

KoPers

Berechtigungs- und Rollenkonzept

Anlage 5

Inhaltsverzeichnis

1	Einleitung.....	1
2	Administrative Zuständigkeiten	2
3	Berechtigungssteuerung	2
3.1	Mandantentrennung.....	3
3.2	Profile	4
3.2.1	Bezeichnungskonventionen	5
3.2.2	Einrichtung und Änderung von Profilen/Musterprofile	5
3.2.2.1	KoPers Passive	6
3.2.2.2	KoPers Aktive.....	6
3.2.2.3	KoPers QuickWin	7
3.2.2.4	KoPers Klientenverwaltung P34	7
3.2.2.5	KoPers Übergreifend Aktiv und Passiv (nicht administrativ).....	8
3.2.3	Administrative Profile	9
3.2.4	Systemprofile, vom Hersteller der Software vorgegeben	11
3.2.5	Profilkombinationen.....	12
3.2.6	Handhabung übergreifender Sachbearbeitung über mehrere Profile.....	12
3.3	Benutzergruppen	12
3.3.1	Bezeichnungskonventionen	13
3.3.1.1	Benutzergruppen Passive.....	13
3.3.1.2	Benutzergruppen Aktive	13
3.3.1.3	Benutzergruppen Quickwin und Bewerberverwaltung.....	15
3.3.1.4	Allgemeine Benutzergruppen	16
3.3.2	Einrichtung und Änderung von Benutzergruppen	16
3.4	Dokumentation von übergreifenden Berechtigungseinstellungen (Profile, Benutzergruppen).....	17
3.5	Benutzer	17
3.5.1	Bezeichnungskonventionen/Allgemeine Regelungen für Benutzer	17
3.5.1.1	Arbeitskennungen	17
3.5.2	Vertretungsregelungen.....	18
3.6	Ausgestaltung und Umsetzung der Satzebenenberechtigung	18
3.6.1	Allgemeine Funktionsweise	18
3.6.2	Datei „Person-Satzebene“	19
3.6.3	Parallelzugriffe auf Daten aus verschiedenen Zuständigkeiten.....	21
4	Sicherheitskonzept KoPers	21
4.1	Kennwortregeln.....	21
4.2	Sperrung von Kennungen nach langer Inaktivität	22
4.3	Einschränkungen der Administratoren	22
4.4	Grundlegende Einstellungen	24

4.5	Standardberechtigungseinstellungen für neue Objekte bei Releasewechseln	24
4.6	Nachweis der Verwaltung von Berechtigungen	26
4.6.1	Dokumentation der Verwaltung von Zugriffsrechten	26
4.6.1.1	Das Admin-Protokoll (Historische Berechtigungen)	26
4.6.2	Vergabe von Zugriffsrechten	28
4.6.2.1	Einrichtung	28
4.6.2.2	Änderung von Zugriffsrechten	28
4.6.2.3	Änderung von Zugriffsrechten bei dezentraler Berechtigungsverwaltung.....	29
5	Kontrolle und Einhaltung des Berechtigungskonzepts	29
6	Spezielle Regelungen für Mitzeichnungsverfahren (elektronische Prozesse).....	29

1 Einleitung

Je nach Arbeitsgebiet sind die Anwender des KoPers-Systems mit hochsensiblen Daten konfrontiert. Zum Schutz dieser personenbezogenen Daten ist die Vergabe von Zugriffsberechtigungen ein wichtiger Bestandteil des gesamten Sicherheitskonzeptes. Das Berechtigungssystem ermöglicht nicht nur die Beschränkung auf die einzelnen Module wie Personalmanagement Aktive FHH, Versorgung oder Zusatzversorgung, sondern auch innerhalb dieser Gebiete eine entsprechende Abgrenzung z. B. auf Datensatzebene.

Durch Berechtigungsprüfungen werden Funktionen und Daten innerhalb des KoPers-Systems geschützt.

Die Erstellung der Berechtigungen für die KoPers-Benutzer obliegt dem Administrator. In der FHH ist die Aufgabe in der Fachlichen Leitstelle ZPD 33 und ZPD 362 Service Line verortet.

Berechtigungen werden in Profilen zusammengefasst und den Benutzern zugeordnet.

Dieses Berechtigungskonzept regelt die Erteilung und Verwaltung von Zugriffsrechten für das Freigabe- und Produktivsystem KoPers. Entsprechende Regelungen für Entwicklungs- und Schulungssysteme des Verfahrens KoPers zu treffen obliegt dem Ermessen der Fachlichen Leitstelle. Entwicklungs- und Testsysteme enthalten keine Echtdateien. Folgende Systeme stehen der FHH zur Verfügung:

Systemumgebung	Mandantenbezeichnung	Berechtigungsverwaltung durch	Echtdateien
Produktion	Mandant 630	Fachliche Leitstelle ZPD	X
Produktion	Mandant 430	Fachliche Leitstelle ZPD	X
Produktion	Mandant 431	Fachliche Leitstelle ZPD	X
Test 1 (Stage 1) Freigabeumgebung	Mandant 330	Fachliche Leitstelle ZPD	
Test 2 (Stage 2)	Mandant 333	Fachliche Leitstelle ZPD	
Test 3 (Stage 3)	Mandant 334	Fachliche Leitstelle ZPD	
Entwicklung	Mandant 030	Fachliche Leitstelle ZPD	
Schulung	Mandant 150	Fachliche Leitstelle ZPD	

Das Berechtigungskonzept verfolgt folgende Zielsetzung:

- Erfolgreiche Vorabkontrolle Datenschutz
- Erfüllung aller kassenrechtlichen Anforderungen
- Reibungsloser, beherrschbarer und störungsfreier Betrieb

Neben der Erfüllung der rechtlichen Anforderungen wird gewährleistet, dass

- die Administrierbarkeit der Profile dauerhaft und praktikabel gegeben ist,
- ein hoher Wiederverwendbarkeitsgrad der einzelnen Profile erreicht wird,
- die Umsetzung und Ablauffähigkeit des elektronischen Mitzeichnungsverfahrens sichergestellt ist und
- eine hinreichende Dokumentation garantiert ist.

Administrative Zuständigkeiten

Die administrativen Zuständigkeiten können grundsätzlich nach zentralen und dezentralen Aufgaben getrennt werden.

