolgt im Opt-In-Verfahren. Der Kandidat erhält ein vorläufiges Passwort per E-Mail, mit dem er sich einloggen kann und das er nach dem ersten Einloggen ändern muss.

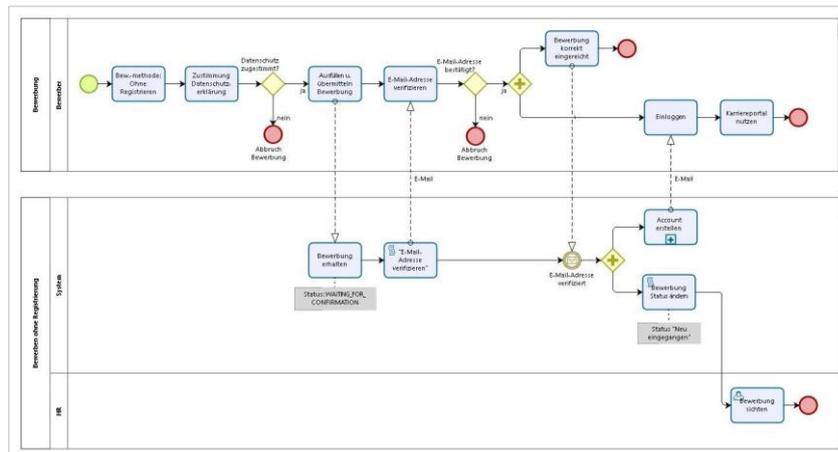
Nur, wenn er sein Passwort ändert, ist der Registrierungsvorgang abgeschlossen und der Frontend Account aktiv.



Prozess der Registrierung und Account-Generierung in der BeeSite Recruiting Edition

9.4 Bewerbung ohne vorherige Registrierung

Ein Kandidat kann sich bewerben, ohne zuvor ein Registrierungsformular auszufüllen. Er übermittelt die Bewerbungsdaten und muss anschließend seine E-Mail-Adresse verifizieren. Hat der das getan, generiert das System automatisch einen Bewerber-Account. Die tatsächliche Nutzung des Accounts erfolgt für den Kandidaten im Opt-In-Verfahren. Der Kandidat erhält ein vorläufiges Passwort per E-Mail, mit dem er sich einloggen kann und das er nach dem ersten Einloggen ändern muss.



Prozess der Account-Generierung ohne vorheriges Registrieren in der BeeSite Recruiting Edition

9.5 Frontend-Account läuft ab

Bei der Registrierung und bei der Bewerbung bestätigt der Kandidat, die Datenschutzhinweise zur Kenntnis genommen zu haben. Werden bei der Bewerbung besondere Kategorien personenbezogener Daten verarbeitet, willigt der Kandidat zusätzlich in die Verarbeitung seiner Daten ein.

Mit Zustimmung ist der Account für eine konfigurierbare Frist gültig. Diese Frist hat keine Datenschutzgründe, sondern dient dem Aufräumen des Systems, um es von veralteten Accounts zu bereinigen. Vor Ablauf der Gültigkeit erhält der Bewerber eine E-Mail mit der Aufforderung, sich erneut am System anzumelden, wenn er seinen Account behalten möchte. Kommt der Kandidat der Aufforderung nicht nach, wird der Account ungültig. Um ungültige Accounts zu bereinigen, kommen folgende Mechanismen zum Einsatz.

Anwendungsfälle:

1. Kandidat reagiert auf den Link und loggt sich ein:
Nach dem Einloggen muss der Kandidat der Datenverarbeitung erneut zustimmen. Der Account ist damit für die konfigurierte Dauer gültig.
2. Kandidat reagiert nicht, hat keine aktiven Bewerbungen und ist in keinem Talentpool:
Der Frontend Account wird deaktiviert.
Nach einer konfigurierbaren Frist wird der Account unwiederbringlich gelöscht.
3. Kandidat reagiert nicht, hat aktive Bewerbungen:
Der Frontend Account wird deaktiviert, aber nicht gelöscht, bis alle aktiven Bewerbungen abgesagt bzw. eingestellt sind. Dieses Verhalten ist konfigurierbar. Wenn ein Kandidat sich nach Ablauf der Frist einloggen möchte, erhält er eine Fehlermeldung und wird gebeten, sich per Kontaktformular zu melden.
4. Kandidat reagiert nicht, ist in einem Talentpool:
Der Kandidat stimmt der Aufnahme in einen Talentpool zu, er erteilt also eine separate Einwilligung zum Zweck der Profilspeicherung. Wenn die Gültigkeit des Accounts abläuft, wird der Frontend-Account deaktiviert.
5. Manuelles Übersteuern durch Administrator:
Wenn ein Kandidat nicht reagiert, kann eine berechtigte Person (Administrator-Rechte) in der Benutzerverwaltung die Datenschutzbestimmung um eine weitere Frist temporär verlängern, wenn sie bereits abgelaufen ist. Diese Zustimmung kann beliebig oft wiederholt werden. Die Frist ist konfigurierbar. Bei der Konfiguration ist folgendes zu beachten: dies sollte nur unter Prüfung des Zwecks der Maßnahme möglich sein, falls der Bewerber keine aktiven Bewerbungen hat und in keinem Talentpool ist. Auf keinen Fall darf eine Verlängerung möglich sein, wenn der Bewerber seinen Account aktiv löscht.

Konfigurierbare Fristen sind im Abschnitt X. Bewerberfristen in KON_FHH-19-002_Dokumentation.docx dargestellt.

Möchte der Bewerber seine Einwilligung in die Datenverarbeitung widerrufen, kann er die Bewerbung zurückziehen bzw. seinen Account löschen.

9.6 Mögliche Änderung des Objekt-Zustands - Überblick

| Aktion ⁴ | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|---|
| Archivieren | nein | n. a. |
| Sperren | nein | n. a. |
| Pseudonymisieren | nein | n. a. |
| Anonymisieren | nein | n. a. |
| Löschen | ja | Der Datensatz wird komplett, auch aus der Datenbank entfernt. |

9.6.1 Archivieren

Es wird keine Archivierung durchgeführt.

9.6.2 Sperren

Es wird keine Sperrung durchgeführt.

9.6.3 Pseudonymisieren

Es wird keine Pseudonymisierung durchgeführt.

9.6.4 Anonymisieren

Es wird keine Anonymisierung durchgeführt.

9.6.5 Löschen

9.6.5.1 Automatische Löschung

Löschen Frontend-Account bei unvollständiger Registrierung

Wird eine begonnene Registrierung nicht erfolgreich abgeschlossen, so wird der zwischenzeitlich gespeicherte Datensatz nach Ablauf einer definierten Frist aus der Datenbank vollständig und unwiederbringlich gelöscht. Es werden keine anonymisierten Daten aufbewahrt.

Der Kandidat erhält hierüber keine Information, bzw. Aufforderung den Vorgang abzuschließen.

Löschen inaktiver Frontend-Account

Nach einer definierten Frist wird ein inaktiver Frontend-Account gelöscht.

Konfigurierbare Fristen im Abschnitt X. Bewerberfristen in Dokument KON_FHH-19-002_Umsetzungs-Dokumentation.docx dargestellt.

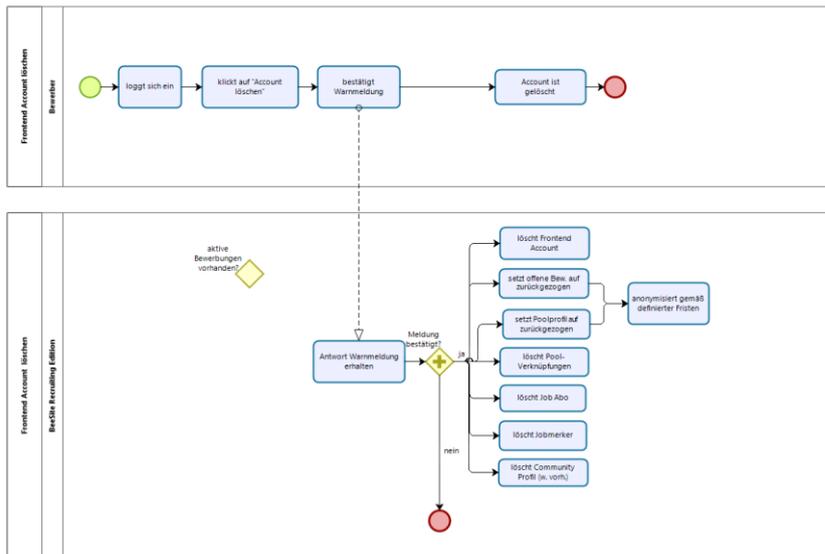
9.6.5.2 Manuelle Löschung

Frontend-Account wird vom Kandidaten gelöscht / zurückgezogen

Ein Kandidat hat auf dem Karriereportal die Möglichkeit, seinen Account zu löschen. Dazu loggt er sich ein und nutzt auf der Seite „Zugangsdaten“ die Aktion „Account löschen“.

⁴ Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

Danach erhält er eine Warnmeldung angezeigt, ob er diesen Schritt wirklich tun möchte und dass er damit seine Bewerbungen zurückzieht und seinen Frontend-Zugang verliert. Erst mit Bestätigung der Warnung wird der Account gelöscht.

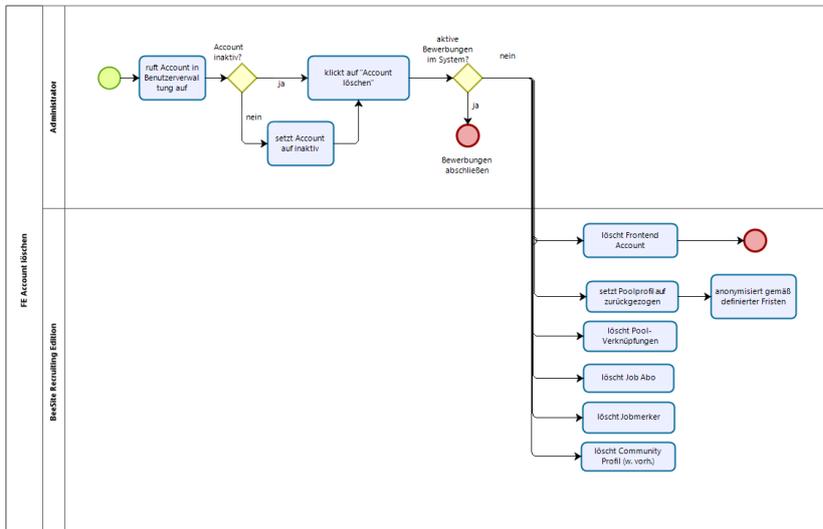


Mit dieser Aktion wird folgendes im System angestoßen:

- Account Daten werden unwiderruflich aus der Datenbank gelöscht.
- Aktive Bewerbungen – sofern vorhanden - werden in den Status „Bewerber zieht zurück“ gesetzt. Damit werden sie gemäß der hierfür definierten Regeln anonymisiert (siehe Kapitel 12, Objekt „Bewerbung“, Seite 30).
- Poolprofile – sofern vorhanden - werden in den Status „Gelöscht“ gesetzt. Damit werden sie gemäß der hierfür definierten Regeln anonymisiert (siehe Kapitel 15, Objekt „Poolprofil“, Seite 40).
- Offene Anfragen zur Poolaufnahme werden – sofern vorhanden – gelöscht.
- Verknüpfungen zu einem oder mehreren Talentpools werden gelöscht.
- Community-Profile - sofern vorhanden - werden in den Status „Gelöscht“ gesetzt. Mit dem Community-Profil weitere verbundene Daten (Likes, Kommentare, Beiträge) werden nicht gelöscht. Da es keine Verbindung zum Profil mehr gibt, sind sie nicht mehr direkt zuordenbar.
- Job-Abonnements und Jobmerker-Einträge – sofern vorhanden - werden gelöscht.

