

**Anlage 3b
zur Interimsvereinbarung**

**Quick Win
Bewerbungsmanagement
P 31 und P34
Berechtigungskonzept**

09.03.2012

Inhalt

1. Allgemeines	3
1.1. Rahmenbedingungen	3
1.2. Technische Grundlagen.....	3
2. Berechtigungssteuerung	4
2.1. Profile	4
2.2. Benutzergruppen	4
2.3. Benutzer	4
2.4. Vertretungsregelungen	5
2.5. Musterprofile.....	6
3. Administrative Zuständigkeiten	10
3.1. Zentrale Berechtigungsverwaltung.....	10
3.2. Dezentrale Berechtigungsverwaltung.....	10

1. Allgemeines

1.1. Rahmenbedingungen

Die FHH organisiert ihre Benutzer- und Berechtigungsverwaltung für das 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 (Berechtigungs Paketen) zur vereinfachten Administration sowie die Pflege im Betrieb, z.B. Passwortfreischaltung. An dezentraler Stelle werden keine administrativen Aufgaben wahrgenommen.

Es ist derzeit von ca. 40 Anwenderinnen und Anwendern der Referate P31 und P34 auszugehen, die die „Interne Personalberatung und –vermittlung“ bearbeiten.

Im Rahmen des Quick Win 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 entsprechend des Leitstellenordnungsrahmens 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 bzw. Behörde besteht Zugriff),
- Zusätzliche Einschränkungen am **Benutzer** durch Datensatzebenenberechtigungen.

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
RG	= Reports erstellen
MR	= Managementreport erstellen
SP	= Kennzeichen „Spezial Klient“
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 gelten 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 des Personalamtes durch das Personalamt selbst festgelegt und im Rahmen der Benutzerpflege durch die fachliche Leitstelle im System hinterlegt.

2.5. Profile

Es wird folgende Profile/Rollen geben:

- Sachbearbeiter Beratung P31,
- Sachbearbeiter Beratung P34,
- Sachbearbeiter Ausschreibung,
- Sachbearbeiter Controlling,
- Sachbearbeiter PSI,
- Referatsleitung,
- Teamleitung P34,
- Fachliche Leitstelle
Der Zugriff der Fachlichen Leitstelle auf personenbezogene Daten ist immer einzelfallbezogen um bei Bedarf, den Personalsachbearbeitern im Rahmen des Support Hilfestellung geben zu können.

lfd. Nr.	Geschäftsfall	Sachbearbeiter Beratung P34	Satzebene	Sachbearbeiter Beratung P34	Satzebene	Sachbearbeiter Ausschreibung	Satzebene	Sachbearbeiter Controlling	Satzebene	Sachbearbeiter PSI	Satzebene	Referatsleitung	Satzebene	Teamleitung P34	Satzebene	Fachliche Leitstelle	Satzebene
1	Stellenausschreibung	SR, RA	alle o. SP	SR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
2	Stellenausschreibung Laufbahn	SR, RA	alle o. SP	SR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
3	Ausschreibung DP/AP erstellen	SR, RA	alle o. SP	SR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
4	Ausschreibung BKZ	SR, RA	alle o. SP	SR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
5	Ausschreibung Stellenkategorie	SR, RA	alle o. SP	SR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
6	Ausschreibung Veröffentlichung	LR, RA	alle o. SP	LR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	LR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
7	Ausschreibung Schule	SR, RA	alle o. SP	SR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
8	Ausschreibung Studium	SR, RA	alle o. SP	SR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
9	Ausschreibung Promotion	SR, RA	alle o. SP	SR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
10	Ausschreibung Kenntnisse	SR, RA	alle o. SP	SR, RA, SP	alle	SR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
11	Klient Personaldaten	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
12	Klient private Erreichbarkeit	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
13	Klient dienstliche Erreichbarkeit	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
14	Klienten Zuordnung	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle
15	Klienten Verwendungswunsch	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA, SP, RG, MR	alle

			SP	SP			SP	DL, SP			SP				SP	RG, MR	
16	Klienten interne Kennung	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
17	Klientenentwicklung und Kosten	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
18	Klientenentwicklung	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
19	Klientenentwicklung Kosten	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
20	Klient Gesundheit	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
21	Klient Gesundheitliche Anforderungen	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
22	Klient Behinderung	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
23	Klient Nebentätigkeit	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
24	Klient Beratergespräch	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
25	Klient Vermittlungsvorschlag	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
26	Klient Qualifizierungsmaßnahme	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
27	Klient Kosten Allgemein	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
28	Klient Dienstverhältnis	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
29	Klient Beschäftigungsverhältnis	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
30	Klient Arbeitszeit	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
31	Klient Ein-/Höhergruppierung	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
32	Klient Ernennung	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
33	Klient Beruflicher Werdegang	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
34	Klient Schulausbildung	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle

			SP	SP			SP	DL, SP			SP				SP	RG, MR	
35	Klient Studium	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
36	Klient Promotion/ Habilitation	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
37	Klient Kenntnisse	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
38	Klient Abwesenheitsübersicht	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	alle
39	Klienten ATZ Arbeitszeit	SR, RA	alle o. SP	SR, RA, SP	alle	LR	alle o. SP	SR, RA, DL, SP	alle	LR	alle o. SP	LR	alle	SR, MR	alle o. SP	SR, RA,SP, RG, MR	Alle

Legende

SR	= Lese- und Schreibrechte
LR	= Leserechte
RA	= definierte Reports ausführen
RG	= Reports erstellen
MR	= Managementreport erstellen
SP	= Kennzeichen „Spezial Klient“
Alle	= alle Datensätze der zugeteilten Organisationseinheit

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),

Datensatzprotokollierung – 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

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