Die FHH organisiert ihre Berechtigungsverwaltung für das Personalverfahren **zentral** im Zentrum für Personaldienste. Dies umfasst alle Schritte vom Anlegen der Kennung, deren Ausgestaltung mit Berechtigungen und das Planen und Bereitstellen von Profilen zur vereinfachten Administration.

Weiterer Bestandteil ist die Pflege im Betrieb, z. B. Passwortfreischaltung.

Einzelne Aktivitäten können zur Vereinfachung des Verfahrens dezentralisiert werden. Vorgesehen für eine dezentrale Berechtigungsverwaltung sind gegenwärtig die Aktivitäten

1. Benutzererkennung sperren/entsperren
2. Passwort zurücksetzen
3. Vertretungsregelungen einrichten

Dezentrale Administratoren haben nur Zugriff auf Kennungen der eigenen Behörde bzw. auf Kennungen der von Ihnen verwalteten Kunden.

Die Aufgabe der zentralen Berechtigungsverwaltung wird im ZPD angesiedelt. Hier werden Benutzerkennungen verwaltet, Profile und Benutzergruppen definiert und zugewiesen sowie Berechtigungseinstellungen auf Satzebene eingerichtet und verwaltet.

2 Berechtigungssteuerung

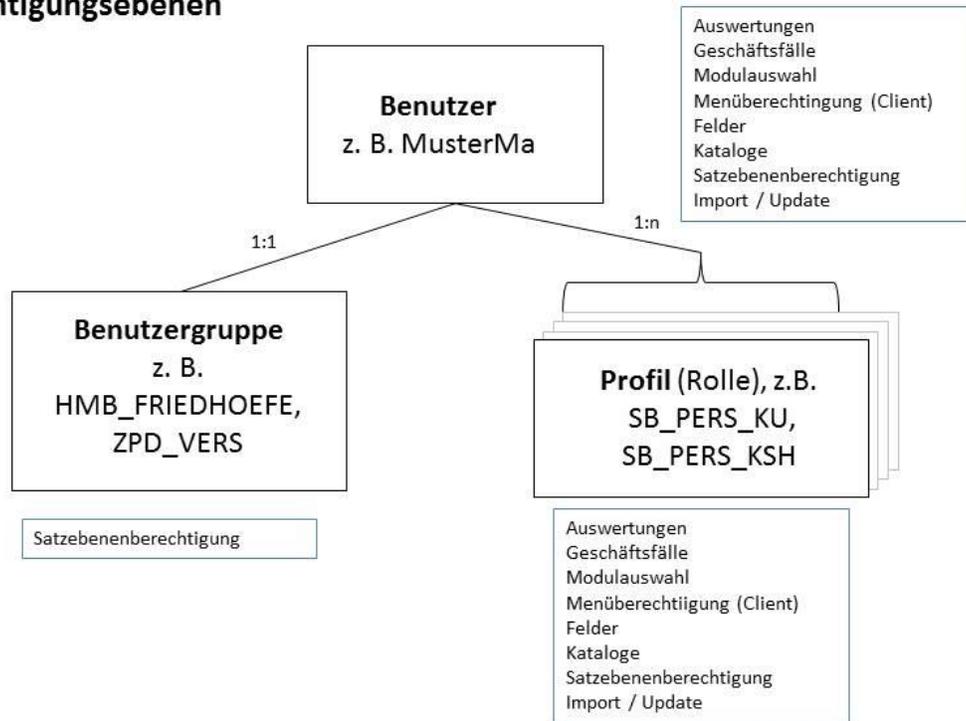
Es wird technisch sichergestellt, dass im eigenen Personalfall keine Änderungen vorgenommen werden können, indem die eigene Personalnummer für den Zugriff gesperrt wird. Ebenso werden die durch einen Benutzer erfassten Daten für die Vier-Augen-Prüfung durch den selben Benutzer gesperrt. Organisatorisch wird ausgeschlossen, dass diese Sicherheitsregelung durch eine zweite Benutzerkennung umgangen werden kann.

Die Berechtigungssteuerung ist in folgende Ebenen unterteilt:

- **Profilspezifische** Zugriffsrechte auf Formate (Geschäftsfälle, Auswertungen, Module, etc.) und Feldinhalte
- Einschränkungen auf inhaltlicher Ebene bei der **Benutzergruppe** mittels Satzebenenberechtigung, z. B. nach organisatorischen oder statusbezogenen Merkmalen.
- Zusätzliche Einschränkungen am **Benutzer** (Buchstabenbereich, etc.) auf Formate und Inhalte (durch Satzebenenberechtigung)

Berechtigungssteuerung KoPers

Berechtigungs Ebenen



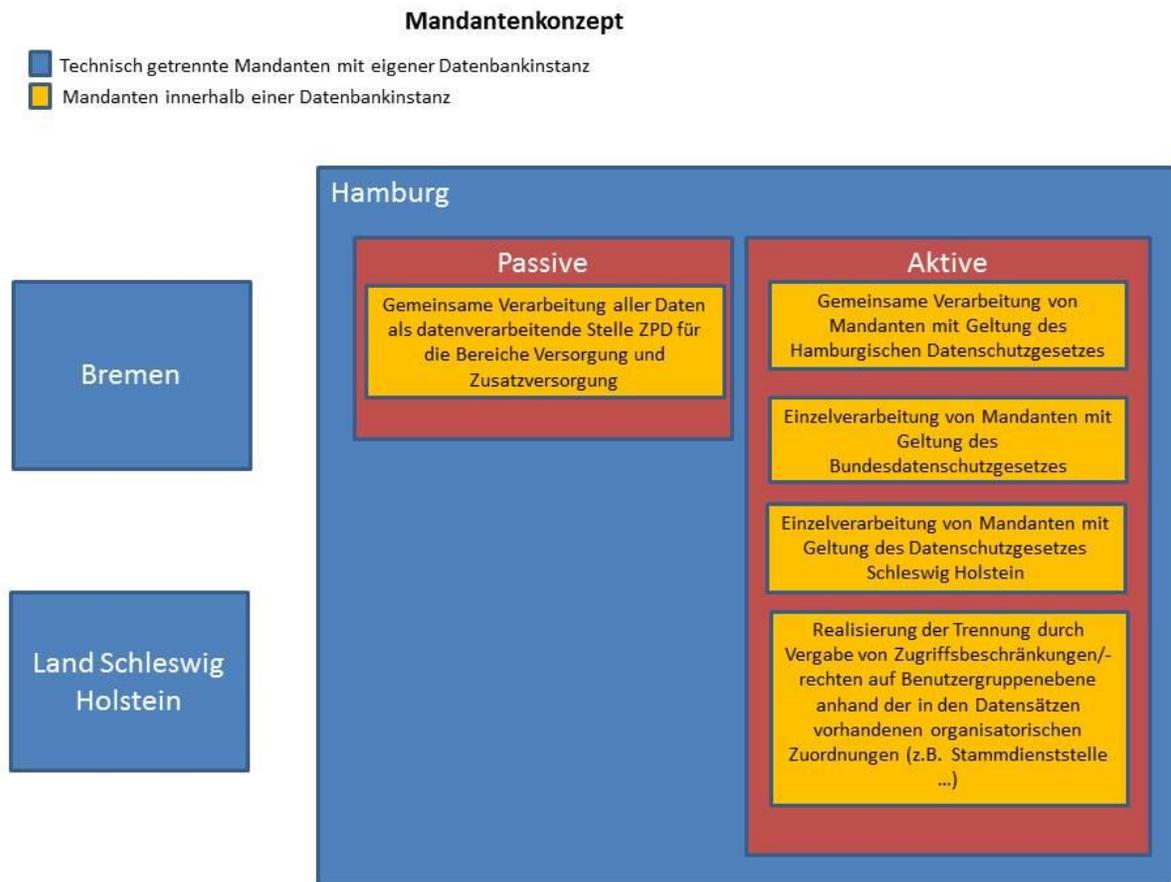
1.

