

**Anlage 3a  
zur Interimsvereinbarung**

**Quick Win  
Bewerbungsmanagement**

**Berechtigungskonzept**

**09.03.2012**

# Inhalt

<b>1. Allgemeines</b> .....	3
1.1. Rahmenbedingungen .....	3
1.2. Technische Grundlagen.....	3
<b>2. Berechtigungssteuerung</b> .....	4
2.1. Profile .....	4
2.2. Benutzergruppen .....	4
2.3. Benutzer .....	4
2.4. Vertretungsregelungen .....	5
2.5. Musterprofile.....	6
<b>3. Administrative Zuständigkeiten</b> .....	8
3.1. Zentrale Berechtigungsverwaltung.....	8
3.2. Dezentrale Berechtigungsverwaltung.....	9

## 1. Allgemeines

### 1.1. Rahmenbedingungen

Die FHH organisiert ihre Benutzer- und Berechtigungsverwaltung für das bestehende Personalverfahren zentral in der Fachlichen Leitstelle im Zentrum für Personaldienste. Für den Quick Win wird die Fachliche Leitstelle durch das Projekt KoPers/ePers wahrgenommen. Dies umfasst alle Schritte vom Anlegen der Kennung, deren Ausgestaltung mit Berechtigungen und das Planen und Bereitstellen von Profilen (Berechtigungspaketen) zur vereinfachten Administration sowie die Pflege im Betrieb, z.B. Passwortfreischaltung. An dezentraler Stelle werden keine administrativen Aufgaben wahrgenommen.

Es ist derzeit von ca. 100 Anwenderinnen und Anwendern auszugehen, die jährlich ca. 50.000 Bewerbungen (inkl. Nachwuchskräfte) bearbeiten werden.

Im Rahmen des QuickWin wird ein mehrstufiges Berechtigungskonzept eingeführt. Auf diesem Weg wird sichergestellt, dass Mitarbeiter nur auf die Daten Zugriff erhalten, die sie für ihre tägliche Arbeit benötigen.

Für die Administration sind entsprechend des Verwaltungsabkommens zwischen Dataport und den Ländern FHH und SH eine technische Leitstelle, die bei Dataport anhängig ist und eine in Hamburg anhängige fachliche Leitstelle zuständig. Die Leitstellen sind mit erweiterten Rollen ausgestattet, welche einen Zugriff auf Daten für Supportzwecke erlauben.

Fachliche Berechtigungen werden durch die fachliche Leitstelle vergeben. Die fachliche Leitstelle berechtigt einzelne Nutzer hinsichtlich der Systemrollen und führt unterstützende Tätigkeiten wie das Zurücksetzen von Nutzerkennungen durch. Berechtigungsänderungen werden durch die fachliche Leitstelle nur nach schriftlichem Auftrag (mindestens per Mail) und Autorisierung durch einen entsprechend entscheidungsbefugten Mitarbeiter vorgenommen.

### 1.2. Technische Grundlagen

Im Zuge der Rollenkonzeption sind insbesondere folgende technische Rahmenbedingungen zu beachten:

- Die Vergabe von Rollen und Rechten erfolgt im Quick Win Mandanten (nur FHH),
- Die Zuordnung von Benutzern zu Benutzergruppen ist ausschließlich exklusiv, d.h. nur einmalig möglich. Ein Benutzer kann somit zu einem Zeitpunkt nur in einer Benutzergruppe enthalten sein,
- Eine Untergliederung einer Benutzergruppe kann nicht vorgenommen werden. Es ist nicht möglich, eine Benutzergruppe in einer anderen Benutzergruppe anzulegen. Insofern ist über die Anwendung nur eine eindimensionale Darstellung der Berechtigungsstrukturen möglich.

## 2. Berechtigungssteuerung

Die Berechtigungssteuerung ist in folgende Ebenen unterteilt:

- **Profilspezifische** Zugriffsrechte auf Formate (Geschäftsfälle, Auswertungen, Module, etc.),
- Einschränkungen auf organisatorischer Ebene bei der **Benutzergruppe** (für welchen organisatorischen Bereich, Abteilung/Behörde - besteht Zugriff),
- Zusätzliche Einschränkungen am **Benutzer** durch Datensatzebenenberechtigung.

