

Anlage 1b
Bewerbungsmanagement P31 und P34
Quick Win

Verfahrensbeschreibung

gemäß § 9 HmbDSG

09.03.2012

„Bewerbungsmanagement Quick Win“

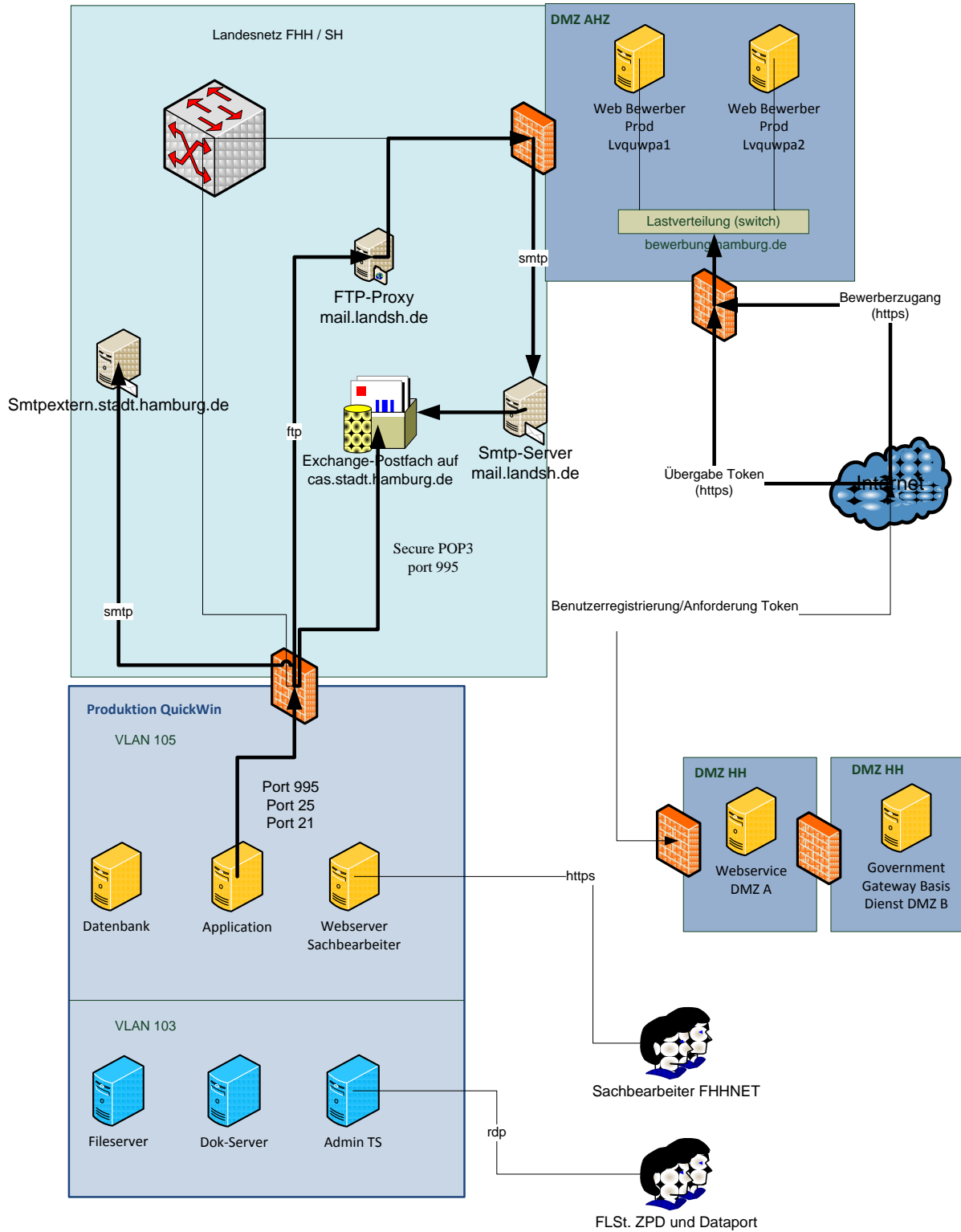
Verfahrensbeschreibung

Verfahrensbeschreibung nach § 9 Hamburgisches Datenschutzgesetz		
1	Name und Anschrift der Daten verarbeitenden Stelle	Senat der Freien Hansestadt Hamburg Personalamt, Referate P31 und P34 Steckelhörn 12, 20457 Hamburg
2.1	Bezeichnung des Verfahrens	Bewerbungsmanagement (Quick Win)
2.2	Zweckbestimmung des Verfahrens	IT-Lösung zur Unterstützung der Wiedereingliederung von Rückkehrern (z.B. Asklepios) und strukturell/ individuell veränderten Mitarbeiterinnen und Mitarbeitern ¹ der Hamburger Verwaltung.
3.1	Art der verarbeiteten Daten	Mitarbeiterdaten, die für eine Vermittlung erforderlich sind: Name, Vorname, Adresse, Schulausbildung, Werdegang, zusätzlich erworbene Qualifikationen sowie Daten über Vermittlungen bzw. Vermittlungsvorschläge mit Angabe der Behörde und der Dauer.
3.2	Rechtsgrundlage	§ 28 Abs. 2 HmbDSG i.V.m. § 85 Abs. 1 HmbBG
4	Kreis der Betroffenen	alle durch die Referate P31 und P34 zu vermittelnden Mitarbeiter und Mitarbeiterinnen der Hamburger Verwaltung (Beschäftigte der FHH) im Rahmen der strukturellen bzw. individuellen Mobilität
5	Empfänger/innen der Daten	-----
5.1	Empfangende dritte Stellen	Keine (i.S.v. § 4 Abs. 4 HmbDSG)
5.2	Auftragsdatenverarbeiter	Dataport i.S.v. § 3 Abs. 1 HmbDSG
5.3	Empfänger/innen innerhalb der Daten verarbeitenden Stelle, die andere Aufgaben wahrnehmen	Personalabteilung des Personalamtes (nur bei erfolgreicher auch befristeter Abordnung)
6	Datenübermittlung nach § 17 Abs. 2 und 3 HmbDSG (Übermittlung an Drittländer)	Keine
7.1	Fristen für die Sperrung der Daten	-----