2.1 Mandantentrennung

Das Verfahren kennt auf der Basis der bestehenden Kooperationsverträge drei datenbankinstanzlich getrennte Mandanten Schleswig Holstein, Bremen und die Freie und Hansestadt Hamburg (FHH).

Innerhalb der Datenbankinstanz FHH werden alle vom Dienstleister ZPD zu betreuenden Mandanten logisch getrennt dargestellt. Die Zugehörigkeit der Datensätze zu einem Mandanten wird über eindeutige am Datensatz enthaltene Attribute ermittelt. Für die Aktiven wäre dies die Behördenzuordnung. Zugriffe erfolgen ausschließlich auf der Basis einer Positivprüfung auf die im Rahmen von Profilen und Benutzergruppen definierten Merkmale.

Nachstehende Abbildung verdeutlicht die Mandantenstruktur in KoPers:



Für die Passiven (Ruhegeld und Versorgung) ist das ZPD datenverarbeitende Stelle im Sinne des Datenschutzgesetzes. Insofern ist eine weitere Unterteilung der Daten nicht erforderlich.

Datenverarbeitende Stelle im Aktivenbereich ist jede Behörde, jeder Landesbetrieb sowie alle rechtlich eigenständigen Organisationseinheiten wie Anstalten des öffentlichen Rechts (z. B. Hamburger Friedhöfe, Statistisches Landesamt für Hamburg und Schleswig Holstein). Die Datentrennung erfolgt anhand der an den Datensätzen enthaltenen eindeutigen Merkmalen der Stammmorganisation (Behörden- und Organisationsmerkmale).

2.2 Profile

Auf Profilebene werden die Zugriffsrechte auf Formate (Geschäftsfälle, Auswertungen, Module, archivierte Objekte etc.) definiert. Ein Benutzer muss mit mindestens einem Profil verknüpft sein, um sich anmelden zu können. Die Zuweisung mehrerer Profile ist möglich.

2.2.1 Bezeichnungskonventionen

Bezeichnungskonventionen für Profile sind notwendig, damit anhand der Namen Rückschlüsse auf den Verwendungszweck gezogen werden können. Dadurch wird administrativer Aufwand, mit-hin Doppelarbeit, durch missverständliche Bezeichnungen ausgeschlossen.

Hierbei identifiziert ein Profilname eine eingenommene Rolle, welche die Person mit diesem Profil ausübt. Die Bezeichnungslänge für Profile ist hierbei auf zwölf Zeichen durch technische Restriktionen beschränkt. Es sind keine Leerzeichen möglich.

Die Profilbezeichnung kann aus mehreren Bestandteilen bestehen. Hierbei gilt die Regelung, dass der erste Teil die ausgeübte Tätigkeit generell (Sachbearbeitung = „SB“), der zweite Teil den Arbeitsbereich speziell (Versorgung = „VERSORG“) beschreibt. Für die Sachbearbeitung im Rahmen der Versorgung würde dies nach o.g. Festlegung zu einem Profil „SB_VERSORG“ führen.

Beispiele:

Ausgeübte Tätigkeit generell		Arbeitsbereich speziell		Profilname
Sachbearbeiter	SB_	Verwaltung und Abrechnung Versorgung	VERSORG	SB_VERSORG
Prüfer	PRF_	Prüfung der von der Sachbearbeitung vorgenommenen kassenrelevanten Eingaben	VERS	PRF_VERS
Sachbearbeiter	SB_	Verwaltung und Abrechnung Kunden FHH	PERS_KU	SB_PERS_KU
Sachbearbeiter	SB_	Zentrale Verwaltung von systembezogenen Einstellungen von Arbeitgeber- und Organisationsdaten durch die Fachliche Leitstelle	AG_FL	SB_AG_FL

2.2.2 Einrichtung und Änderung von Profilen/Musterprofile

Profile berücksichtigen ausschließlich die fachliche Ausrichtung des Verfahrens. Notwendige Zugriffsrechte außerhalb der Anwendung mit rein technischem Hintergrund, z. B. Zugriffsrechte auf Server oder Datenbanken, liegen im Zuständigkeitsbereich der Technischen Leitstelle Dataport und werden im vorliegenden Konzept nicht beschrieben.

Über die Einrichtung und Ausgestaltung von Profilen entscheidet die Fachliche Leitstelle im ZPD HR Systemhaus auf der Basis fachlicher Erfordernisse. Sie trifft auch die Entscheidung, auf welchen Systemen (Entwicklung, Freigabe, Produktion, Schulung) die Profile zur Verfügung gestellt werden.

Die Umsetzung erfolgt grundsätzlich in der KoPers-Entwicklungsumgebung. Von dort werden die Einstellungen elektronisch in die Testumgebung und nach Freigabe durch den Testbetrieb nach Produktion verteilt.