Frontend Account wird vom Administrator gelöscht

Ein Administrator hat in der Benutzerverwaltung die Möglichkeit, einen Frontend-Account zu löschen. Dazu ruft er den Frontend Account auf, inaktiviert zunächst, falls der Account noch aktiv ist und nutzt die Aktion „Account löschen“. Wenn noch aktive Bewerbungen im System sind, erhält der Administrator eine Warnmeldung, dass die Bewerbungen zunächst abzuschließen sind. Sind keine aktiven Bewerbungen mehr im System, wird der Account gelöscht.



Mit dieser Aktion wird folgendes im System angestoßen:

- Account-Daten werden unwiderruflich aus der Datenbank gelöscht.
- Löschung möglicher Social-Network-Account Verknüpfungen
- Löschung der Login-Historie
- Löschung der Passwort-Historie
- Poolprofile – sofern vorhanden - werden in den Status „Gelöscht“ gesetzt. Damit werden sie gemäß der hierfür definierten Regeln anonymisiert (siehe Kapitel 15, Objekt „Poolprofil“, Seite 40).
- Verknüpfungen zu einem oder mehreren Talentpools werden gelöscht.
- Community-Profil - sofern vorhanden - werden in den Status „Gelöscht“ gesetzt. Mit dem Community-Profil weitere verbundene Daten (Likes, Kommentare, Beiträge) werden nicht gelöscht. Da es keine Verbindung zum Profil mehr gibt, sind sie nicht mehr direkt zuordenbar.
- Job-Abonnements und Jobmerker-Einträge – sofern vorhanden - werden gelöscht.

Konfigurierbare Fristen sind im Abschnitt X. Bewerberfristen in KON_FHH-19-002_Dokumentation.docx dargestellt.

10 Objekt "Jobmerker"

10.1 Beschreibung

Mit dieser Funktion wird der Kandidat in die Lage versetzt, interessante Stellen auf einer Merkliste abzuspeichern, um sich später darauf bewerben zu können.

10.2 Beinhaltete Daten

Zur Nutzung des Jobmerkers ist ein Frontend Account nötig, siehe Kapitel 9, Objekt „Frontend Account (Bewerber-Account)“, Seite 22.

Im Jobmerker sind keine weiteren persönlichen Daten gespeichert, so dass nach Zweckerfüllung die Aktionen des Frontend Accounts greifen.

10.3 Mögliche Änderung des Objekt-Zustands - Überblick

Die Nutzung des Jobmerkers ist an den Frontend-Account geknüpft. Ein Jobmerker verfügt über keine eigenen Aktionen.

| Aktion ⁵ | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|-------------|
| Archivieren | nein | n. a. |
| Sperren | nein | n. a. |
| Pseudonymisieren | nein | n. a. |
| Anonymisieren | nein | n. a. |
| Löschen | nein | n. a. |

⁵ Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

11 Objekt „Job-Abo“

11.1 Beschreibung

Mit dieser Funktion kann sich der Kandidat interessante Stellen auf Basis eines persönlichen Suchprofils per E-Mail zusenden lassen.

11.2 Beinhaltete Daten

Folgende Daten des Kandidaten werden gespeichert:

- E-Mail-Adresse.

Die weiteren Daten sind Suchkriterien für Stellenanzeigen wie gesuchtes Einstiegslevel, Tätigkeitsbereich, etc... Eine detaillierte Beschreibung der Felder findet sich in der Frontendbeschreibung.

11.3 Mögliche Änderung des Objekt-Zustands - Überblick

Ein Job Abo verfügt außer Löschen über keine eigenen Aktionen.

| Aktion ⁶ | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|---|
| Archivieren | nein | n. a. |
| Sperren | nein | n. a. |
| Pseudonymisieren | nein | n. a. |
| Anonymisieren | nein | n. a. |
| Löschen | ja | Das Job-Abo ist unwiederbringlich gelöscht. |

11.3.1 Archivieren

Es wird keine Archivierung durchgeführt.

11.3.2 Sperren

Es wird keine Sperrung durchgeführt.

11.3.3 Pseudonymisieren

Es wird keine Pseudonymisierung durchgeführt.

11.3.4 Anonymisieren

Es wird keine Anonymisierung durchgeführt.

11.3.5 Löschen

Der Nutzer kann das Job Abo durch Anklicken eines Links in der Stellenvorschlags-E-Mail löschen.

Die E-Mail-Adresse wird unwiderruflich gelöscht, sofern sie nicht in einem Frontend-Account- oder Bewerbungs-Datensatz gespeichert ist.

⁶ Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

12 Objekt „Bewerbung“

12.1 Beschreibung

Die Bewerbung umfasst

- alle von einem Kandidaten (intern oder extern) eingereichten Daten und Anhänge,
- von Backend-Anwendern des Unternehmens ergänzte Informationen, zum Beispiel Interview-Notizen sowie
- durch das Recruiting-System generierte Daten.

Ein Kandidat kann gleichzeitig mehrere aktive Bewerbungen im Bewerbungsprozess haben.

12.2 Beinhaltete Daten

Die abgefragten Daten werden vom Kunden selbst definiert. Sie können sich je nach Anforderungen der Stelle unterscheiden. Daher können Daten folgender Kategorien verarbeitet werden:

- Persönliche Daten (zum Beispiel Vor- und Nachname, Geburtsdatum, akademischer Titel, Geschlecht)
- Kontaktdaten (zum Beispiel Anschrift, Telefonnummer, Mobilfunknummer, E-Mail-Adresse, Social Media-Profil)
- Angaben zur Ausbildung/Qualifikationen (zum Beispiel Schule/Ausbildung/Studium, Ausbildungsart, Abschluss)
- Angaben zu sonst. Qualifikationen (zum Beispiel Sprachkenntnisse, EDV-Kenntnisse)
- Daten zum bisherigen beruflichen Werdegang, Ausbildungs- und Arbeitszeugnisse, Anschreiben, Lebenslauf (aus hochgeladenen Anhängen)
- Accountdaten (zum Beispiel Benutzername, Passwort)
- Daten, die das System generiert (zum Beispiel Bewerber-ID, Bewerbungsprozesshistorie, Termine bezogen auf das Bewerbungsverfahren)
- Technische Nutzungsdaten bei der Benutzung der Bewerbungsplattform/Besuch der Webseite (zum Beispiel IP-Adresse, Zeit und Datum des Zugriffs, das aufgerufene Dokument sowie verwendeter Browsertyp und Version).
- E-Mail-Korrespondenz bezogen auf das Bewerbungsverfahren
- Besondere Arten personenbezogener Daten (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) werden **tätigkeitsneutral nicht** absichtlich erhoben.
- Besondere Arten personenbezogener Daten hier **Schwerbehinderteneigenschaft** gemäß § 26 Abs. 3 BDSG: Hier ist die Datenverarbeitung erlaubt, da sie gem. § 7 AGG i.V.m. § 164 SGB IX zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht und des Sozialschutzes erforderlich sind.
- Besondere Arten personenbezogener Daten können **tätigkeitsbezogen** erhoben werden, falls zum Beispiel nach einem Foto gefragt wird.
- Backend-Anwenderdaten, z.B. bei Kommentaren, werden lediglich in Form einer Referenz-ID gespeichert, es werden keine weiteren personenbezogenen Daten gespeichert.

12.3 Mögliche Änderung des Objekt-Zustands - Überblick

| Aktion ⁷ | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|--|
| Archivieren | Ja | Die Bewerbung wird im Archiv angezeigt. Sie ist nicht mehr im Navigationsbaum, in der Bewerbersuche und in den Desktops zu finden. Die Bewerbung ist ausschließlich für Personen einsehbar, die für das Archiv berechtigt sind. Die Bewerbung kann nicht bearbeitet werden mit Ausnahme von Kommentaren und "Im Frontend anzeigen". Die Bewerbung kann von berechtigten Personen re-archiviert werden. |
| Sperren | Ja | Die Bewerbung ist pro Workflow-Schritt nur für die berechtigten Personen einseh- oder bearbeitbar. Sind die Anwender für den Prozess-Schritt nicht berechtigt, haben Sie keinen Zugriff auf die Bewerbung. Bei Sperrung für alle Anwender: Die Bewerbung ist für Backend-Anwender nicht einsehbar. Die Bewerbung ist mittels Sonderberechtigung von einem Datenbank-Administrator einsehbar. |
| Pseudonymisieren | Ja | E-Mails: Die Ablage der Nachrichten erfolgt über eine zufällig vergebene individuelle ID, welche in der Datenbank direkt beim Kandidaten gespeichert wird. |
| Anonymisieren | ja | Es werden alle Datenfelder ersetzt, die einen Rückschluss auf eine Person ermöglichen würden (* String = „Anonym.“, * Datum = „0000-00-00“). Ein Rückschluss auf die Person ist nicht möglich. |
| Löschen | Nein | n. a. |

12.3.1 Archivieren

12.3.1.1 Automatische Archivierung

Es wird keine automatische Archivierung durchgeführt.

12.3.1.2 Manuelle Archivierung

Eine berechtigte Person kann eine Bewerbung in das Archiv verschieben.

⁷ Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

12.3.2 Sperren

12.3.2.1 Für einzelne Anwender

Es wird eine Sperrung durch die Konfiguration der Berechtigungen pro Status-Schritt durchgeführt. Je nach Workflow-Schritt ist eine Bewerbung nur für die jeweils zuständigen (berechtigten) Backend-Anwender sichtbar.