7.2	Fristen für die Löschung der Daten	Daten werden nach erfolgreicher Vermittlung (Stelle ist unbefristet und ausfinanziert) physisch gelöscht.

¹ Im Folgenden wird nur die männliche Form (der Kürze halber) von den hier erwähnten Personengruppen benutzt, die gleichermaßen die weiblichen Personen beinhaltet.

8	Technische und organisatorische Maßnahmen nach § 8 HmbDSG	Siehe Risikoanalyse Ziffer 2, 3, 4, 5, 9. (Auszug auf Seiten 5 – 8 dieser Verfahrensbeschreibung)
9.1	Art der Geräte	ESARI-PC, siehe zus. Anhang (Systemdarstellung)
9.2	Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benachrichtigung	Übermittlung: erfolgt nicht Sperrung: erfolgt nicht Löschung: Durch den Sachbearbeiter wird ein Datum „Ende des Verfahrens“ gesetzt. Nach Überprüfung, ob Daten wirklich gelöscht werden können, wird eine manuelle Wiedervorlage an die Fachliche Leitstelle erstellt. Die Fachliche Leitstelle löscht die Daten (physisch) und meldet die Löschung zurück an die Sachbearbeiter. Auskunftserteilung gem. § 12 Abs. 1 HmbDSG: Der Ansprechpartner/Vermittler wird dem Mitarbeiter schriftlich durch das Referat P 34 mitgeteilt. Benachrichtigung: nicht erforderlich

QuickWin Produktionsumgebung



Auszug aus der Risikoanalyse Quick Win

2. Art der verarbeiteten Daten

2.1 Werden personenbezogene Daten verarbeitet? ja nein

2.2 Welche Rechtsgrundlagen bestehen?

Die Verarbeitung der erfassten Bewerberdaten geschieht auf Grundlage von § 85 Abs.1 des Hamburgischen Beamtengesetzes (HmbBG) in Verbindung mit § 28 Abs. 2 + 3 des Hamburger Datenschutzgesetz (HmbDSG).

2.3 Welche Daten werden verarbeitet?

Die abgefragten Bewerberdaten orientieren sich grundsätzlich am Anforderungsprofil der Stelle. Auf diesem Weg wird dem Prinzip der Datensparsamkeit Rechnung getragen.