Nachstehend erfolgt eine Auflistung der in der Produktionsumgebung KoPers verwendeten Profile.

2.2.2.1 KoPers Passive

Musterprofil für	Abkürzung	Erläuterung	Adressaten
Sachbearbeitung Personalwirtschaft Versorgung	SB_VERSORG	Standardprofil der Versorgungssachbearbeitung	ZPD 42
Prüfung Versorgung (Vier-Augen-Prinzip)	PRF_VERS	Prüferprofil Versorgung	ZPD 42
Prüfung Versorgung durch Festsetzer (Vier-Augen-Prinzip)	PRF_VERSdFS	Prüferprofil Versorgung	ZPD 42
Sachbearbeitung Zusatzversorgung	SB_ZUVERS	Standardprofil der Zusatzversorgungssachbearbeitung	ZPD 43
Prüfung Zusatzversorgung (Vier-Augen-Prinzip)	PRF_ZUVERS1	Prüferprofil Zusatzversorgung, Trennung nach Buchstabenraten	ZPD 43
Prüfung Zusatzversorgung Festsetzer (Vier-Augen-Prinzip)	PRF_ZUVERSFS	Prüferprofil Zusatzversorgung	ZPD 43
Prüfer Zusatzversorgung Teamleiter	PRF_ZUVERSTL	Prüferprofil Zusatzversorgung für Teamleitung	ZPD 43
Geschäftszimmer Passive	GZ_PASSIVE	Lesender Zugriff auf einzelne Geschäftsfälle der Versorgung und Zusatzversorgung	Gemeinsames Geschäftszimmer ZPD 42 und ZPD 43

2.2.2.2 KoPers Aktive

Musterprofil für	Abkürzung	Erläuterung	Adressaten
Sachbearbeitung Personalwirtschaft Aktive	SB_PERSONAL	Standardprofil für Personalsachbearbeiter Aktive	Personalsachbearbeiter Kernbereich FHH
Sachbearbeitung Personalwirtschaft Aktive	SB_PERS_LES	LESE-Profil Personalsachbearbeiter Aktive (Azubi etc)	Angehende Personalsachbearbeiter Kernbereich FHH
Sachbearbeitung Personalwirtschaft Aktive	SB_PERS_mLOE	Sonderprofil für Personalsachbearbeitung mit Löschberechtigung in ausgewählten Geschäftsfällen gemäß Löschkonzept	Personalsachbearbeiter
Prüfung Eingaben durch Sachbearbeiter (4-Augen-Prüfung)	PRF_PERSONAL	Prüferprofil für kassenrechtliche 4-Augen-Prüfung	Personalsachbearbeiter Kernbereich FHH

Prüfung Eingaben durch Sachbearbeiter (4-Augen-Prüfung)	PRF_PERS_KU	Prüferprofil für kassenrechtliche 4-Augen-Prüfung	Personalsachbearbeiter Kunden FHH
Sachbearbeitung Dienstposten, Arbeitsplätze und Stellen	SB_ORGA	Standardprofil für Organisations-sachbearbeiter Aktive	Organisations-sachbearbeiter
Sachbearbeitung Stellen	SB_STELLEN	Standardprofil für Organisations-sachbearbeiter Aktive ohne Dienstposten und Arbeitsplätze	Organisations-sachbearbeiter
Sachbearbeitung Dienstposten und Arbeitsplätze	SB_DPAP	Standardprofil für Organisations-sachbearbeiter Aktive ohne Stellenbewirtschaftung	Organisations-sachbearbeiter externe Kunden
Sachbearbeitung Familienkasse Kunden	SB_KIGELD_KU	Standardprofil für Familienkassensachbearbeitung beim Kunden	Familienkasse Hamburger Friedhöfe
Prüfungsprofil für Familienkasse Kunden	PRF_KIGE_KU	Standardprüferrolle für Familienkassensachbearbeitung beim Kunden	Familienkasse Hamburger Friedhöfe

2.2.2.3 KoPers QuickWin

Musterprofil für	Abkürzung	Erläuterung	Adressaten
Sachbearbeitung Bewerbungsmanagement	SB_BEW	Sachbearbeitung Bewerbungsmanagement	An QuickWin teilnehmende Behörden
Fachliche Leitstelle Bewerbungsmanagement	FL_BEWMGMT	Fachliche Leitstelle Bewerbungsmanagement	Fachliche Leitstelle QuickWin und Service Line
Vorgesetzter Bewerbungsverwaltung	VORG_BEW	Vorgesetzter Bewerbungsverwaltung	An QuickWin teilnehmende Behörden

2.2.2.4 KoPers Klientenverwaltung P34

Musterprofil für	Abkürzung	Erläuterung
Teamleitung Klientenverwaltung P34	SB_KL_P34_TL	Referats- und Teamleitung P31 und P34: Lesender Zugriff auf alle Geschäftsfälle der Klientenverwaltung. Zugriff auf definierte Auswertungen.
Fachliche Leitstelle P34	FL_P34	Zugriff auf alle Geschäftsfälle und Auswertungen der Klientenverwaltung. Berechtigung für das Erstellen von Auswertungen.
Sachbearbeitung Ausschreibung P34	SB_AUSS_P34	Zugriff beschränkt auf Geschäftsfälle und Auswertungen des Bereichs „Stellenausschreibung“ der Klientenverwaltung.
Sachbearbeitung Beratung P31	SB_KL_P34S	Zugriff auf alle Geschäftsfälle der Klientenverwaltung. Über ein Kennzeichen kann der Zugriff auf einzelne Klientensätze nur für das Referat P31 gesteuert werden. Zugriff auf definierte Auswertungen.

Sachbearbeitung Beratung P34	SB_KL_P34	Zugriff auf alle Geschäftsfälle der Klientenverwaltung exklusive gekennzeichnete P31-Klientensätze. Zugriff auf definierte Auswertungen.
Sachbearbeitung Controlling P34	SB_CNT_P34	Zugriff auf alle Geschäftsfälle und Auswertungen der Klientenverwaltung. Zusätzlich Zugriff auf Auswertungen für den Bereich Controlling.
Referatsleitung	REF_LTG_P34	Zugriff auf alle Geschäftsfälle und Auswertungen der Klientenverwaltung. Zusätzlich Zugriff auf Auswertungen für den Bereich Leitung.

