Anlage 1a

Bewerbungsmanagement
QuickWin

Verfahrensbeschreibung

gemäß § 9 HmbDSG

09.03.2012

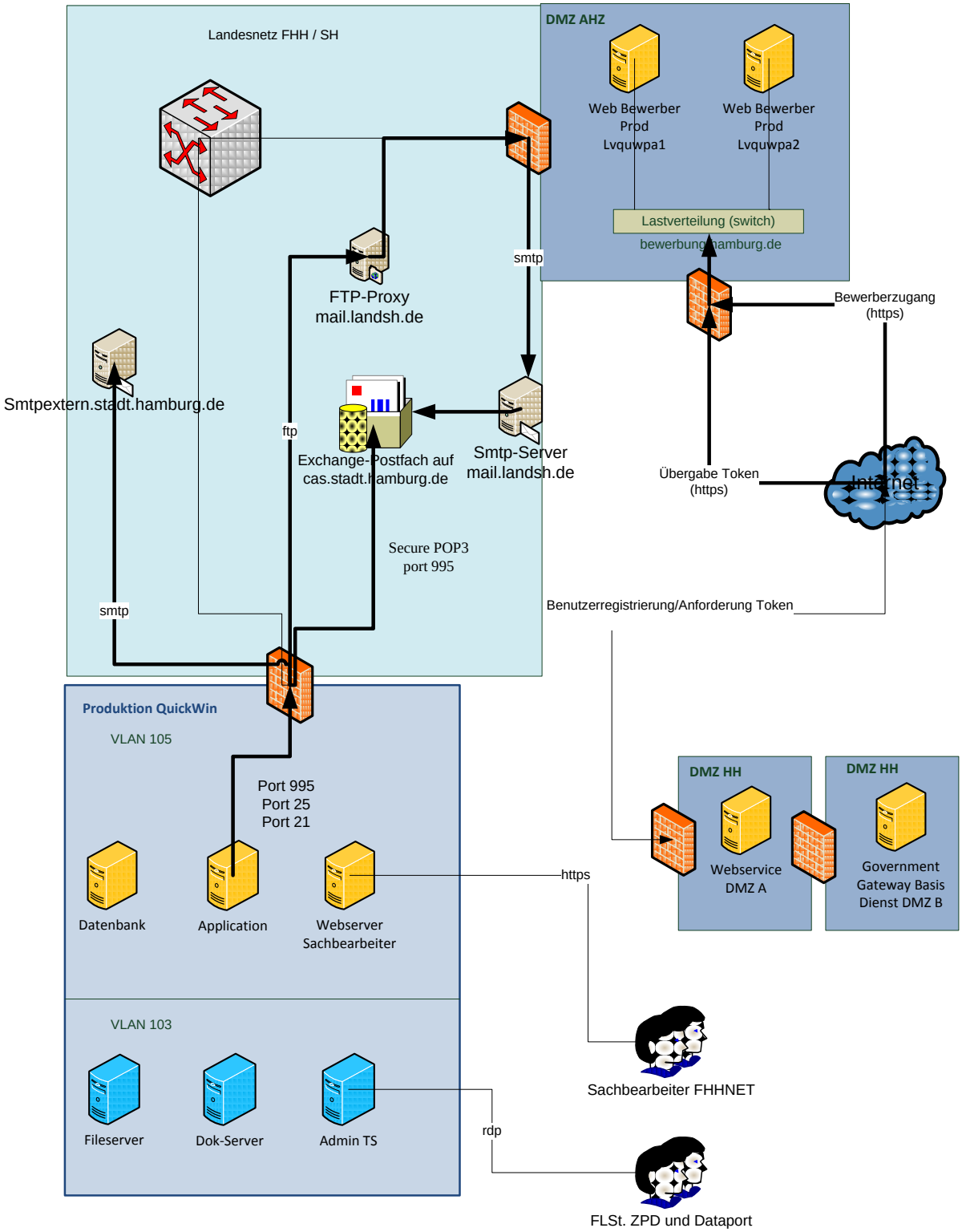
Verfahrensbeschreibung nach § 9 Hamburgisches Datenschutzgesetz		
1	Name und Anschrift der Daten verarbeitenden Stelle	jeweilige Personalabteilung in den am Pilotbetrieb teilnehmenden Fachbehörden – (siehe unten)
2.1	Bezeichnung des Verfahrens	Bewerbungsmanagement (QuickWin)
2.2	Zweckbestimmung des Verfahrens	IT-Lösung zur Unterstützung der Bewerberverwaltung von Mitarbeiterinnen und Mitarbeitern[1] der Hamburger Verwaltung, sowie Externer (Nichtbeschäftigte der FHH).
3.1	Art der verarbeiteten Daten	Bewerberdaten wie Nachname, Vorname, Anschrift, Geburtsdatum sowie Daten der Schulbildung, der Ausbildung, des beruflichen Werdegangs sowie zusätzlich erworbene Qualifikationen.
3.2	Rechtsgrundlage	§ 28 Abs. 2 HmbDSG i.V.m. § 85 Abs. 1 HmbBG
4	Kreis der Betroffenen	Alle Bewerber für eine Anstellung in der Hamburger Verwaltung (Beschäftigte der FHH und Nichtbeschäftigte der FHH)
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	Keine
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	Sofern keine Einstellung erfolgt: unverzüglich, spätestens sechs Monate nach Beendigung des Bewerbungsverfahrens
8	Technische und organisatorische Maßnahmen nach § 8 HmbDSG	Siehe Risikoanalyse Ziffer 2, 3, 4, 5, 9. (Auszug auf Seiten 5 – 10 dieser Verfahrensbeschreibung)
9.1	Art der Geräte	ESARI-PC, siehe zus. Anhang (Systemdarstellung)
9.2	Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benach-	Übermittlung: erfolgt nicht Sperrung: erfolgt nicht Löschung: Durch den Sachbearbeiter/in wird ein