### 2.1. Profile

Auf Profilebene wird der funktionale Zugriff, also das Zugriffsrecht auf Formate (Geschäftsfälle, Auswertungen, Module etc.) definiert. Mit der Anmeldung im System ist die Übernahme einer bestimmten Rolle sowie eines Aufgaben- und Zuständigkeitsgebietes verbunden. Diese Rolle wird in der P&I Berechtigungsverwaltung im Profil beschrieben. Ein Benutzer muss mit mindestens einem Profil verknüpft sein, um sich anmelden zu können.

Im Quick Win werden Geschäftsfälle und Auswertungen zu einem Profil zusammengefasst und mit unterschiedlichen Zugriffsrechten versehen

Legende

SR	= Lese- und Schreibrechte
LR	= Leserechte
RA	= definierte Reports ausführen (Statistische)
RG	= Reports erstellen (Statistische)
Alle	= alle Datensätze der zugeteilten Organisationseinheit

### 2.2. Benutzergruppen

In einer Benutzergruppe werden die Benutzerrechte zu einer Organisationseinheit (Behörde) zusammengefasst. Jedem Benutzer kann genau eine Benutzergruppe zugeordnet werden.

Im Quick Win werden die Benutzer je Behörde einer Benutzergruppe zugeordnet, diese steuert die Berechtigung der einzelnen Ausschreibungen/Bewerberdaten je Behörde und verhindert einen Zugriff auf Daten außerhalb seiner Organisationseinheit.

### 2.3. Benutzer

Jeder Benutzer wird im System mit seinem Benutzernamen, der Funktion, einem Kennwort sowie der Benutzerkennung (entspricht dem Namen) angelegt. Benutzer des Quick Win-Systems ist jede natürliche Person, die sich an dem System anmelden darf. Hierzu wird jedem Benutzer eine eindeutige Benutzerkennung zugeteilt. Diese Benutzerkennung wird bei allen Aktivitäten des Benutzers in der P&I Software in den Logdateien abgespeichert, um die datenschutzrechtlichen Anforderungen (Transparenz) zu erfüllen. Daher muss aus der Benutzerkennung zweifelsfrei erkennbar sein, um welche natürliche Person es sich handelt.

Im Quick Win werden den Benutzern Profile und eine Benutzergruppe zugewiesen. Damit wird sichergestellt, dass nur Daten bearbeitet/eingesehen werden können, für die der jeweilige Benutzer berechtigt ist (Profile). Diese auch nur innerhalb der ihm zugeordneten Behörde (Benutzergruppe). Eine zusätzliche Einschränkung auf Satzebene wird nicht vorgenommen.

Diese Daten werden nicht zur individuellen Leistungs- und Verhaltenskontrolle der Sachbearbeiterinnen und Sachbearbeiter herangezogen und verarbeitet.

#### **2.4. Vertretungsregelungen**

Hinsichtlich der Realisierung der Vertretungsverhältnisse lassen sich zwei Ansätze verfolgen:

Zum einen die **permanente Vertretung** im Rahmen derer dem Vertreter die Berechtigungen des zu Vertretenden dauerhaft und unabhängig von der tatsächlichen Abwesenheit dieser Person zugewiesen werden. Die permanente Vertretung garantiert die Arbeitsfähigkeit der Dienststellen im Vertretungsfall unter Minimierung des administrativen Aufwands, gestattet jedoch den Zugriff auf die Daten des/der zu Vertretenden auch im Nichtvertretungsfall.

Zum anderen die **anlassbezogene Vertretung**, die sich dadurch auszeichnet, dass dem Vertreter Vertretungsrechte ausschließlich für die Zeit der Abwesenheit des zu Vertretenden aktiv eingeräumt werden. Die anlassbezogene Vertretung stellt die zugriffsschutzrechtlich umfassendste Lösung dar, bedingt jedoch einen enormen administrativen Aufwand, da Zugriffsrechte im Rahmen geplanter sowie unvorhergesehener Abwesenheiten zugewiesen und wieder entzogen werden müssen.

Um die datenschutzrechtlich notwendige eindeutige Protokollierung zu gewährleisten, wird folgende Lösung umgesetzt:

- Vertretern werden für den Vertretungsfall zusätzliche Benutzerkennungen zugewiesen,
- Die Zuweisung soll generell permanent bzw. – soweit erforderlich - in Sonderfällen anlassbezogen erfolgen,
- Sofern sich mehr als zwei Personen gegenseitig vertreten, muss pro Person für jeden Vertreter eine Vertreterkennung eingerichtet werden. Um den durch die Pflege der Vertretungskennungen entstehenden Administrationsaufwand möglichst gering zu halten, könnte alternativ in solchen Fällen – soweit möglich - die Geschäftsverteilung derart erfolgen, dass jede Person für den Gesamtaufgabenbereich aller zuständig ist. In diesem Fall könnten die Zugriffsrechte für alle Personen entsprechend umfassend festgelegt werden, eine Vertretung im originären Sinne findet dann nicht statt.