2.2.2.5 KoPers Übergreifend Aktiv und Passiv (nicht administrativ)

Musterprofil für	Abkürzung	Erläuterung	Adressaten
Sachbearbeitung Grundlagen	SB_GRUNDL	Übergreifendes Profil für die fachliche Grundlagensachbearbeitung (nur lesen)	Fachliche Leitstelle ZPD 3
Sachbearbeitung Kindergeld	SB_KIGELD	Standardprofil für die Familienkasse	ZPD 46
Sachbearbeitung Pfändung	SB_PFAEND	Standardprofil für die Pfändungssachbearbeitung	ZPD 412
Externe Prüfung (Beschäftigung)	Profil RH	Profil für Innenrevisionistische Tätigkeiten wie Rechnungshof oder Innenrevision mit lesendem Zugriff auf alle Personaldaten und Systemeinstellungen	Rechnungshof, HmbBfDI, Innenrevision
Fachliche Leitstelle Fehlerklärung	FL_FEHLERKL	Standardprofil der Fachlichen Leitstelle für Aufklärung von Fehlersituationen und die Beratung der Personalstellen und Fachbereiche im ZPD im Rahmen der Anwenderunterstützung (Nur lesender Zugriff)	ZPD 36, ZPD 32, ZPD 35, ZPD 33
Fachliche Leitstelle Löschanforderungen in Sondersituationen	FL_LOESCH	Sonderprofil der Fachlichen Leitstelle für das Löschen von Datensätzen gemäß Löschanforderungen	ZPD 36
Prüfung Kindergeld (Vier-Augen-Prinzip)	PRF_KIGE1	Prüferprofile der Familienkasse, Trennung nach Buchstabenraten	ZPD 46
Prüfung Pfändung (Vier-Augen-Prinzip)	PRF_PFAEND	Prüferprofil für die Pfändungssachbearbeitung	ZPD 412
Qualitätssicherung Haushalt	QS_HAUSH	Lesenden Zugriff für ZPD 44 für die QS zur Freigabe der Abrechnung sowie der Aufklärung von Fehlersituationen und die Beratung der Personalstellen und Fachbereiche im ZPD	ZPD 47
Fachaufsicht Querbewirtschaftung	AUFS_HAUSH	Fachaufsicht durch den BfH-AOB97 mit lesendem Zugriff auf alle Personaldaten	ZPD 4
Fachliche Leitstelle Beihilfe	LES_BEIHILFE	Lesende Zugriffe für Qualitätskontrollen der Schnittstelle KoPers-PermisB	ZPD 51

Fachliche Leitstelle Beihilfe	LES_BEIH_KOR	Ändernder Zugriff für Testmandanten -nicht für Produktion-	ZPD 51
Geschäftszimmer Familienkasse	GZ_KIGELD	Zugriff für Geschäftszimmertätigkeit der Familienkasse auf einzelne Geschäftsfälle	ZPD 46 Geschäftszimmer
Pflege von Arbeitgeberdaten in Produktion	SB_AG_FL	Pflege von Arbeitgeberinformationen im Verfahren	ZPD 3
Prüfung Arbeitgeberdaten (Vier-Augen-Prinzip)	PRF_AG_FL	Prüfung geänderter Arbeitgeberdaten im Rahmen von Mitzeichnungsverfahren	ZPD 44, ZPD 3
Unterstützung der Arbeitgeberfunktionen im Bereich Sozialversicherung und Steuern	SB_AG_FU_LES	Profil für die Unterstützung des Meldewesens Sozialversicherung und Steuern. Nur lesende Zugriffe auf benötigte Geschäftsfälle der Aktiven und Passiven.	ZPD 44
Unterstützung Poststelle ZPD bei der Postverteilung	LES_POSTST	Lesender Zugriff auf die Geschäftsfälle Sachbearbeiterzuordnung der einzelnen Fachgebiete	ZPD 13
Pflege von Sachbearbeiterzuordnungen	FL_SACHB_ZO	Schreibender Zugriff auf die Geschäftsfälle für Sachbearbeiterzuordnungen	ZPD 36
Sachbearbeitereinsicht in Grundtabellen	SB_AGDAT_LES	Lesender Zugriff auf Systemtabellen wie Krankenkassendaten, Bankleitzahlen, Gemeindegennzahlen und Postleitzahlen	Personalsachbearbeiter
Sachbearbeitung Zentrale Dienstunfallfürsorge im ZPD	SB_ZEUS	Standardprofil für die Bearbeitung im Rahmen der Dienstunfallfürsorge	ZPD 411
Prüfung Zentrale Dienstunfallfürsorge (Vier-Augen-Prinzip)	PRF_ZEUS	Prüferprofilprofil für die Bearbeitung im Rahmen der Dienstunfallfürsorge	ZPD 411
Sachbearbeitung Arbeitgeberfunktion für Lohnsteueranmeldungen	SB_AG_LSTA	Standardprofil für die Bearbeitung von Lohnsteueranmeldungen als Arbeitgeberfunktion	ZPD 47
Prüfung Eingaben Lohnsteueranmeldung (Vier-Augen-Prinzip)	PRF_AG_LSTA	Prüferprofilprofil für die Bearbeitung von Lohnsteueranmeldungen als Arbeitgeberfunktion	ZPD 47

2.2.3 Administrative Profile

Musterprofil für	Abkürzung	Erläuterung	Adressaten
Administration Auswertungen und Kataloge	ADM_AUSWERT	Dieses Profil wird in Produktion nicht vergeben. Erstellung und Pflege von Auswertungen und Katalogen auf Entwicklung	Fachliche Leitstelle ZPD 3