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

	richtigung	Datum „Ende des Verfahrens“ gesetzt. Das System generiert eine automatische Wiedervorlage (Datum+6 Monate). Nach Überprüfung ob Daten wirklich gelöscht werden können, wird eine manuelle Wiedervorlage an die Fachliche Leitstelle erstellt. Die Fachliche Leistelle löscht die Daten (physisch) und meldet die Löschung zurück an die Sachbearbeiter/in. Auskunftserteilung gem. § 12 Abs. 1 HmbDSG: Auskünfte über das Bewerbungsverfahren erteilt dem Bewerber die ausschreibende Behörde. Die Ansprechpartner sind in der jeweiligen Ausschreibung aufgeführt. Behördenseitig werden Verfahrensstände dem Bewerber schriftlich mitgeteilt. Benachrichtigung: nicht erforderlich

Nr.	Behörde/ Amt
1	Personalamt - Referat Interne Personalberatung und -vermittlung, PersonalService Integration (P34)
2	Personalamt -Zentrum für Personaldienste
3	Behörde für Justiz und Gleichstellung - Strafvollzugsamt
4	Behörde für Inneres und Sport - Polizei
5	Behörde für Inneres uns Sport - Einstellungsstelle der Polizei
6	Behörde für Schule und Berufsbildung (für die Bereiche V432 (Verwaltungs-, Haus- und technisches Personal), V439 (Nichtpädagogisches Personal an Schulen), VHS (Volkshochschule) und LI (Landesinstitut für Lehrerbildung und Schulentwicklung)
7	Bezirksamt Eimsbüttel
8	Bezirksamt Hamburg Mitte
9	Bezirksamt Harburg
10	Finanzbehörde - Steuerverwaltung
11	Finanzbehörde - Steuerverwaltung (Nachwuchskräfte)
12	Finanzbehörde
13	Behörde für Gesundheit und Verbraucherschutz

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 eingereichter 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 QuickWin 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) personenbezogene 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. Die 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.