Siehe auch Verfahrensbeschreibung Ziffer 3.1. Darüber hinaus werden je nach ausgeschriebener Stelle (z.B. für Bewerbungen im Bereich des Polizeivollzugsdienstes) auch Angaben erfasst, die möglicherweise Rückschlüsse auf den Gesundheitszustand eines Bewerbers zulassen: Informationen zu einer Schwerbehinderung oder von am Arbeitsplatz benötigten Hilfsmitteln.

Protokolldaten werden nicht für Zwecke der Leistungs- oder Verhaltenskontrolle genutzt.

2.4 Kann der Umfang der verarbeiteten Daten reduziert werden?

(vgl. § 5 Abs. 4 HmbDSG)

ja (ggf. erforderliche Voraussetzungen) nein (Begründung)

Ziel des Bewerbungsprozesses ist eine optimale Besetzung öffentlicher Stellen nach dem Leistungsprinzip (vgl. Art. 33 Abs. 2 GG). Ein Urteil darüber, ob ein Bewerber den Anforderungen einer Stelle entspricht und insbesondere, ob er für die zu besetzende Stelle besser geeignet ist als ein Mitbewerber, kann nur durch ein vollständiges Bewerberprofil, welches Angaben zu jeder Stellenanforderung beinhaltet, getroffen werden.

Dem Prinzip der Datensparsamkeit wird Rechnung getragen indem im Rahmen einer Stellenbeschreibung nur relevante Anforderungen genannt werden. Sollte ein Bewerber dennoch weiterführende Angaben tätigen, die mit der angestrebten Tätigkeit nicht in Bezug stehen, so werden diese Informationen im Bewerbungsprozess nicht verarbeitet.

2.5. Können personenbezogene Daten anonymisiert oder pseudonymisiert werden?

(vgl. § 4 Abs. 9 und 10 HmbDSG)

ja (Beschreibung) nein (Begründung)

Die FHH hat bisher keine Grundsatzentscheidung zu anonymen Bewerbungen getroffen. Derzeit sind anonyme Bewerbungen im System nicht möglich. Dies müsste ggf. im Rahmen der späteren Konzeption des Bewerbungsmanagement für das Gesamtsystem berücksichtigt werden.

2.6 Werden die Betroffenen über die Erfassung ihrer personenbezogenen Daten informiert?

(vgl. § 12 a HmbDSG)

ja (schriftlich) nein (Begründung)

In alle Stellenanzeigen unabhängig vom Veröffentlichungsweg wird ein Hinweis aufgenommen, der auf die elektronische Erfassung schriftlich eingereicherter Bewerbungen hinweist.

2.7 Woher kommen die Daten?

2.7.1 Werden die Daten direkt bei den Betroffenen erhoben? ja nein

Wenn ja, in welcher Form ?

Die Bewerbungsdaten werden von den Bewerbern jeweils selbst erfasst. Der Bewerber hat die Möglichkeit eine Bewerbung online in Form eines strukturierten Formulars zu erstellen. Die Bewerbung wird auf diesem Weg direkt in das P&I Bewerbermodul aufgenommen. Alternativ kann ein Bewerber eine Papierbewerbung erstellen, welche im Nachgang durch die Personalsachbearbeitung der ausschreibenden Organisationseinheit in das P&I Modul eingegeben wird.

2.7.2 Wenn keine Direkterhebung: Auf welchem Weg erfolgt die Datenübermittlung?

2.8 Werden Informationen/Daten aus anderen IT-Anwendungen genutzt? ja nein

- Wenn ja, welche?

- Schnittstelle?

2.9 Ist eine Altdatenübernahme erforderlich ? ja nein

Wenn ja, in welcher Form?

Umfang und Historienzeitraum?

2.10 Werden Daten an andere IT-Anwendungen bzw. Stellen übermittelt?

ja, ohne automatisiertes Abrufverfahren ja, mit automatisiertem Abrufverfahren nein

Aufgrund der zukünftigen Integration, z.B. zu den ressourcensteuernden Verfahren, werden zu einem späteren Zeitpunkt im Rahmen des Projektes Schnittstellen realisiert. Diese werden durch die gesonderte Risikobetrachtung KoPers bewertet.

3. Sperrung und Löschung (vgl. § 19 HmbDSG)

Die erhobenen und gespeicherten Daten werden nach Ablauf des Bewerbungsverfahrens für eine Zeit von 6 Monaten gespeichert gem. § 28 Abs. 6 HmbDSG unter Berücksichtigung des AGG (Allgemeines Gleichbehandlungsgesetz).