Administration Benutzer	ADM_BENUTZER	Dieses Profil wird in Produktion nicht vergeben. Benutzerverwaltung auf Entwicklung, Freigabe und Schulung	Fachliche Leitstelle ZPD 3
Administration Kataloge	ADM_KATALOGE	Dieses Profil wird in Produktion nicht vergeben. Erstellung und Pflege von Katalogen auf Entwicklung	Fachliche Leitstelle ZPD 3
Administration Mitzeichnungsverfahren	ADM_MZV	Dieses Profil wird in Produktion nicht vergeben. Einrichtung und Pflege von Mitzeichnungsverfahren auf Entwicklung	Fachliche Leitstelle ZPD 3
Administration Protokoll	ADM_PROTOKOL	Profil für Einsichtnahme in Protokolldateien	BfH-AOB97, Einzelpersonen bei ZPD 3
Benutzerverwaltung	ADM_BEN_PROD	Benutzerverwaltung auf Produktion mit dem eingeschränkten Recht zur Benutzerverwaltung. Keine Berechtigung zur Anpassung von Profilen oder Benutzergruppen.	ZPD 36, s. a. Ziffer 3.3
Dezentrale Benutzeradministration	ADM_BEN_DEZ	Eingeschränkte Benutzerverwaltung für Administratoren in den Personalstellen. Möglich ist das Sperren/Entsperren von Kennungen, Passwortänderungen sowie die Einrichtung von Vertreterregelungen.	Anwendungsberater
Administrationsprofil für Dataport	ADM_DP_PROD	Profil für DP-Mitarbeiter in Produktion, um nach Einspielen von Systemaktualisierungen die Anmeldung und die Versionsnummer kontrollieren zu können. Einspielen von Krankenkassendaten der ITSG.	Dataport KoPers Technische Leitstelle
Administrationsprofil für Systemadministratoren mit übergreifenden Zuständigkeiten	ADM_SYSTEM	Umfangreiches Profil zur Administration, wenn die eingeschränkten Administrationsprofile nicht ausreichen. -nicht für Produktion-	Administratoren auf Entwicklungstest und Schulungsumgebungen
Entwickler/Test	Anwender_FHH	Profil zum Testen von Funktionalitäten, insbesondere Fehleranalyse bei Auswertungen -nicht für Produktion-	ZPD 34

2.2.4 Systemprofile, vom Hersteller der Software vorgegeben

Einige Profile sind vom Hersteller P & I vorgegeben und für bestimmte Systemfunktionalitäten Voraussetzung. Von den nachstehend aufgeführten Profilen ist nur der Master PUI_SYSTEM für den Passiven-Teil des Verfahrens KoPers relevant. Die anderen Profile sind vorhanden, werden aber wegen fehlender fachlicher Notwendigkeit nicht vergeben.

Musterprofil für	Abkürzung	Erläuterung	Adressaten
Master	PUI_SYSTEM	Hauptadministrationsprofil ohne Einschränkungen. Dieses Profil wird in Produktion nicht vergeben , um eine Akkumulation von administrativen Zugriffsrechten auf eine Person zu vermeiden. Es wird nur für Notfalleingriffe nach einem geregelten Verfahren zur Verfügung gestellt. Die Vergabe und Verwendung wird schriftlich dokumentiert.	Vergabe im Rahmen von Notfallzugriffen an autorisierte Personen, s.a. Ziffer 3.3 Regelung in der DA-KoPers, Anlage 1, Nr.5
Anwender	Anwender	Standardprofil der P&I zur Verwendung für die Teilnahme von Beschäftigten an ESS. Wird zur Zeit nur im Test als Generalanwender für alle Module verwendet. Eine Nutzung ist nicht vorgesehen.	
Mitarbeiter	Mitarbeiter	Es liegt keine Beschreibung vor. Eine Nutzung ist nicht vorgesehen.	
Vorgesetzter	Vorgesetzter	Profil für Vorgesetzte zur Teilnahme an Mitzeichnungsverfahren Eine Nutzung ist nicht vorgesehen.	
Shared Service Center	SSC	Vorgegebenes Profil für Verwendung durch Beschäftigte in Shared Service Centern. Es liegt keine nähere Beschreibung vor. Eine Nutzung ist nicht vorgesehen.	

Employee Self Service	ESS	Vorgegebenes Profil für die Funktionalitäten des ESS-Moduls. Es liegt keine nähere Beschreibung vor. Eine Nutzung ist nicht vorgesehen.	
-----------------------	-----	---	--

2.2.5 Profilkombinationen

Benutzern können gleichzeitig mehrere Profile zugeordnet werden. Technisch bedingte Abhängigkeiten i. S. von ‚Hat jemand Profil A, so ist die Vergabe Profil B ausgeschlossen‘ existieren nicht. Berechtigungsadministratoren haben bei der Vergabe von Profilen darauf zu achten, dass die Kombinationen nicht zu ungewollten Akkumulationen von Berechtigungen führen.

Kombinationen wie SB_VERSORG (Sachbearbeitung Versorgung) i. V. mit PRF_VERS (Prüfung Versorgung) oder SB_PERS_KU mit PRF_PERSONAL sind gewollt und unschädlich. Die eingerichteten Mitzeichnungsverfahren stellen technisch durch die definierten Einstellungen sicher, dass Benutzer Ihre eigenen Eingaben nicht selbst freigeben können. Es findet hier eine Prüfung gegen die auslösende Benutzererkennung statt.

Für die Kontrolle, ob ungewollte Kombinationen vergeben wurden, steht die Auswertung ‚BER Profile/Benutzer‘ zur Verfügung, s.a. Kapitel 3.6.1.1.

2.2.6 Handhabung übergreifender Sachbearbeitung über mehrere Profile

Soll vom Nutzungsbereich eines Profils in den Nutzungsbereich eines anderen Profils gewechselt werden (Bsp.: Sachbearbeitung Personal nach Sachbearbeitung Organisation) ist dies nur über die manuelle Auswahl des neuen Profils über die Benutzeroberfläche möglich, da die einzelnen Profile nicht kumulativ wirken.

Profile wirken immer separierend, niemals additiv, d. h. es gelten immer nur die Zugriffsrechte des Profils, mit dem die Person zu einem Zeitpunkt angemeldet ist. Ein Profilwechsel entspricht technisch einer Neuansmeldung am System. Entsprechend werden bei einem Wechsel die gerade bestehenden Rechte gelöscht und die Zugriffsrechte des neuen Profils geladen.

2.3 Benutzergruppen

Eine Benutzergruppe ist eine weitere Möglichkeit, Benutzerrechte zu strukturieren. Jedem Benutzer kann genau eine Benutzergruppe zugeordnet werden. Der Zugriff auf Daten z.B nach Mandant oder basierend auf der Organisationsstruktur wird dabei mit Hilfe der Satzebenenberechtigungen (siehe unten unter 2.6) für die Benutzergruppe definiert.