Sind die Anwender für den Prozess-Schritt nicht berechtigt, haben Sie keinen Zugriff auf die Bewerbung.

12.3.2.2 Für alle Anwender

Eine Bewerbung kann manuell für alle Anwender gesperrt werden, wenn sie inaktiv ist.

Die Bewerbung wird dafür in den Workflow-Status „gelöscht“ gesetzt.

12.3.3 Pseudonymisieren

In der BeeSite Recruiting Edition werden Daten durch Generieren eines eindeutigen Hash-Wertes automatisch pseudonymisiert.

12.3.3.1 E-Mails

Mit Eingang einer Bewerbung wird automatisch ein begleitendes E-Mail-Postfach (zur Kommunikation mit dem Recruiter) angelegt.

Die Ablage der Nachrichten im begleitenden E-Mail Postfach innerhalb des Mailservers erfolgt über einen zufällig vergebene individuelle eindeutige ID. Die ID wird in der Datenbank direkt beim Kandidat gespeichert.

12.3.4 Anonymisieren

Beim Anonymisieren werden alle Datenfelder des Bewerbungsformulars ersetzt, die einen Rückschluss auf eine Person ermöglichen würden. Eine Ausnahme sind die in den Anonymisierungs- und Löschrregeln genannten Daten. Diese definierten Daten werden nicht anonymisiert, da sie für statistische, nicht personenbezogene Auswertungen herangezogen werden.

Es werden alle Datenfelder ersetzt, die einen Rückschluss auf eine Person ermöglichen würden:

Alle Felder mit „String“ = „Anon.“,

Alle Felder mit „Datum“ = „1800-01-01“.

Alle Felder mit „Uhrzeit“ = „00:00:00“

Alle Felder mit „Nummer“ = „null“

Weitere vorliegende Daten aus beispielsweise Anhängen oder E-Mails werden gelöscht.

Eine vollständige Liste der zu anonymisierenden Daten ist hier nicht beschreibbar, da tätigkeitsbezogen unterschiedliche Daten abgefragt werden und somit von Bewerbung zu Bewerbung verschiedene Daten vorliegen können.

Daher beschreiben die Löschrregeln, welche Daten NICHT anonymisiert oder gelöscht werden. Es ist also implizit ausgedrückt, dass alle anderen Daten anonymisiert bzw. gelöscht werden.

Die Beschreibung der Regeln und Fristen ist im Abschnitt X. Bewerberfristen in KON_FHH-19-002_Dokumentation.docx dargelegt.

12.3.4.1 Automatische Anonymisierung

Bewerbungen in definierten Status, die den Bewerbungsprozess beenden (z. B. eingestellt, abgesagt, nicht eingereicht), werden nach einer konfigurierbaren Frist automatisch anonymisiert. In der Regel werden verschiedene Endstatus zu Statusgruppen zusammengefasst, für die einheitliche Regeln gelten.

Interne und externe Bewerbungen können dabei unterschiedliche Fristen haben.

Konfigurierbare Fristen sind im Abschnitt X. Bewerberfristen in KON_FHH-19-002_Dokumentation.docx dargestellt.

12.3.4.2 Manuelle Anonymisierung

Manuell kann die Anonymisierung im Frontend angestoßen werden:

Der Kandidat kann seine Bewerbung zurückziehen. Dafür loggt er sich in seinen persönlichen Karrierebereich ein und setzt die Bewerbung in den Status „Bewerbung zurückgezogen“. Die Anonymisierung selbst erfolgt dann automatisch - gemäß der für diesen Absage-Status bei externen Bewerbungen definierten Regeln.

12.3.5 Löschen

Bestimmte Datenquellen und damit auch die enthaltenen Daten werden im Zuge der Anonymisierung gelöscht. Welche Daten komplett gelöscht werden, ist im Abschnitt X. Bewerberfristen in KON_FHH-19-002_Dokumentation.docx dargestellt.

Ansonsten wird keine generelle Löschung durchgeführt.

Ein Löschen ist aufgrund der Integrität der erfassten Daten (Konsistenz der Datenbank) nicht möglich.

Werden Daten wie unter Anonymisieren beschrieben verändert, kommt dies einer Löschung gleich.

13 Objekt "Backend-Account" (BeeSite-Anwender / BeeSite-User)

13.1 Beschreibung

Um Stellenanzeigen erstellen oder Kandidaten prozessieren zu können, wird ein Zugriff auf das BeeSite-Backend benötigt.

Mit dem Backend-Account erhält der Anwender (BeeSite-User) gemäß seiner Rolle und Berechtigungen Zugriff auf die Funktionen des Backends, um bspw. Stellen zu veröffentlichen, Bewerbungen zu prozessieren oder administrative Aufgaben zu erledigen. Ein Anwender ist in der Regel Mitarbeiter des Unternehmens.

Ein Backend-Account kann vom Anwender selbst oder von einem Administrator geändert werden.

13.2 Nicht Bestandteil dieses Dokuments

13.2.1.1 Berechtigungen

Die Berechtigungsvergabe für Anwender im Backend ist nicht Teil dieses Dokuments. Es werden keine zugewiesenen Gruppen automatisch durch das System gelöscht bzw. entfernt.

13.2.1.2 Passwörter

Zu jedem Account gibt es ablaufende Passwörter. Da ein abgelaufenes Passwort keinen Einfluss auf eine Deaktivierung oder Löschung des Backend-Accounts hat, wird dies hier nicht weiter behandelt.

Bei Single-Sign-On werden die Passwörter der BeeSite nicht verwendet.

13.3 Beinhaltete Daten

In der Benutzerverwaltung werden mindestens folgende Daten für einen Anwender im Backend erfasst (Pflichtfelder):

- Benutzername
- Sprache
- Passwort (Hash)
- Passworthistorie
- Gruppenzugehörigkeit (Rolle)
- Vorname
- Nachname
- Unternehmens-E-Mail-Adresse des Backend-Anwenders

Weiterhin können folgende Daten erfasst sein (Keine Pflichtfelder):

- Anrede
- Titel
- 2. Vorname
- Personalnummer
- Organisationszugehörigkeit (z.B. zu Standort)
- Postadresse des Unternehmens

- Website des Unternehmens
- Unternehmens-Telefonnummer
- Unternehmens-Faxnummer
- Abteilung
- Bereich
- Funktion

Im Rahmen von SSO (Single Sign On)-Anbindungen können zusätzliche kundenspezifische Daten gespeichert sein.

13.4 Mögliche Änderung des Objekt-Zustands - Überblick

| Aktion ⁸ | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|---|
| Archivieren | nein | n. a. |
| Sperren | ja | <p>Der Anwender kann sich nicht mehr in das System einloggen, wenn sein Account inaktiv ist.</p> <p>Inaktive Accounts sind für andere Anwender nicht mehr auswählbar, um sie als Prozessbeteiligte zu hinterlegen.</p> <p>--- ---</p> <p>Bei Sperrung für alle Anwender (entspricht Status „gelöscht“):</p> <p>Die Accountdaten sind für Backend-Anwender nicht einsehbar.</p> <p>Die Accountdaten sind mittels Sonderberechtigung von einem Datenbank-Administrator einsehbar.</p> |
| Pseudonymisieren | nein | n. a. |
| Anonymisieren | nein | n. a. |
| Löschen | nein | n. a. |

13.4.1 Archivieren

Es wird keine Archivierung durchgeführt.

13.4.2 Sperren

13.4.2.1 Sperren für einzelne Anwender

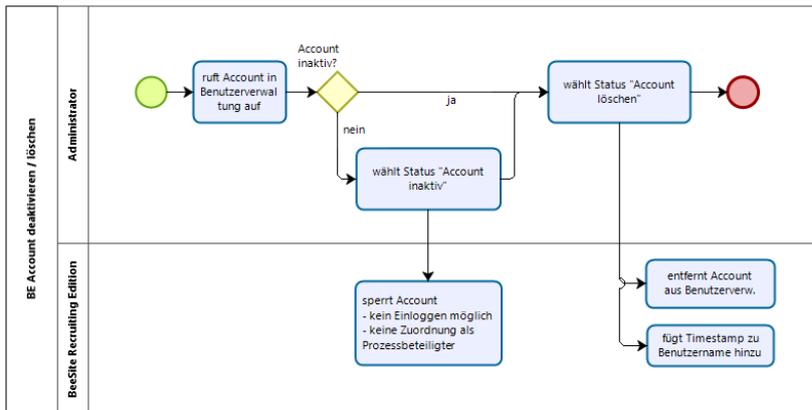
Ein inaktiver Backend Account ist für den Anwender gesperrt. Er hat dann keinen Zugang zum System.

Ein Anwender mit einem inaktiven Account kann von anderen Anwendern nicht als Prozessbeteiligter hinterlegt werden, er wird nicht zur Auswahl angezeigt.

⁸ Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

13.4.2.2 Sperren für alle Anwender

Ein Backend-Account kann manuell für alle Anwender gesperrt werden, wenn er inaktiv ist. Ein Backend-Account wird dafür in den Workflow-Status „gelöscht“ gesetzt. Er ist dann im Backend von keinem Anwender mehr einsehbar. Ein Datenbank-Administrator kann den Backend-Account mittels Sonderberechtigung einsehen.



Powered by
bizagi
Modeler

Beim Sperren für alle Anwender wird der Benutzername zu „\$deletedTIMESTAMP_BENUTZERNAME“ geändert, damit der Benutzername in Zukunft neu vergeben werden kann.

Beispiel: Der Benutzername mmeier wird z.B. zu „\$deleted1493372926_mmeier“

Ein auf „gelöscht“ gesetzter Backend Account kann nicht reaktiviert werden.

13.4.2.3 Erneutes Anlegen eines auf „gelöscht“ gesetzten Accounts bei SSO

Bei Kunden, deren Anwender über eine Schnittstelle automatisch in das System überführt werden, kann es passieren, dass ein gelöschter Account erneut über die Schnittstelle übertragen wird.

In diesem Fall wird ein neuer Account angelegt, der keine Referenz zu dem vorher auf „gelöscht“ gesetzten Account hat. Damit kann es zwei Vorgänge mit demselben Anwendernamen, aber unterschiedliche Accounts geben.

Der neue Account erhält keinen Zugriff auf Vorgänge, Projekte, Vakanzen des alten Accounts.

13.4.3 Pseudonymisieren

Es wird keine Pseudonymisierung durchgeführt.

13.4.4 Anonymisieren

Es wird keine Anonymisierung durchgeführt.