9. Beschreibung der technischen und organisatorischen Maßnahmen

9.1. Client-PCs und Notebooks werden über den BASIS-Standard geschützt (Virenscanner, Passwortschutz, usw.)
9.2. Einsatz von SafeGuard zur Festplattenverschlüsselung auf allen Notebooks.
9.3. Passwortgeschützter Bildschirmschoner verkürzt auf 10 Minuten.
9.4. Zugriff auf die Anwendung ist passwortgeschützt, kein Single-Sign-On.
9.5. Passwortschutz entsprechend der Passwort-Richtlinie realisiert. Die Verwaltung der Kennungen, Passwörter und Benutzerberechtigungen erfolgt durch die Fachliche Leitstelle Bewerbermanagement. Ein Zugang zum Verfahren wird nur nach autorisiertem Benutzerantrag freigeschaltet. Der Benutzerantrag wird revisionssicher aufbewahrt.
9.6. Die Installation von Programmen, die Administrationsrechte benötigen, ist nicht möglich.
9.7. Zugriffsverwaltung auf Basis eines Berechtigungskonzepts, Trennung zwischen Benutzerverwaltung und Anwendung (vgl. Freigaberichtlinie, siehe auch 9.5.).
9.8. Datenschutzrechtliche Belehrung der Anwenderinnen und Anwender über die Benutzung von USB-Sticks oder CD-ROM (vgl. Richtlinie über die Sicherheit der Datenverarbeitung auf Arbeitsplatzrechnern und sonstigen Endgeräten). Bei Vorliegen geeigneter technischer Lösungen wird die gezielte Sperrung von USB-Ports erneut geprüft.
9.9. Alle Benutzerinnen und Benutzer sind bereits durch die bestehenden Arbeitsprozesse sensibilisiert. Die Gefahren des Missbrauchs von Zugangskennungen und der Passwörter sind allgemein bekannt (vgl. Passwortrichtlinie).
9.10. Alle Benutzerinnen und Benutzer werden umfassend geschult und über datenschutzrelevante Aspekte informiert (vgl. Richtlinie zur Datensicherheit im IuK-Bereich).
9.11. Anbindung der Weboberfläche mit Hilfe des sicheren Transportprotokolls HTTPS. Innerhalb des FHHNET ist ein zusätzlicher Schutz durch das FHHNET Sicherheitskonzept, welches eine Verschlüsselung der Transportwege vorsieht, gegeben.
9.12. Im Rahmen des Verfahrens erfolgt keine Übermittlung sensibler persönlicher Daten per E-Mail.
9.13. Ein Zugang zur Datenbank erfolgt nur über die Anwendung. Ein Zugriff aus anderen Programmen, insbesondere direkt durch den Webclient, erfolgt nicht.
9.14. Server-Betrieb im gesicherten Rechenzentrum von Dataport (Datenverarbeitung im Auftrag). Siehe hierzu auch Datenschutz-Merkblatt sowie die Datenschutzleitlinie von Dataport.
9.15. Vor der Installation der Software bzw. Softwareänderungen werden dies entsprechend des Anforderungsprozesses des Projektes *e*Pers/KoPers (entspricht der Freigaberichtlinie der FHH) einem Funktions- u. Abnahmetest unterzogen.
9.16. Zugangsverfügbarkeit des FHHNETs liegt lt. Dataport bei etwa 98% (redundanter - mehrfach-paralleler - Betrieb der Web- und Anwendungsserver).
9.17. Austausch defekter Workstations kann von Dataport innerhalb von 24 Stunden gewährleistet werden.
9.18. Protokollierungen im Fachverfahren: Neben den eigentlichen Bewerbungsdaten werden im neuen IT-Verfahren alle schreibenden Datenzugriffe sowie Administrationsdaten, z.B. entsprechend der Passwortrichtlinie (Anmeldeprotokoll, Benutzerprotokoll) protokolliert. Auf diesem Weg wird die § 8 Abs.2 Nr. 5 HmbDSG geforderte Revisionssicherheit gewährleistet, so dass feststellbar ist, wer wann welche Daten in welcher Weise verarbeitet hat. Der Einblick in Protokolldaten ist nur einem Nutzer der Fachlichen Leitstelle mit extra Berechtigung möglich, der Zugriff wird im Benutzerprotokoll festgehalten und darf nur in besonderen Einzelfällen erfolgen (z.B. Verdacht der unzulässigen Veränderung von Daten). Die Protokolldateien werden nach einer Frist von einem Kalenderjahr durch die Fachliche Leitstelle gelöscht. Frist wird durch Wiedervorlage überwacht.
9.19. Revisionssichere Mitarbeiterdaten-/Bewerberhistorie
9.20. Zutrittskontrolle zu den Büroräumen der Personalsachbearbeiter (sowohl im Persona-

lamt, als auch in den dezentralen Einheiten) durch Schließsysteme, kein längerer, unbeaufsichtigter Aufenthalt organisationsfremder Personen in den Büroräumen.

9.21. Alle Drucker befinden sich in verschlossenen Räumen mit Knauf an der Tür. Die Benutzerinnen/Benutzer sind über den Schutzbedarf der Ausdrucke informiert. Es besteht die Möglichkeit, Dokumente vertraulich zu drucken.

9.22. Festplatten von Kopierern/Druckern werden nach Beendigung des Druck/Kopierauftrages automatisch gelöscht (Systemeinstellung).

9.23. SQL-Injektion wird in der P&I-Software vermieden indem grundsätzlich mit Bind-Variablen gearbeitet wird. wird. Dies bedeutet, dass zum Einbinden variabler Parameter keine Ersetzung auf String-Ebene stattfindet.

9.24. Monitoring durch die technische Leitstelle zur Erkennung ungewöhnlicher Systemaktivitäten.

9.25. Externe Bewerber können lediglich auf eigene Bewerberinformationen und dies auch nur bis zum Absendezeitpunkt zugreifen.

9.26. Betrieb der Webserver in einer demilitarisierten Zone (DMZ).