Technische Einschränkungen der Benutzergruppen

- Ein Benutzer kann zu einem Zeitpunkt nur einer Benutzergruppe zugeordnet sein. Ist er keiner Benutzergruppe zugeordnet, so hat er grundsätzlich zunächst Zugriff auf den gesamten Mandanten.

- 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 realisierbar.

2.3.1 Bezeichnungskonventionen

Zu wählen sind möglichst sprechende Bezeichnungen für die Benennung von Benutzergruppen. Darin sollte der fachliche Zusammenhang mindestens angedeutet werden, z. B. die Organisation wie die Familienkasse im ZPD.

Folgende Benutzergruppen sind vorgesehen:

2.3.1.1 Benutzergruppen Passive

Benutzergruppe	Abkürzung	Erläuterung	Adressaten
ZPD Versorgung	ZPD_VERS	Zusammenfassung aller Benutzer der Versorgung in einer Benutzergruppe	Personen mit der Funktion Sachbearbeitung und/oder Prüfung in der Versorgung
ZPD Zusatzversorgung	ZPD_ZUVERS	Zusammenfassung aller Benutzer der Zusatzversorgung in einer Benutzergruppe	Personen mit der Funktion Sachbearbeitung und/oder Prüfung in der Zusatzversorgung

2.3.1.2 Benutzergruppen Aktive

Benutzergruppe	Abkürzung	Erläuterung	Adressaten
Hamburger Friedhöfe	HMB_FRIEDHOEFE	Zusammenfassung aller Benutzer der Hamburger Friedhöfe in einer Benutzergruppe	Personalabteilung
Landesamt für Statistik für Hamburg und Schleswig Holstein	STATISTIKAMT_NORD	Zusammenfassung aller Benutzer des Statistikamt Nords in einer Benutzergruppe	Personalabteilung
ZPD Auftragssachbearbeitung	ZPD_AUFTRAGSSACHBEARBEITUNG	Zusammenfassung <i>verschiedener</i> Firmen, bei denen das ZPD die Sachbearbeitung übernimmt	Personalabteilung
Rechnungshof	RECHNUNGSHOF	Zusammenfassung aller Benutzer des Rechnungshofes in einer Benutzergruppe	Personalabteilung und Organisationsmanagement
Personalamt	PERSONALAMT	Zusammenfassung aller Benutzer der Personalabteilung des Personalamts in einer Benutzergruppe mit Kunden ohne Senatskanzlei	Personalabteilung
Personalamt	PERSONALAMT_ORG	Zusammenfassung aller Benutzer des Personalamts in einer Benutzergruppe ohne Kundenzugriffe	Organisationsabteilung

Personalamt	PERSONALAMT_SO	Zusammenfassung aller Benutzer der Personalabteilung des Personalamts und Kunden in einer Benutzergruppe einschließlich Senatskanzlei	Personalabteilung
Hamburgischer Datenschutzbeauftragter	HMBBFDI_ORG	Zusammenfassung aller Benutzer der Organisationsabteilung des HmbBfDI in einer Benutzergruppe	Organisationsabteilung
Senatskanzlei und Senatsämter	SENATSKANZLEI_ORG	Zusammenfassung aller Benutzer der Organisationsabteilung der Senatskanzlei und Senatsämter in einer Benutzergruppe	Organisationsabteilung
Behörde für Wissenschaft, Forschung und Gleichstellung	BWFG_ORG	Zusammenfassung aller Benutzer Organisationsabteilung der BWFG in einer Benutzergruppe	Organisationsabteilung
Behörde für Kultur und Medien	BKM_ORG	Zusammenfassung aller Benutzer der Organisationsabteilung der BKM in einer Benutzergruppe	Organisationsabteilung
Behörde für Arbeit, Soziales, Familie und Integration	BASFI	Zusammenfassung aller Benutzer Personalabteilung der BASFI in einer Benutzergruppe	Personalabteilung
Behörde für Arbeit, Soziales, Familie und Integration	BASFI_ORG	Zusammenfassung aller Benutzer der Organisationsabteilung der BASFI in einer Benutzergruppe	Organisationsabteilung
Team Arbeit Hamburg	BASFI_TAH_ORG	Zusammenfassung aller Benutzer der Organisationsabteilung der BASFI t.a.h. in einer Benutzergruppe	Organisationsabteilung
Behörde für Stadtentwicklung und Wohnen	BSW_ORG	Zusammenfassung aller Benutzer der Organisationsabteilung der BSW in einer Benutzergruppe	Organisationsabteilung
Behörde für Umwelt und Energie	BUE	Zusammenfassung aller Benutzer der Personalabteilung der BUE in einer Benutzergruppe	Personalabteilung
Behörde für Umwelt und Energie	BUE_ORG	Zusammenfassung aller Benutzer der Organisationsabteilung der BUE in einer Benutzergruppe	Organisationsabteilung
Behörde für Wirtschaft, Verkehr und Innovation	BWVI	Zusammenfassung aller Benutzer der BWVI in einer Benutzergruppe	Personalabteilung und Organisationsmanagement
Finanzbehörde	FINANZBEHOERDE	Zusammenfassung aller Benutzer der Finanzbehörde in einer Benutzergruppe	Personalabteilung und Organisationsmanagement

Finanzbehörde Steuer- verwaltung	FINANZBEHOERDE_STV	Zusammenfassung aller Benutzer der Steuerverwal- tung in einer Benutzer- gruppe	Personalabteilung und Organisati- onsmanagement
Hamburgische Öffentli- che Bücherhallen	BUECHERHALLEN	Zusammenfassung aller Benutzer der HÖB in einer Benutzergruppe	Personalabteilung und Organisati- onsmanagement