13.4.5 Löschen

Es ist aufgrund der Konsistenz der Datenbank nicht möglich eine Löschung durchzuführen. Stattdessen findet über die KPT-Schnittstelle eine tägliche Überführung und Aktualisierung der Anwender-Daten statt. Wenn Anwender keine Zugriffsberechtigungen mehr haben, wird durch die Aktualisierung der Anwender-Account deaktiviert. Er hat dann keinen Zugang zum System. Dieser Anwender kann von anderen Anwendern nicht als Prozessbeteiligter hinterlegt werden, er wird nicht zur Auswahl angezeigt.

14 Objekt „Termin“

14.1 Beschreibung

Ein Termin ist ein Event, das einen oder mehrere Tage umfasst. Innerhalb eines Termins werden Zeitspannen (Uhrzeit von/bis) eingerichtet, zu denen der Kandidat per E-Mail eingeladen wird.

14.2 Beinhaltete Daten

Ein Termin enthält die Veranstaltungsinformationen: Was, Wann, Wo, mit wem (Bewerber und Mitarbeiter als referenzierte Daten).

In einem Termin werden keine personenbezogenen Daten von Kandidaten gespeichert.

In einem Termin wird lediglich eine Referenz-ID zu Backend-Anwendern gespeichert, keine weiteren personenbezogenen Daten.

Alle weiteren Felder dienen der Information und/oder zur Prozesssteuerung. Eine detaillierte Auflistung der Felder findet sich im Dokument KON_FHH-19-002_Umsetzungs-Dokumentation.docx.

14.3 Mögliche Änderung des Objekt-Zustands – Überblick

| Aktion ⁹ | Kommt zur Anwendung | Erläuterung |
|---------------------|---------------------|--|
| Archivieren | ja | Ein Termin kann archiviert werden. Der Termin steht nicht zur Auswahl bei einer Einladung zur Verfügung. Der Termin ist im Menü Terminplaner als „archiviert“ zu finden. |
| Sperrern | ja | Der Termin ist für Backend-Anwender nicht einsehbar. Der Termin ist mittels Sonderberechtigung von einem Datenbank-Administrator einsehbar. |
| Pseudonymisieren | nein | n. a. |
| Anonymisieren | nein | n. a. |
| Löschen | nein | n. a. |

14.3.1 Archivieren

14.3.1.1 Automatische Archivierung

Es wird keine automatische Archivierung durchgeführt.

⁹ Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

14.3.1.2 Manuelle Archivierung

Ein Termin kann von berechtigten Personen archiviert werden. Der Termin steht dann nicht mehr zur Auswahl bei einer Einladung zur Verfügung.

Der Termin ist im Menü Terminplaner als „archiviert“ zu finden.

Zu beachten:

Wenn ein Kalender archiviert wird, werden die zugehörigen Termine nicht archiviert. Sie behalten in der Datenbank ihren aktuellen Status. Grund: Wenn man mit dem Archivieren des Kalenders auch die zugehörigen Termine archiviert, dann müsste man beim „Zurückholen“ des Kalenders aus dem Archiv auch alle Termine aus dem Archiv zurückholen und in einen passenden Status überführen.

Kommentiert [VS1]: Feedback Tania

14.3.2 Sperren

14.3.2.1 Automatische Sperrung

Es wird keine automatische Sperrung durchgeführt.

14.3.2.2 Manuelle Sperrung

Ein Termin kann manuell für alle Anwender gesperrt werden, wenn sie inaktiv ist und keine Objekte darunter existieren.

Die Personalanforderung wird dafür in den Workflow-Status „gelöscht“ gesetzt.

14.3.3 Pseudonymisieren

Es wird keine Pseudonymisierung durchgeführt.

14.3.4 Anonymisieren

Es wird keine Anonymisierung durchgeführt.

14.3.5 Löschen

Es wird keine Löschung durchgeführt.

15 Objekt „Poolprofil“

15.1 Beschreibung

Das Profil eines Kandidaten in einem Talentpool („Poolprofil“) entspricht einer Bewerbung. Wenn ein Kandidat der Aufnahme in einen Talentpool zustimmt, wird eine Kopie einer Bewerbung im Talentpool als Poolprofil angelegt.

Ein Kandidat kann gleichzeitig mehreren Talentpools zugeordnet sein. Dann wird das Poolprofil mit mehreren Talentpools verknüpft, es wird immer auf dasselbe Poolprofil referenziert.

15.2 Beinhaltete Daten

Die im Datensatz enthaltenen Daten entsprechen den Datenkategorien einer Bewerbung, siehe Kapitel 12.2, Beinhaltete Daten, Seite 30.

15.3 Mögliche Änderung des Objekt-Zustands – Überblick

| Aktion ¹⁰ | Kommt zur Anwendung | Erläuterung |
|----------------------|---------------------|---|
| Archivieren | ja | Das Poolprofil wird im Archiv angezeigt. Es ist nicht mehr in der Talentpool-Verwaltung zu finden. Das Poolprofil ist ausschließlich für Personen einsehbar, die für das Archiv berechtigt sind. Das Poolprofil kann von berechtigten Personen re-archiviert werden. |
| Sperren | nein | n. a. |
| Pseudonymisieren | nein | n. a. |
| Anonymisieren | ja | Das Poolprofil wird nach einer konfigurierbaren Frist anonymisiert. Ein Rückschluss auf die Person ist nicht möglich. |
| Löschen | nein | n. a. |

15.3.1 Archivieren

15.3.1.1 Automatische Archivierung

Es wird keine automatische Archivierung durchgeführt.

15.3.1.2 Manuelle Archivierung

Eine berechtigte Person kann ein Poolprofil in das Archiv verschieben.

¹⁰ Die Begriffe der Änderung des Objekt-Zustands sind hier erklärt: Kapitel 3.8, Allgemeine Begriffs-Definition Aktion / Zustand, Seite 12

15.3.2 Sperren

Es wird keine Sperrung durchgeführt.

15.3.3 Pseudonymisieren

Es wird keine Pseudonymisierung durchgeführt.

15.3.4 Anonymisieren

Ein Poolprofil wird wie eine Bewerbung behandelt, siehe Kapitel 12.3.4 Anonymisieren, Seite 32.

15.3.4.1 Automatische Anonymisierung

Das Poolprofil wird unter folgenden Bedingungen nach konfigurierbaren Fristen automatisch anonymisiert:

- Frontend-Account wird gelöscht.
- Zustimmung zum Talentpool wird nicht erteilt. Nach einer konfigurierbaren Frist wird die Pool-Einladung ungültig. Ein Poolprofil wird gar nicht erst erzeugt.

Talentprofil bei Einstellung

Wird ein Kandidat eingestellt, bleibt aktuell sein Talentprofil erhalten. Über die Rules Engine kann eine Bedingung definiert werden, wann ein Talentprofil anonymisiert wird. Abhängig von der Zielgruppe (z.B. Direkteinstieg, Praktikanten) gibt es unterschiedliche Anforderungen, was mit dem Talentprofil passieren soll.

Konfigurierbare Fristen sind im Abschnitt X. Bewerberfristen in KON_FHH-19-002_Dokumentation.docx dargestellt.

15.3.4.2 Manuelle Anonymisierung

Manuell kann die Anonymisierung im Frontend oder im Backend angestoßen werden:

- Der Kandidat kann seinen Frontend Account löschen. Siehe Kapitel 9.6.5.2, „Manuelle Löschung“, Seite 25. Die Anonymisierung selbst erfolgt dann automatisch – gemäß der für diesen Absage-Status definierten Regeln.

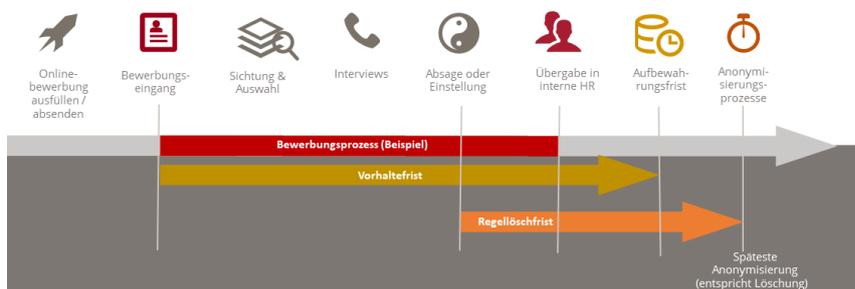
15.3.5 Löschen

Es wird keine Löschung durchgeführt.

16 Anhang –Fristen

16.1 Schaubild Überblick Vorhalte- und Regellöschfrist am Beispiel der Bewerbung

ÜBERBLICK FRISTEN FÜR EINE BEWERBUNG



Vorhaltefrist: das ist die Aufbewahrungsfrist, die zum Beispiel durch rechtliche Vorgaben oder aufgrund von Anforderungen der eigenen Geschäftsprozesse für eine Bewerbung nötig ist.

Regellöschfrist: das ist die Frist für die Löschung einer Bewerbung bei regulärer Verarbeitung. Sie hat im Fall der Bewerbung als Startzeitpunkt das Ende des Bewerbungsprozesses.

Späteste Anonymisierung: An das Ende der Vorhaltefrist kann sich noch eine datenschutzrechtlich vertretbare Frist anschließen, die für die technische Umsetzung der Löschung bzw. Anonymisierung notwendig ist, zum Beispiel automatisierte Anonymisierung nur einmal pro Nacht.

16.2 Konfigurierte Fristen

Folgende Fristen sind konfiguriert.

Siehe Abschnitt X. Bewerberfristen in KON_FHH-19-002_Dokumentation.docx

---- End of Document ----

Anlage 4.2 der Vereinbarung nach § 93 HmbPersVG Vereinbarung über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS)



Projekt

Berbermanagement Einführung (BMS)

Löschfristen

Projektleitung Zentrum für Personaldienste Hamburg

Friederike Vieth (Leitung)
ZPD 21 HR Digital 040 42805-2596 friederike.vieth@zpd.hamburg.de

Stefan Kasimir (Stellvertretung)
ZPD 21 HR Digital 040 42805-2132 stefan.kasimir@zpd.hamburg.de

Version: 1.1
Stand: 16.12.2020

I. Zweck und Aufbau des Dokuments

Ergänzend zum Anonymisierungskonzept (siehe Anlage) werden in diesem Dokument die Bedingungen und Fristen für die Anonymisierung und Löschung von Bewerberdaten festgelegt (Abschnitt II). Ferner werden die Statusgruppen definiert (Abschnitt III), die Account-Regeln beschrieben (Abschnitt IV) und die Erinnerungsregel aufgeführt (Abschnitt V). Zuletzt wird der Umgang mit personenbezogenen Daten aus erweiterten Formularen beschrieben (Abschnitt VI).