Die Vertretungsregelung im Quick Win wird in Anlehnung an die jeweilige Organisationsstruktur der Behörden durch die jeweiligen Behörden selbst festgelegt und im Rahmen der Benutzerpflege durch die fachliche Leitstelle im System hinterlegt.

## 2.5. Profile

Es wird folgende Profile geben:

- Personalsachbearbeiter der jeweiligen datenverarbeitenden Stelle,
- Vorgesetzte/r der Personalsachbearbeiter  
Zur Einsichtnahme und Kenntnisnahme eines Auswahlverfahrens und zur Auskunftserstattung der Verfahrensstandes für Bewerber,
- Fachliche Leitstelle  
Der Zugriff der Fachlichen Leitstelle auf personenbezogene Daten ist immer einzelfallbezogen, um bei Bedarf den Personalsachbearbeitern im Rahmen des Supports Hilfestellung geben zu können.

lfd. Nr.	Geschäftsfall	Sachbearbeiter/in	Satzebene	Vorgesetzter	Satzebene	Fachliche Leitstelle	Satzebene
1	Ausschreibung DP/ AP erstellen	SR, RA	alle	LR	alle	SR, RA, RG,	alle
2	Ausschreibung Schule	SR, RA	alle	LR	alle	SR, RA, RG	alle
3	Ausschreibung Studium	SR, RA	alle	LR	alle	SR, RA, RG	alle
4	Ausschreibung Promotion	SR, RA	alle	LR	alle	SR, RA, RG	alle
5	Ausschreibung Beruf	SR, RA	alle	LR	alle	SR, RA, RG	alle
6	Ausschreibung Kenntnisse	SR, RA	alle	LR	alle	SR, RA, RG	alle
7	Ausschreibung Veröffentlichung	SR, RA	alle	LR	alle	SR, RA, RG	alle
8	BEW Personaldaten	SR, RA	alle	LR	alle	SR, RA, RG	alle
9	BEW Verfahrensinfo	SR, RA	alle	LR	alle	SR, RA, RG	alle
10	BEW Anschrift	SR, RA	alle	LR	alle	SR, RA, RG	alle
11	BEW Wehr- Ersatzdienst	SR, RA	alle	LR	alle	SR, RA, RG	alle
12	BEW Vertreter/-in Bevollmächtigte	SR, RA	alle	LR	alle	SR, RA, RG	alle
13	BEW Eltern	SR, RA	alle	LR	alle	SR, RA, RG	alle
14	BEW Schulausbildung	SR, RA	alle	LR	alle	SR, RA, RG	alle
15	BEW Studium	SR, RA	alle	LR	alle	SR, RA, RG	alle
16	BEW Promotion/ Habilitation	SR, RA	alle	LR	alle	SR, RA, RG	alle
17	BEW Berufsausbildung/Beruf	SR, RA	alle	LR	alle	SR, RA, RG	alle
18	BEW Kenntnisse	SR, RA	alle	LR	alle	SR, RA, RG	alle
19	BEW Praktika	SR, RA	alle	LR	alle	SR, RA, RG	alle
20	BEW Weiterbildung	SR, RA	alle	LR	alle	SR, RA, RG	alle
21	BEW Berufserfahrung	SR, RA	alle	LR	alle	SR, RA, RG	alle
22	BEW Nebentätigkeit	SR, RA	alle	LR	alle	SR, RA, RG	alle
23	BEW Bewerbung Ausschreibung	SR, RA	alle	LR	alle	SR, RA, RG	alle
24	BEW Fehlende Unterlagen	SR, RA	alle	LR	alle	SR, RA, RG	alle
25	BEW Einladungsverfahren	SR, RA	alle	LR	alle	SR, RA, RG	alle
26	BEW Testergebnis	SR, RA	alle	LR	alle	SR, RA, RG	alle
27	BEW Vorstellungsgespräch	SR, RA	alle	LR	alle	SR, RA, RG	alle
28	BEW Einladung gesundheitlicher Eignungstest	SR, RA	alle	LR	alle	SR, RA, RG	alle
29	BEW Fehlende medizinische Unterlagen	SR, RA	alle	LR	alle	SR, RA, RG	alle
30	BEW Ärztliche Untersuchung	SR, RA	alle	LR	alle	SR, RA, RG	alle
31	BEW Gesamtbewertung	SR, RA	alle	LR	alle	SR, RA, RG	alle
32	BEW Absage nach Vorauswahl	SR, RA	alle	LR	alle	SR, RA, RG	alle
33	BEW Absage nach Eignungsprüfung	SR, RA	alle	LR	alle	SR, RA, RG	alle
34	BEW Absage durch Med.Dienst	SR, RA	alle	LR	alle	SR, RA, RG	alle
35	BEW Bewerbung Abgabe	SR, RA	alle	LR	alle	SR, RA, RG	alle
36	BEW Absage med.Dienst	SR, RA	alle	LR	alle	SR, RA, RG	alle
37	BEW Absage allgemein	SR, RA	alle	LR	alle	SR, RA, RG	alle
38	BEW Zusage	SR, RA	alle	LR	alle	SR, RA, RG	alle
39	BEW MB Einladungen	SR, RA	alle	LR	alle	SR, RA, RG	alle
40	BEW MB Vorstellungsgespräch	SR, RA	alle	LR	alle	SR, RA, RG	alle
41	BEW MB Absage	SR, RA	alle	LR	alle	SR, RA, RG	alle
42	BEW MB Zusage	SR, RA	alle	LR	alle	SR, RA, RG	alle
43	BEW MB Bewerber Status					SR, RA, RG	Alle
44	Protokolldateien	SR, RA	Alle	LR	alle	PT	alle