4. Berechtigungskonzept

siehe im Dokument Berechtigungskonzept

5. IT- Konzept

Die technische Architektur des Quick Win umfasst sowohl zentral bereitgestellte Komponenten, als auch dezentrale Komponenten. **Zentrale Komponenten** werden in der sicheren Be-

triebsumgebung des Betriebsdienstleisters Dataport betrieben. Hierzu gehören:

- Webserver (zur Generierung der Weboberfläche für die Personalsachbearbeiter),
- Webserver (zur Generierung des Webformulars für externe Bewerber),
- Anwendungsserver (zur Verarbeitung einzelnen Anwendungsfälle/Fachlogik),
- Dokumentenserver (zur Generierung von Dokumenten),
- Datenbank (zur persistenten Ablage von Informationen),
- Client BASIS Modelllinie 1.

Die in der Datenbank vorgehaltenen Informationen werden ausschließlich verschlüsselt, mit Hilfe der Technologie Oracle TDE (Transparent Date Encryption), abgelegt. Die zentralen Komponenten werden physisch in einer eigenen Umgebung betrieben. Der KoPers-Kooperationspartner SH hat auf diese keinen Zugriff.

Dezentrale Komponenten werden zum Zugriff auf die zentralen Komponenten benötigt. Es handelt sich dabei um:

- Web-Oberfläche für die Personalsachbearbeiter,
- Web-Oberfläche für externe Bewerber.

Die Web-Oberflächen kommunizieren verschlüsselt mit Hilfe des HTTPS Protokolls mit dem zentral in der sicheren Betriebsumgebung laufendem Webserver. Auf dem dezentralen Client werden Sie innerhalb eines Browsers (Internet Explorer) vorgehalten. Auf den dezentralen Clients wird keine Programmlogik (lediglich JavaScript für die Darstellung) ausgeführt. Somit ist die gesamte Geschäftslogik auf den zentralen Komponenten gekapselt und ein Kompromittieren der Anwendung wird erschwert. Die Komponenten (Web- und Mailserver) zur Anbindung der Web-Oberfläche für die Bewerber führen eine Zwischenspeicherung (Caching) personenbezogener Daten nur durch, falls und solange dies für die technische Übertragung der Informationen notwendig ist.

Der Zugriff auf die Geschäftslogik über die per Web-Oberfläche für die Personalsachbearbeiter angebotene Funktionalität ist durch ein Passwort abgesichert, welches systemisch der aktuellen Passwortrichtlinie entsprechen muss. Nur die Angabe einer gültigen Nutzer/Passwort Kombination erlaubt einen Zugriff auf die im Rahmen der Berechtigung vorgesehenen Geschäftsfälle. Ein Single-Sign-On (SSO) in Kombination mit anderen Fachverfahren ist nicht vorgesehen. Somit ist bei jedem Öffnen der Web-Oberfläche eine individuelle Eingabe des Passwortes erforderlich.

Eine Integration des Webformulars für die Bewerber in das Hamburg Gateway ist vorgesehen. Das Formular für Bewerber wird durch einen Webserver erzeugt, der in einer demilitarisierten Zone (DMZ Altenholz) gehostet wird. Das Formular greift somit nicht direkt auf die in der sicheren Betriebsinfrastruktur vorgehaltenen zentralen Komponenten zu. So wird verhindert, dass Bewerber einen unbefugten Zugriff auf das Fachverfahren bzw. andere Inhalte des FHH Netzes erlangen können. Bewerber benötigen einen Zugang für das Hamburg Gateway in der Stufe 1 (Authentifizierung über eine eMail-Adresse).

Notfallkonzept

Ein Notfallkonzept, welches den Betrieb bzw. die Wiederaufnahme des Betriebs des Quick Wins im Falle schwerwiegender Betriebsstörungen sicherstellt, wird als Bestandteil des Betriebskonzepts durch die Firma Dataport erarbeitet. Da der Schutzbedarf im Grundwert Verfügbarkeit für den Quick Win „Normal“ beträgt, ist die Notfallkonzeption zum jetzigen Zeitpunkt vernachlässigbar. Sollten aufgrund des Ausfalls von KoPers Daten außerhalb dieses Verfahrens verarbeitet werden, so gelten die bisherigen Regelungen für nicht durch KoPers unterstützte Bewerbungsverfahren.