II. Löschrufen

| Objekt | Beispiel, Anwendungsfall | Auslöser | Aktion | Start ¹ | Frist ² | Allgemeines, Hintergrund |
|--------------------------------------|-----------------------------------|------------------------------|---------------|--------------------|----------------------------------|--|
| Bewerbung (extern und intern) | Status wird auf gelöscht gesetzt. | Statuswechsel auf „gelöscht“ | anonymisieren | Status gesetzt | mindestens ³ 400 Tage | Grundsätzlich sind Bewerberdaten zu löschen, sobald ihre Speicherung für die Bewerbung nicht mehr erforderlich ist. Die Löschroutine muss deshalb grundsätzlich zeitnah erfolgen. Aber: Einer sofortigen Löschung kann ein berechtigtes Interesse des Verantwortlichen/eine Aufbewahrungsfrist entgegenstehen. Anwendungsfall: Abgesagter Bewerber widerruft seine Einwilligung oder verlangt Löschung all seiner Daten. 2 Monate später meldet er sich wegen Diskriminierung und erhebt weitere 2 Monate später Klage. Um diesen AGG Vorwurf erwidern zu können, dürfen die Bewerberdaten auch nach Zweckwegfall gespeichert bleiben. |

¹ Startzeitpunkt, ab dem die Regellöschfrist läuft

² Frist = Regellöschfrist (Aufbewahrungsfrist). Die Aufbewahrungszeit einer Bewerbung sollte in der Regel sechs Monate nicht überschreiten. **Die Abweichung hier ergibt sich aus der längeren Einspruchsfrist des Beamtenrechts.** Für Angestellte gilt: Ein abgelehnter Bewerber muss derzeit eine Diskriminierung im Bewerbungsverfahren innerhalb von zwei Monaten nach der Ablehnung schriftlich geltend machen. Eine daran anschließende Klage muss gemäß § 61 Abs. 1 ArbGG i.V.m. § 15 AGG innerhalb von drei Monaten, nachdem der Anspruch schriftlich geltend gemacht worden ist, erhoben werden.

³ **Das „mindestens“ ist wie folgt zu verstehen:** Im Widerspruchs- bzw. Klagefall wird die betreffende Vakanz von Hand durch den Recruiter oder Administrator auf den Status „Rechtsstreit“ gesetzt. Das weitere Hochzählen der Löschrufen wird damit ausgesetzt, bis das Verfahren entschieden ist. Daraufhin wird vom Recruiter oder Administrator der neue Status „Rechtsstreit beendet“ gesetzt. Das System ermittelt nun die Differenz zwischen der Regellöschfrist 400 Tage und der Dauer vom Beginn der Ausschreibung bis zum Statuswechsel „Rechtsstreit beendet“, um die verbleibende Speicherdauer zu ermitteln. Die Anzahl der verbleibenden Speichertage beträgt aus Gründen der Verfahrensdokumentation mindestens 30 Tage, ggf. füllt das System die verbleibenden Speichertage entsprechend auf.

| | | | | | | |
|--------------------------------------|--|---|-------------------------------|-----------------------|----------------------|---|
| Bewerbung (extern und intern) | Sonderfall Bewerber nimmt sein Recht auf Widerruf der Einwilligung oder auf Datenlöschung in Anspruch und Administrator setzt den Status auf "Direktanonymisierung". | Statuswechsel auf "Direktanonymisierung" | anonymisieren | Status gesetzt | 1Tag | |
| Bewerbung (extern und intern) | Bewerber ist abgesagt. Auch: Bewerber zieht Bewerbung zurück, nachdem er sie eingereicht hatte. | Statuswechsel auf Status in der Statusgruppe „Abgesagt“ | anonymisieren | Status gesetzt | mindestens* 400 Tage | Vgl. dazu den in Zeile 1 oben geschilderten Anwendungsfall. |
| Bewerbung (extern und intern) | Bewerber reicht Bewerbung nicht ein, speichert sie nur in seinem/ ihrem Account. | Bewerbung abgespeichert | Statuswechsel auf "gelöscht". | Bewerbung gespeichert | 21 Tage | |
| Bewerbung (extern und intern) | Bewerben ohne vorheriges Registrieren erfordert Verifizierung der E-Mail-Adresse. E-Mail-Verifizierung findet nicht statt. | Bewerbung (ohne vorheriges Registrieren) abgesendet | Statuswechsel auf "gelöscht" | Bewerbung gesendet | 21 Tage | |
| Bewerbung (extern und intern) | Bewerber ist abgesagt. Auch: Bewerber zieht Bewerbung zurück, nachdem er sie eingereicht hatte. | Statuswechsel auf Status in der Statusgruppe „Abgesagt“ ⁴ oder „Archiviert“ mit direktem Vorgängerstatus der Statusgruppe „Abgesagt“ | anonymisieren | Status gesetzt | mindestens* 400 Tage | Vgl. dazu den in Zeile 1 oben geschilderten Anwendungsfall. |
| Bewerbung (extern und intern) | Bewerber ist eingestellt. | Statuswechsel auf Status in der Statusgruppe „Eingestellt“ oder „Archiviert“ mit direktem Vorgängerstatus der Statusgruppe „Eingestellt“ | anonymisieren | Status gesetzt | mindestens* 400 Tage | |

⁴ Siehe dazu die Auflistung unter III. unten.

| | | | | | | |
|--------------------------------------|---|---|---------------|-------------------|---|--|
| Bewerbung (extern und intern) | Rechtsstreit ist beendet | Statuswechsel auf Status in der Statusgruppe „Rechtsstreit beendet“ | anonymisieren | Status gesetzt | mindestens* 400 Tage | |
| Bewerbung (extern und intern) | Rechtsstreit ist beendet | Statuswechsel auf „Rechtsstreit beendet“ und Vorgängerstatus in der Historie der Statusgruppe „Eingestellt“ oder „Abgesagt“ | anonymisieren | Status gesetzt | mindestens* 400 Tage ausgehend vom Endstatus; es zählt der Statuswechsel der Gruppe „Abgesagt“ oder „Eingestellt“ | |
| Frontend-Account | Beim Bewerben mit Registrierung: Registrierung nicht abgeschlossen. | Registrierung wurde begonnen und Status ist "noch nicht in Betrieb genommen" (0). | löschen | Account generiert | 21 Tage | |
| Frontend-Account | Administrator / Recruiter generiert Frontend-Account im Backend zu einer Bewerbung. Bewerber reagiert nicht fristgerecht, der Account wird vom Bewerber nicht fristgerecht aktiviert. | Account generiert | löschen | Account generiert | 21 Tage | |
| Frontend-Account | Sonderfall Administrator löscht Frontend Account in der Benutzerverwaltung. | Administrator nutzt Löschen-Funktion. | löschen | Löschen-Aktion | sofort | Kann nur genutzt werden, wenn keine aktiven Bewerbungen mehr im System sind. Ergebnis: * Account-Daten löschen * Job-Abo löschen * Jobmerker löschen |

| | | | | | | |
|-------------------------------------|---|--|---------------|-----------------|----------|--|
| Frontend-Account | Benutzer nutzt Löschen-Funktion im Frontend. | Benutzer löscht seinen Frontend-Account. | löschen | Löschen-Aktion | sofort | Ergebnis: * Account-Daten löschen * Aktive Bewerbungen in Status "Bewerber zieht zurück" setzen. * Poolprofil, sofern vorhanden, in Status "gelöscht" setzen * Verknüpfungen zu Talentpools, sofern vorhanden, löschen * Community-Profil, sofern vorhanden, in Status "gelöscht" setzen * Gespeicherte, nicht eingereichte Bewerbungen auf Status "Gelöscht" setzen * Job-Abo löschen * Jobmerker löschen |
| Frontend-Account | Inaktivität (keine aktive Bewerbungen und letzter Login ist 6 Monate her, eine) Erinnerung zum erneuten Login erfolgt 14 Tage vor Ablauf der 6 Monate | | löschen | Aktivierung | 180 Tage | |
| Job Abo | Nutzer löscht das Job Abo durch Anklicken des Abbestellen-Links in der Stellenvorschlags-E-Mail. | Link angeklickt | löschen | Link angeklickt | sofort | |
| Bewerber (intern und extern) | Alle Bewerbungen, Profile und der Account wurden bereits anonymisiert bzw. gelöscht | | anonymisieren | | sofort | wird eine Bewerbung anonymisiert verliert sie die Verknüpfung zum Datensatz des Bewerbers - folglich kann ein Bewerberdatensatz anonymisiert |

| | | | | | | |
|------------------------|---|--|---------------|--|---|---|
| | | | | | | werden, wenn es keine verknüpften Bewerbungen oder Accounts gibt. |
| Backend Account | Mitarbeiter ist nicht mehr im Unternehmen | | anonymisieren | | nie, bzw. organisatorisch lösen, keine Funktion | Ein Löschen des Datensatzes darf nicht erfolgen, es kann lediglich eine Anonymisierung erfolgen. Sonst geht die Konsistenz der Datenbank verloren. Aktuell kann das nur organisatorisch gelöst werden: bei der Implementierung ist in Absprache mit dem Kunden kann ein Aufräumen (manuell oder programmiert) berücksichtigt werden. Keine Standardfunktionalität! |

III. Statusgruppen

Statusgruppe „Abgesagt“:

- Abgesagt
- Bewerber zieht zurück
- Vermittlung fehlgeschlagen⁵

⁵ Endstatus für Klientenbewerbung im Rahmen eines nicht positiv abgeschlossenen Vermittlungsversuchs.

Statusgruppe „Rechtsstreit beendet“

- Rechtsstreit beendet

Statusgruppe „Eingestellt“:

- Einstellung

Statusgruppe „Archiviert“:

- Archiviert

IV.Account-Regeln

- Nach 5-maliger falscher Passwort-Eingabe wird der Account für 10 Minuten gesperrt.
- Will der Bewerber das Passwort des Accounts ändern, werden die 5 letzten Passwörter geprüft; das neue darf mit einem dieser Passwörter übereinstimmen.
- Das selbst gesetzte Passwort ist 60 Tage gültig.
- Ein generiertes Passwort ist 48 Stunden gültig.
- Passwort vergessen: der Link zur Erzeugung eines neuen Passwortes ist 48 Stunden gültig.

V. Erinnerungen

Bewerber, die Bewerbungen noch nicht bestätigt haben, bekommen nach 7 und 14 Tagen eine Erinnerungs-E-Mail.