Legende

Ausschreibung = Stellenausschreibung  
BEW = Bewerbungsverwaltung

MB	= mehrfach Buchungsmaske
SR	= Lese- und Schreibrechte
LR	= Leserechte
RA	= definierte Reports ausführen (Statistische)
RG	= Reports erstellen (Statistische)
Alle	= alle Datensätze der zugeteilten Organisationseinheit
PT	= Protokolldateien einsehen

### 3. Administrative Zuständigkeiten

#### 3.1. Zentrale Berechtigungsverwaltung

Die Aufgabe der zentralen Berechtigungsverwaltung wird bei der Fachlichen Leitstelle angesiedelt. Hier werden Profile definiert, Benutzer Benutzergruppen zugewiesen und grundsätzliche Optionen (u.a. Mindestlänge des Kennwortes, Anzahl der erlaubten Fehlversuche) festgelegt.

Die Einrichtung von neuen Benutzerkennungen wird durch die Anwendungsberater der Behörden mit Nennung des Profils in der Fachlichen Leitstelle beantragt.

Alle Änderungen an Datensätzen mit Personenbezug werden automatisch mit der Benutzerkennung in einer Protokolldatei gespeichert.

Die Protokolldateien entsprechen den allgemeinen Anforderungen an Datensicherheit und Datenschutz. Diese Daten werden nicht zur individuellen Leistungs- und Verhaltenskontrolle der Sachbearbeiterinnen und Sachbearbeiter herangezogen und verarbeitet. Folgende Protokolle sind systemseitig vorgesehen.

#### Anmeldeprotokoll

Die Anmeldungen bzw. Anmeldeversuche der Nutzer werden mit IP-Adresse – Benutzerkennung – Anzahl Anmeldeversuche – Ergebnis – Datum und Uhrzeit gespeichert.

#### Benutzerprotokoll

Gespeichert werden: der Modulaufruf, z.B. Bewerbungsmanagement, die aufgerufene Geschäftsfallmaske, z.B. Bewerberdaten, und die Aktion (Neuanlage/Änderung/Buchen),

Datensatzprotokollierungen – alle Änderungen an Datensätzen mit Benutzerkennung, Datum und Aktion,

Neuanlage Reports – Struktur, Name der Auswertung,

Neuanlage von Geschäftsfallmasken – Namen der Tabelle/Name des Geschäftsfalles.

Der Aufruf der Protokolldateien ist nur über eine separate Benutzerrolle, die ausschließlich das Recht hat, Protokolldateien einzusehen, möglich. Diese Rolle wird den Mitarbeitern der Fachlichen Leitstelle zugewiesen, ein Wechsel der Benutzerrollen wird im Anmeldeprotokoll protokolliert.



### **3.2. Dezentrale Berechtigungsverwaltung**

Im Quick Win wird von der Einrichtung der dezentralen Berechtigungsverwaltung kein Gebrauch gemacht.