Bewerber, die sich 5 Monate und 2 Wochen nicht mit ihrem Benutzerkonto eingeloggt haben, bekommen eine Erinnerungs-E-Mail.

VI.Daten aus erweiterten Bewerbungsformularen

Werden über erweiterte Formulare des Systems, die auch von der Fachlichen Leitstelle selbst angelegt werden können, zusätzliche Daten erfasst, ist im Verfahrensbetriebskonzept zu definieren, ob diese Daten ebenfalls gelöscht werden sollen. Dies gilt auch für die Bewertungsfragebögen, die vom Recruiter ausgefüllt werden. Dabei gelten die gleichen Aufbewahrungsregeln, sofern es sich um personenbezogene Daten handelt. Aus technischen Gründen muss dies allerdings separat definiert werden.

Anhang

- Anonymisierungskonzept (Version 1.0)

Anlage 5 der Vereinbarung nach § 93 HmbPersVG Vereinbarung über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS)

BMS

Katalog der Schnittstellen

| Lfd. Nr. | Bezeichnung der Schnittstelle | Fachlicher Hintergrund | Art der Schnittstelle | Transport | Liefersystem | Zielsystem | Periodizität | Art der Daten |
|----------|-------------------------------|--|-----------------------|-----------|--------------|------------|--------------|---|
| 1 | HASI-Datenexport | Daten zur Personellen Nutzungsberechtigungen und Zuordnung von Nutzenden zu Benutzergruppen | Filesharing | CSV-Datei | HASI | BMS | Täglich | Daten zur Organisation der Berechtigungen und der personellen Zuordnung von Nutzenden zu Benutzergruppen |
| 2 | BMS-Bewerbungsdatenexport | Bewerbungsdaten von den im Stellenbesetzungsverfahren ausgewählten Bewerbenden werden nach KoPers übergeben und den Personalstellen für den weiteren Einstellungsprozess zur Verfügung gestellt. | Webservice | XML | BMS | KoPers | Täglich | Bewerbungsdaten aus dem Bewerbungsverfahren für den Einstellungsprozess im Personalmanagementsystem KoPers. |



Qualifizierungskonzept

zur Einführung des neuen Bewerbungsmanagementsystems
in der Freien und Hansestadt Hamburg

Änderungshistorie

| Version | Datum | Änderung | Autor |
|---------|----------|-------------------------------|---------------|
| 0.1 | 02.04.20 | Ersterstellung erster Entwurf | Manfred Book |
| 0.2 | 27.10.20 | Erstellung Version 0.2 | Nina Lachmann |
| 0.3 | 12.11.20 | Änderungen und Bearbeitung | Nina Lachmann |
| 0.4 | 18.11.20 | Änderungen und Bearbeitung | Nina Lachmann |
| 0.5 | 20.11.20 | Änderungen und Bearbeitung | Nina Lachmann |
| 1.0 | 02.12.20 | Finalisierung | Nina Lachmann |
| | | | |
| | | | |

Glossar

| Abkürzung | Erläuterung |
|--------------------|--|
| BMS | Bewerbungsmanagementsystem |
| BMS Sollprozess | Bezeichnet den Bewerbungsprozess der FHH, der für angebundene Dienststellen mit dem BMS abgebildet wird |
| DSGVO | Datenschutzgrundverordnung |
| FB | Fachbereich |
| FHH | Freie und Hansestadt Hamburg |
| FL | Fachliche Leitstelle |
| ggf. | Gegebenenfalls |
| GSB | Gleichstellungsbeauftragte |
| i. d. R. | In der Regel |
| IE | Informationsempfangende |
| Mobilien-Vorschlag | mobil gemeldete Mitarbeitende innerhalb einer Behörde |
| OE | Organisationseinheit |
| PR | Personalrat |
| PSB | Personalsachbearbeitung |
| R | Recruiting |
| SBV | Schwerbehindertenvertretung |
| SteA | Stellenausschreibung |
| z. B. | zum Beispiel |
| Vakanzen | Vakanzen sind in BMS ein übergreifendes Datenobjekt, zu dem das Recruiting Stellenanzeigen anlegt und zuständige Personen und Personengruppen zuordnet |

Inhalt

| | |
|--|-----------|
| Änderungshistorie | 2 |
| Glossar..... | 3 |
| 1 Einleitung | 5 |
| 1.1 Projekthintergrund und Zielsetzung..... | 5 |
| 1.2 Aufbau des Dokuments..... | 5 |
| 2 Beschreibung des Produkts | 5 |
| 2.1 Beschreibung der Software..... | 5 |
| 2.2 Beschreibung des BMS Sollprozesses..... | 5 |
| 3 Rollen im BMS und Qualifizierungsmaßnahmen..... | 6 |
| 3.1 Recruiting..... | 6 |
| 3.2 Führungskräfte der Fachbereiche | 8 |
| 3.3 Lektorat..... | 8 |
| 3.4 Personalamt P 31 | 9 |
| 3.5 Personalamt P 34 | 10 |
| 3.5.1 P 341 | 10 |
| 3.5.2 P 342 | 10 |
| 3.6 Gremien..... | 11 |
| 3.6.1 Personalrat..... | 11 |
| 3.6.2 Schwerbehindertenvertretung | 12 |
| 3.6.3 Gleichstellungsbeauftragte..... | 12 |
| 3.7 Personalsachbearbeitung | 13 |
| 4 Verantwortliche Stelle für die Qualifizierungsmaßnahmen | 13 |
| 5 Qualitätssicherung und Evaluation | 13 |

1 Einleitung

1.1 Projekthintergrund und Zielsetzung

Für die Freie und Hansestadt Hamburg (FHH) soll eine integrierte und einheitliche Lösung für ein digitales Bewerbungsmanagementsystem (BMS) geschaffen werden. Hierzu wurde vom 02.01.2019 bis zum 31.10.2019 das „Projekt zur Vorbereitung und Durchführung eines Vergabeverfahrens zum Erwerb eines Bewerbungsmanagementsystems für die FHH“ (Projekt-ID: P0000901) umgesetzt. Dieses Projekt endete mit der Beschaffung der Software „BeeSite Recruiting Edition“ der Firma „milch & zucker“. Das am 01.06.2019 gestartete Einführungsprojekt zielt darauf ab, bis zum Projektende am 31.12.2021 für alle potenziellen Personal-Dienststellen die eingekaufte Software einzuführen.

Hiervon ausgeklammert werden die Behörde für Schule und Berufsbildung (inklusive dem Landesbetrieb Hamburgisches Institut für Berufliche Bildung), die Polizei Hamburg, die Feuerwehr Hamburg sowie das Zentrum für Aus- und Fortbildung (Ausbildungsbereich). Der Bewerbungsprozess in diesen Dienststellen ist komplexer als in den anderen Dienststellen und erfordert eine gesonderte Betrachtung der softwareseitigen Anpassungserfordernisse. Vor diesem Hintergrund ist es geplant, in Zusammenarbeit mit diesen Dienststellen im Jahr 2021 separate Projekte für die softwarebezogene Anforderungsgestaltung einzusetzen. In den Verwaltungen der genannten Dienststellen wird jedoch die Software in 2021 eingeführt.

Im vorliegenden Qualifizierungskonzept werden die Qualifizierungsmaßnahmen für die Anwendenden in den Dienststellen der Freien und Hansestadt Hamburg (FHH) beschrieben. Ziel des Qualifizierungskonzeptes ist, die Maßnahmen darzustellen, die künftige Anwendende des neuen BMS vor Anschluss der Behörde an das System befähigen, ihre neuen Aufgaben selbständig und sicher zu erledigen.

1.2 Aufbau des Dokuments

Das Dokument beleuchtet zunächst das Produkt, das für die Qualifizierungsmaßnahmen maßgebend ist. Danach werden die einzelnen Rollen sowie die für die Rollen notwendigen Qualifizierungsmaßnahmen erläutert. Abschließend werden der Zeitraum der geplanten Maßnahmen und die Qualitätssicherung und Evaluation definiert.

2 Beschreibung des Produkts

2.1 Beschreibung der Software

Bei dem BMS der FHH handelt es sich um eine integrierte und einheitliche Standardsoftware der Firma milch & zucker. Das BMS besteht neben dem sogenannten Backend (welches den Recruiting-Prozess auf Seiten der FHH abbildet) auch aus dem sogenannten Frontend (dem Stellenportal, auf dem alle Stellen veröffentlicht werden sowie dem Bewerbungs-Cockpit zur Einreichung der Bewerbungsunterlagen). Beide Module können nicht losgelöst voneinander betrieben werden. Mit Einführung des BMS erfolgt daher auch die Ablösung des bisherigen Stellenportals der FHH.

2.2 Beschreibung des BMS Sollprozesses

Mit der Entwicklung des BMS Sollprozesses soll für alle Dienststellen der FHH eine Vereinheitlichung und Standardisierung im Bewerbungsprozess erzielt werden. Um einen

praxisnahen Sollprozess im neuen BMS abzubilden, der eine geregelte Prozessorientierung und -sicherheit mit der Zielsetzung der Effizienzsteigerung im Bearbeitungsprozess ermöglicht, wurden im Jahr 2019 mehrere Workshops mit den sog. Pilotdienststellen durchgeführt. Das zentrale Charakteristikum des BMS Sollprozesses ist die Rolle des Recruitings als „Hüter des Verfahrens“, die den gesamten Prozess federführend verantwortet bzw. steuert. Der entwickelte BMS Sollprozess, wie er im BMS abgebildet wird, ist die Grundvoraussetzung dafür, das neue Verfahren nutzen zu können und um eine Qualifizierung zu erhalten.

Start der Einführung des BMS erfolgt in den Pilotdienststellen – danach in alle anderen Dienststellen der FHH. Weitere Informationen dazu sind dem [Roll Out Konzept](#) zu entnehmen.

In dem vorliegenden Konzept werden die zentralen Prozessschritte nur soweit herangezogen, wie sie für die Erläuterung im Vorgehen der Qualifizierung notwendig sind. Weitergehende Informationen zum Bewerbungsprozess sind dem [Fachkonzept](#) zu entnehmen. Die Darstellung des gesamten BMS Sollprozesses Metaebene findet sich [hier](#).

3 Rollen im BMS und Qualifizierungsmaßnahmen

Mit der Einführung des neuen BMS ändern sich die Medien, mit dem die Anwendenden ihre Arbeitsaufgaben erledigen. Die dafür erforderlichen Qualifizierungsmaßnahmen verfolgen das Ziel, die Anwendenden entsprechend ihrer Rolle zu einer selbstständigen und sicheren Erledigung ihrer fachlichen Aufgaben zu befähigen.

Bei der Planung der Maßnahmen werden individuelle Faktoren wie Erfahrungen und Aufgaben der Anwendenden, gruppen- und personenspezifische Besonderheiten wie beispielweise Teilzeitarbeit oder körperliche Einschränkung und ggf. geänderte Arbeitsorganisation und Aufgabenstellungen berücksichtigt.

Um die Software nutzen zu können werden die Rollen anhand von Schulungen, Lernvideos und Handbüchern qualifiziert. Die Lernvideos stehen den Anwendenden im Profikanal sowie im Lernportal des ZAF zur Verfügung, die Handbücher sind im BMS hinterlegt. Die Schulungen werden zwei bis drei Wochen vor Anschluss an das BMS angeboten und aufgrund der derzeitigen Corona Situation digital ausgerichtet. Die Inhalte der Qualifizierungsmaßnahmen ergeben sich aus den Lernzielen der einzelnen Zielgruppen. Die Themen wurden in Abstimmung zwischen FHH und milch & zucker erarbeitet.

Vor und während der Einführung steht den Anwendenden innerhalb der eigenen Behörde das sog. Roll Out Gremium zur Seite. Das Roll Out Gremium wird aus dem Roll Out Management (Personalleitung oder Teamleitung) sowie einer Person aus dem Recruiting (Funktion als Multiplikator) gebildet und steht in engem Austausch mit den Mitarbeitenden des Projektteams.

Im laufenden Betrieb werden neue Funktionalitäten im BMS anhand von Release-Notes an alle angeschlossenen Behörden kommuniziert. Ggf. können zusätzliche Kurzschulungen für die Nutzung neuer Funktionalitäten notwendig sein.

3.1 Recruiting

Das Recruiting als „Hüter des Verfahrens“ steuert federführend den gesamten Recruiting-Prozess. Ausgewählte Personen aus dem Recruiting haben zudem die Funktion der Multiplikatoren. Sie sind für den Wissenstransfer innerhalb der eigenen Behörde zuständig – für Führungskräfte, Mitarbeitende, die nur selten mit dem BMS arbeiten und neue Mitarbeitende. Das Recruiting erstellt die Stellenanzeigen, und ist für die Veröffentlichung zuständig. Weiterhin verantwortet und überwacht das Recruiting den Bewerbungsprozess.

Bewerbungsprozess

Das Recruiting hat Zugriff auf alle Informationen zu den Vakanzen und Stellenausschreibungen, für die es berechtigt¹ ist. Zentrale Aktivitäten im Prozess sind:

- Vakanzen anlegen und Kontaktpersonen und Gruppen (Gremien) zuordnen
- Anforderungsprofil mit konstitutiven und vorteilhaften Bedingungen festlegen
- Festlegung der Legende für das Bewerbungsranking in der Vakanzen
- Anlegen der StA (neu oder aus Vorlage erstellen) und SteA bearbeiten
- Einleitung der Abstimmung zur Stellenanzeige zwischen FB, PR und GSB
- Einbindung des Personalamts P 34 oder P 31 zur Sichtung und Freigabe der SteA
- Veröffentlichung der SteA über das Stellenportal
- Terminmanagement aufsetzen und durchführen
- Bewerbungen sichten inklusive Bewerbungsrecht der Bewerbungen prüfen
- Vollständigkeit der Bewerbungen und formale Eignung prüfen
- Finalisierung der Daten für den Bewerbungsvergleich
- Durchführen der Bewerbervorauswahl durch Bewerbungsranking/Bewerbungsvergleich und Weiterleitung der Bewerbungen an Fachbereich, PR und GSB, ggf. SBV
- Prüfung der Gleichbehandlung, falls das Bewerbungsranking geändert wurden
- Durchführung der Einladungsprozesse für die Bewerbenden
- Pflege der Bewertungen nach den Auswahlgesprächen
- Aufbereitung der Daten für die Auswahlentscheidung
- Abstimmung der Auswahlentscheidung mit FB Einbindung des PR, GSB und ggf. SBV zur Auswahlentscheidung
- Aufbereitung der Einstellungsdokumente und Absageprozess einleiten
- Weiterleitung Einstellungsdokumente an Personalsachbearbeitung
- Abschließen der Vakanzen im BMS

Qualifizierungsmaßnahmen und Lernziele

Das Recruiting bildet die größte Gruppe der Anwendenden und muss am intensivsten in der Nutzung des BMS geschult werden.

Folgende Maßnahmen sind vorgesehen:

- Schulung für Recruiting
- Multiplikatoren aus Recruiting für den Wissenstransfer
- Handbuch für Recruiting, begleitend auch als Schulungsunterlage

Die Lernziele sind:

- Sicherer Umgang mit dem gesamten Funktionsumfang des BSM, der dieser Rolle zugeordnet ist
- Durchführung aller Aktivitäten der Rolle im Bewerbungsprozess
- Kenntnisse über Statusmodell der Vakanzen, Stellenanzeigen und Bewerbungen
- Suchen und Auffinden von BMS Datenobjekten (Vakanzen, Stellenanzeigen, Bewerbungen)
- Kenntnisse über die Einbindung und Aktivitäten anderer Rollen
- Kenntnis über die Erinnerungsfunktionen

¹¹ Berechtigungen finden sich im [Berechtigungskonzept](#)

3.2 Führungskräfte der Fachbereiche

Die Führungskräfte der Fachbereiche einer Behörde beauftragen eine zu besetzende Stelle und tragen die fachliche Verantwortung für die Ausschreibungen sowie die Besetzung der Vakanz. Die Führungskräfte in dem stellenausschreibenden Fachbereich sind im Bewerbungsprozess eingebunden und erhalten Zugriff auf das BMS.

Bewerbungsprozess

Das Recruiting arbeitet eng mit dem Fachbereich zusammen, daher integriert das BMS die Führungskräfte der Fachbereiche in den Bewerbungsprozess zu folgenden wesentlichen Aktivitäten:

- Abstimmung der Stelleanzeige mit dem Recruiting vor Veröffentlichung (optional)
- Prüfung der SteA im BMS mit der Möglichkeit Anpassungen vorzunehmen
- Freigabe der SteA im BMS und Rückleitung des Vorgangs an das Recruiting
- Berücksichtigung eines Mobilen-Vorschlags
- Abstimmung der formalen Prüfung einer Bewerbung auf Anfrage des Recruitings
- Überprüfung des Bewerbungsvergleiches (Bewerbungsranking)
- Einsicht der Bewerbungsunterlagen / Interviewleitfaden im BMS
- Bestätigung oder Ablehnung der Auswahlentscheidung im BMS

Qualifizierungsmaßnahmen und Lernziele

Die Führungskräfte der Fachbereiche werden über SteA und Bewerbungen im BMS informiert und im Prozess eingebunden. Die Benutzung des BMS für diese Rolle ist weitestgehend intuitiv.

Folgende Maßnahmen sind vorgesehen:

- Lernvideos
- Multiplikatoren aus Recruiting für den Wissenstransfer
- Handbuch für Führungskräfte der Fachbereiche

Die Lernziele sind:

- Einbindung des Fachbereichs im Bewerbungsprozess und automatisierte Mitteilungen
- Überprüfung, Bearbeitung und Freigabe von Stellenanzeige vor Veröffentlichung
- Abstimmung der formalen Prüfung einer Bewerbung auf Anfrage des Recruitings
- Information, Einsicht und Überprüfung des Bewerbungsvergleiches (Bewerbungsranking)
- Bestätigung oder Ablehnung der Auswahlentscheidungen im BMS

3.3 Lektorat

Das Lektorat wird von dem Recruiting zu einem Ausschreibungsverfahren im BMS festgelegt und somit zu ausgewählten Schritten durch das BMS automatisch informiert. Das Lektorat überprüft die SteA im BMS und nimmt ggf. textliche Änderungen vor, die an das Recruiting über das BMS zurückgemeldet werden.

Bewerbungsprozess

Das Lektorat verantwortet selbst vorgenommene Änderungen der SteA im BMS und ist Teil des Fachbereichs. Es ergeben sich folgende Aktivitäten:

- Benachrichtigung per E-Mail über neue SteA
- Textliche Änderung der SteA und Kommentarfunktion

Qualifizierungsmaßnahmen und Lernziele

Die Qualifizierungsmaßnahmen umfassen die Funktionen, die zur Bedienung und Nutzung der Daten notwendig sind.

Folgende Maßnahmen sind vorgesehen:

- Lernvideo
- Multiplikatoren aus Recruiting für den Wissenstransfer
- Handbuch für Lektorat

Die Lernziele sind:

- Einbindung des Lektorats im Bewerbungsprozess und automatisierte Mitteilungen
- Überprüfung, Bearbeitung und Kommentierung von Stellenanzeige vor Veröffentlichung

3.4 Personalamt P 31

Im Personalamt wird die Qualitätssicherung der SteA für Stellen ab A/E15 im Referat P 31 (Führungskräftegewinnung und -entwicklung) sowie die Prüfung der mobil gemeldeten Mitarbeitenden durchgeführt.

Bewerbungsprozess

Das Personalamt P 31 nutzt folgende zentralen Arbeitsschritte in dem BMS:

- Sichtung und Qualitätskontrolle der an P31 zugeordneten neuen SteA und Vakanzen
- Durchführung der Prüfung der mobil gemeldeten Mitarbeitenden
- Zuordnung möglicher Kandidaten an die Vakanz und Mobilen-Vorschlag an das Recruiting weiterleiten
- Bei Bedarf Anpassung der SteA beim zuständigen Recruiting anstoßen
- Sichtung des Bewerbungsvergleichs und Stellungnahme im BMS
- Nach den Bewerbungsgesprächen, Auswahl der Bewerbenden prüfen und freigeben

Qualifizierungsmaßnahmen und Lernziele

Die Qualifizierung umfasst die Funktionen, die zur Qualitätssicherung der SteA notwendig sind sowie die Möglichkeit des Mobilen-Vorschlags.

Folgende Maßnahmen sind vorgesehen:

- Schulung für P 31
- Handbuch für P 31, begleitend auch als Schulungsunterlage

Die Lernziele sind:

- E-Mail-Benachrichtigungen als automatisierte Informationsquelle
- Bedienkonzept des BMS und Funktionen im Benutzer-Cockpit
- Integration der Prüfung mobil gemeldeter Mitarbeitenden im BMS
- Vorgehen bei der Qualitätsprüfung der SteA und Kommentarfunktion
- Nutzung des Bewerbungsvergleichs mit Kommentarfunktion
- Prozessabläufe und Interaktionen zwischen PA und Recruiting zur Abstimmung
- Abstimmungsprozess und Freigabe der Bewerbungsauswahl

3.5 Personalamt P 34

3.5.1 P 341

Im Personalamt verantwortet das Team P 341 der Abteilung P 34 (Personalgewinnung, Beratung und Controlling) die Qualitätssicherung der SteA für Stellen bis A/E14 sowie die Prüfung der mobil gemeldeten Mitarbeitenden.

Bewerbungsprozess

Das Personalamt P34 Team P341 nutzt das BMS für die folgenden zentralen Arbeitsschritte:

- Sichtung der an P 34 zugeordneten neuen Vakanzen und SteA
- Durchführung der Prüfung der mobil gemeldeten Mitarbeitenden
- Zuordnung möglicher Kandidaten an die Vakanz und Mobilien-Vorschlag an das Recruiting weiterleiten
- Sichtung der SteA im BMS und Qualitätssicherung vor Veröffentlichung
- Bei Bedarf wird eine Anpassung der SteA bei dem zuständigen Recruiting angestoßen

Qualifizierungsmaßnahmen und Lernziele

Die Qualifizierung umfasst die Funktionen zur Qualitätssicherung der SteA und der Prüfung mobil gemeldeter Mitarbeitenden.

Folgende Maßnahmen sind vorgesehen:

- Schulung für P 341
- Handbuch für P 341,

Die Lernziele sind:

- E-Mail-Benachrichtigungen als automatisierte Informationsquelle
- Bedienkonzept und Funktionen im BMS
- Integration der Prüfung mobil gemeldeter Mitarbeitenden im BMS
- Vorgehen bei der Qualitätsprüfung der SteA und Kommentarfunktion
- Nutzung des Bewerbungsvergleichs mit Kommentarfunktion
- Prozessabläufe und Interaktionen zwischen PA und Recruiting zur Abstimmung

3.5.2 P 342

Das Team P342 der Abteilung P34 im Personalamt (Personalgewinnung, Beratung und Controlling) überträgt alle Vakanzen und Stellenanzeigen der Behörden, die nicht an das BMS angeschlossen sind, unabhängig von deren Wertigkeit, in die BMS Anwendung ein.

Bewerbungsprozess

Das Team P 342 ist nicht in den BMS Bewerbungsprozess sondern in den Stellenveröffentlichungsprozess involviert, welcher auch Teil des gesamten BMS-Prozesses ist. Das Team übernimmt die Qualitätssicherung und Eingabe der Stellenanzeigen sowie die Veröffentlichung der SteA für Behörden, die nicht an das BMS angebunden sind. Der verbleibende Bewerbungsprozess wird wie bisher übernommen. Folgende zentrale Aktivitäten werden im BMS durchgeführt:

- Anlegen einer Vakanz und SteA im BMS
- Freigabe der Stellenanzeige und Freischaltung in den Stellenportalen

Qualifizierungsmaßnahmen und Lernziele

Die Qualifizierungsmaßnahmen umfassen die Funktionen, die zur Eingabe der Daten notwendig sind.

Folgende Maßnahmen sind vorgesehen:

- Schulung für P 342
- Handbuch für P 342, begleitend auch als Schulungsunterlage

Die Lernziele sind:

- Bedienkonzept des BMS
- Anlegen einer neuen Vakanz und SteA sowie Stellenveröffentlichung
- Prozessschritte zum „Abschließen einer Vakanz“

3.6 Gremien

Die Gremien der Dienststellen sind in den BMS Sollprozess integriert und haben ein Recht zur Stellungnahme nach § 93 HmbPersVG. Die Behörden wählen drei Vertreter der Gremien, die an den Schulungen teilnehmen sollen.

3.6.1 Personalrat

Zielgruppe

Die Personalratsmitglieder werden gemäß Hamburger Personalvertretungsgesetz eingebunden.

Bewerbungsprozess

Der Personalrat wird zu definierten Zeitpunkten im Bewerbungsprozess zur Kenntnisnahme informiert und zur Stellungnahme aufgefordert:

- Benachrichtigung per E-Mail über neue Vakanz im zuständigen Bereich
- Benachrichtigung per E-Mail über veröffentlichte SteA im zuständigen Bereich
- Benachrichtigung per E-Mail, sobald Bewerbung eingeht und somit Sichtrecht auf Bewerbungen
- Einsichtnahme im Bewerbungsvergleich (Bewerbungsranking)
- Zustimmung oder Ablehnung durch den Personalrat zu der getroffenen Auswahl

Qualifizierungsmaßnahmen und Lernziele

Die Qualifizierungsmaßnahmen umfassen die Funktionen, die zur Bedienung und Eingabe der Daten notwendig sind.

Folgende Maßnahmen sind vorgesehen:

- Schulung für PR
- Multiplikatoren aus Recruiting für den Wissenstransfer
- Handbuch für PR, begleitend auch als Schulungsunterlage

Die Lernziele sind:

- Zeitpunkte und Inhalte der E-Mail-Benachrichtigungen
- Bearbeitung der Stellungnahme zu einer SteA
- Funktionsweise des Bewerbungsvergleich (Bewerbungsranking)
- Prozess und BMS Funktionen zur Zustimmung oder Ablehnung von Bewerbungen durch den Personalrat nach dem Auswahlverfahren
- Rückmeldung über das BMS (Bearbeitung der Stellungnahme)

3.6.2 Schwerbehindertenvertretung

Die Schwerbehindertenvertretung wird gemäß SGB IX eingebunden.

Bewerbungsprozess

Die Schwerbehindertenvertretung wird zu definierten Zeitpunkten im Bewerbungsprozess eingebunden:

- Benachrichtigung per E-Mail über neue Vakanzen im zuständigen Bereich
- Einsichtnahme in Bewerbungsvergleich (Bewerbungsranking) bei Kennzeichnung einer Schwerbehinderung einer Bewerbung
- Benachrichtigung per E-Mail über Bewerbungsauswahl
- Benachrichtigung per E-Mail über Bewerbung mit Kennzeichnung einer Schwerbehinderung im Absageprozess

Qualifizierungsmaßnahmen und Lernziele

Die Qualifizierungsmaßnahmen umfassen die Funktionen, die zur Bedienung und Eingabe der Daten notwendig sind.

Folgende Maßnahmen sind vorgesehen:

- Schulung für SBV
- Multiplikatoren aus Recruiting für den Wissenstransfer
- Handbuch für SBV, begleitend auch als Schulungsunterlage

Die Lernziele sind:

- Zeitpunkte und Inhalte der E-Mail-Benachrichtigungen
- Funktionsweise Bewerbungsvergleich (Bewerbungsranking)
- Rückmeldung über das BMS (Bearbeitung der Stellungnahme)

3.6.3 Gleichstellungsbeauftragte

Die Einbindung der Gleichstellungsbeauftragten erfolgt gemäß Hamburger Gleichstellungsgesetz.

Bewerbungsprozess

Die Gleichstellungsbeauftragten werden zu definierten Zeitpunkten im Bewerbungsprozess eingebunden:

- Benachrichtigung per E-Mail über neue Vakanzen im zuständigen Bereich
- Entwurf der SteA zu Kenntnisnahme
- Benachrichtigung per E-Mail über veröffentliche SteA im zuständigen Bereich
- Einsichtnahme in Bewerbungsvergleich (Bewerbungsranking) zur Kenntnis
- Stellungnahme zur Auswahlentscheidung

Qualifizierungsmaßnahmen und Lernziele

Die Qualifizierungsmaßnahmen umfassen die Funktionen, die zur Bedienung und Eingabe der Daten notwendig sind.

- Schulung für GSB
- Multiplikatoren aus Recruiting für den Wissenstransfer
- Handbuch für GSB, begleitend auch als Schulungsunterlage

Die Lernziele sind:

- Zeitpunkte und Inhalte der E-Mail-Benachrichtigungen

- Funktionsweise Bewerbungsvergleich (Bewerbungsranking)
- Rückmeldung über das BMS (Bearbeitung der Stellungnahme)

3.7 Personalsachbearbeitung

Die Personalsachbearbeitung verantwortet die Einstellung der einzustellenden Person nach der Auswahl und ist damit nicht Teil des eigentlichen Bewerbungsprozesses.

Bewerbungsprozess

Nachdem der Bewerbungsauswahlprozess abgeschlossen ist, erhält die Personalsachbearbeitung Zugriff auf die einstellungsrelevanten Unterlagen.

- Durch das Recruiting erfolgt die Übergabe der einzustellenden Person und dessen Bewerbung an die Personalsachbearbeitung
- Die Personalsachbearbeitung erhält aus dem BMS eine Benachrichtigung per E-Mail

Qualifizierungsmaßnahmen und Lernziele

Die Qualifizierungsmaßnahmen umfassen die Funktionen, die zur Bedienung und Nutzung der Daten notwendig sind.

- Multiplikatoren aus Recruiting für den Wissenstransfer
- Handbuch für PSB

Die Lernziele sind:

- Zeitpunkte und Inhalte der E-Mail-Benachrichtigungen
- Ansicht der Bewerbung, Stellenanzeige, Vakanz
- Öffnen des Dossiers

4 Verantwortliche Stelle für die Qualifizierungsmaßnahmen

Während der Einführung in 2021 übernimmt das Projektteam die Verantwortung für die Qualifizierungsmaßnahmen.

Nach der Einführung wird die Fachliche Leitstelle für die Qualifizierungen zuständig sein. Sie übernimmt dabei die Koordination und/oder Durchführung von Anwendungsschulungen im Rahmen des Anschlusses neuer Dienststellen, neuer Mitarbeitender in den Dienststellen oder nach Einspielung neuer Funktionalitäten und Releases. Sie übernimmt die Erstellung, Pflege und Veröffentlichung von Handbüchern und ähnlichem.

5 Qualitätssicherung und Evaluation

Anwendende, denen eine Schulung zusteht, nehmen an einem festgelegten Schulungstermin teil. Die Termine werden rechtzeitig vor Anbindung der Behörde an das BMS vom Projektteam bekannt gegeben. Sollte eine Person an einem Termin nicht teilnehmen können, wird ein Ausweichtermin angeboten. Der Ausweichtermin richtet sich nach der Zahl der rückgemeldeten Anwendenden und wird bei Bedarf vereinbart.

Die Evaluation des Schulungserfolgs erfolgt unmittelbar im Anschluss einer Schulung durch digitale Fragebögen, entwickelt vom ZAF, die von den Teilnehmenden ausgefüllt an das Projektteam bzw. (noch zu klären) zurück gesendet und im Anschluss ausgewertet werden. Ggf. wird, je nach Ergebnis, ein Systemcoaching in den Behörden angeboten.