2.3.1.3 Benutzergruppen Quickwin und Bewerberverwaltung

Benutzergruppe	Abkürzung	Erläuterung
QuickWin Personal- amt	QW_01_Personalamt	Zusammenfassung aller QW- Benutzer aus der Personalabtei- lung des Personalamts
QuickWin ZPD	QW_02_Zentrum für Personaldienste	Zusammenfassung aller QW- Benutzer aus dem ZPD
QuickWin Behörde für Justiz und Gleich- stellung	QW_03_Behörde für Justiz und Gleichstell	Zusammenfassung aller QW- Benutzer aus der BJJ
QuickWin Polizei	QW_04_POLIZEI.PersAngel.	Zusammenfassung aller QW- Benutzer der Polizei Personalab- teilung
QuickWin Polizei	QW_04a_POLIZEI.PersAngel._ZP52	Zusammenfassung aller QW- Benutzer der Polizei ZP52
QuickWin Polizei	QW_04b_POLIZEI.PersAngel._ZP531	Zusammenfassung aller QW- Benutzer der Polizei ZP531
QuickWin Polizei	QW_04c_POLIZEI.PersAngel._ZP532	Zusammenfassung aller QW- Benutzer der Polizei ZP532
QuickWin Polizei	QW_05_POLIZEI.Perseinstellungen	Zusammenfassung aller QW- Benutzer der Polizei
QuickWin BSB	QW_06a_BehSchule_AmtfVW_V432	Zusammenfassung aller QW- Benutzer der BSB V432
QuickWin BSB	QW_06b_BehSchule_AmtfVW_V439	Zusammenfassung aller QW- Benutzer der BSB V439
QuickWin BSB	QW_06c_BehSchule_LIfLuS	Zusammenfassung aller QW- Benutzer der BSB
QuickWin BSB	QW_06d_BehSchule_LHV	Zusammenfassung aller QW- Benutzer der BSB
QuickWin BGV	QW_07_BGV_Personal und Ressourcenpla- nung	Zusammenfassung aller QW- Benutzer der BGV
QuickWin E/BA	QW_08_Bezirksamt Eimsbüttel	Zusammenfassung aller QW- Benutzer des Bezirksamtes Eimsbüttel
QuickWin M/BA	QW_09_Bezirksamt Hamburg Mitte	Zusammenfassung aller QW- Benutzer des Bezirksamtes Hamburg Mitte
QuickWin H/BA	QW_10_Bezirksamt Harburg	Zusammenfassung aller QW- Benutzer des Bezirksamtes Har- burg
QuickWin W/BA	QW_13_Bezirksamt Wandsbek	Zusammenfassung aller QW- Benutzer des Bezirksamtes Wandsbek

QuickWin Finanzbehörde	QW_11a_Finanzbehörde.SV_550	Zusammenfassung aller QW-Benutzer aus dem ZPD
QuickWin Finanzbehörde	QW_11b_Finanzbehörde.SV_553	Zusammenfassung aller QW-Benutzer der Finanzbehörde SV 553
QuickWin Finanzbehörde	QW_12_Finanzbehörde.Organisation und ZD	Zusammenfassung aller QW-Benutzer der Finanzbehörde Organisation und Zentrale Dienste

2.3.1.4 Allgemeine Benutzergruppen

Benutzergruppe	Abkürzung	Erläuterung	Adressaten
Ohne Gruppenzuordnung	Ohne Gruppenzuordnung	Standard-Benutzergruppe für Administratoren, insbesondere Berechtigungsadministration	Insbesondere Berechtigungsadministratoren
Anwender	Anwender	Standardbenutzergruppe der P&I	In Produktion sollte hier niemand zugeordnet sein
P&I-Mitarbeiter	P&I-Mitarbeiter	Zusammenfassung aller Mitarbeiterkennungen der P&I zum Zwecke der Systemkonsolidierung Passive und Aktive	P&I-Mitarbeiter
ZPD Arbeitgeberfunktion	ZPD_AGFU	ZPD 47	Personen im ZPD mit der Aufgabe Arbeitgeberfunktionen SV und steuerrechtlicher Art wahrzunehmen (ZPD 47)
ZPD Fachliche Leitstelle	ZPD_FL	ZPD 3	Personen der Fachlichen Leitstelle im ZPD (ZPD 3)
ZPD Qualitätssicherung Haushalt Fachaufsicht Querbewirtschaftung	ZPD_QUERBEW	ZPD 4 und ZPD 44	Personen mit der Aufgabe, die kassenrechtliche Ordnung des Verfahrens zu gewährleisten (ZPD 4 und ZPD 44)
ZPD Familienkasse	ZPD_FK	Zusammenfassung aller Benutzer der Familienkasse in einer Benutzergruppe	Personen mit der Funktion Sachbearbeitung und/oder Prüfung in der Familienkasse
ZPD Pfändung	ZPD_PF	Zusammenfassung aller Benutzer der Pfändung in einer Benutzergruppe	Personen mit der Funktion Sachbearbeitung und/oder Prüfung in der Pfändung
ZPD Zentrale Unfallfürsorge Service	ZPD_ZEUS	Zusammenfassung aller Benutzer der Zentralen Unfallfürsorgesachbearbeitung	ZPD 41

2.3.2 Einrichtung und Änderung von Benutzergruppen

Über die Einrichtung und Ausgestaltung von Benutzergruppen entscheidet die Fachliche Leitstelle im ZPD. Sie trifft auch die Entscheidung, auf welchen Systemen (Entwicklung, Test (Stage), Produktion, Schulung) die Benutzergruppen zur Verfügung gestellt werden.

Die Umsetzung erfolgt grundsätzlich in der KoPers-Entwicklungsumgebung. Von dort werden die Einstellungen elektronisch in die Testumgebung und nach Freigabe durch den Testbetrieb nach Produktion transportiert.

2.4 Dokumentation von übergreifenden Berechtigungseinstellungen (Profile, Benutzergruppen)

Berechtigungseinstellungen werden über ein Auftragsmanagementsystem in-Step von den zuständigen Personen beauftragt und im Rahmen eines Prozesses umgesetzt, qualitätsgesichert und für den Einsatz in Produktion freigegeben. Jede Änderung ist über entsprechende Aufträge dokumentiert.

Die Umsetzung erfolgt grundsätzlich in der KoPers-Entwicklungsumgebung. Von dort werden die Einstellungen elektronisch in die Testumgebung und nach Freigabe durch den Testbetrieb nach Produktion transportiert.

Daneben stehen Auswertungen über die vorhandenen Einstellungen zur Verfügung („BER Profileauswahl Formateauswahl“) sowie für die Umsetzungstätigkeiten das Protokoll „Historische Berechtigungen“.

2.5 Benutzer

2.5.1 Bezeichnungskonventionen/Allgemeine Regelungen für Benutzer

Benutzer des HR-IT-Systems ist jede Person, die sich am System anmelden darf. Hierzu wird jeder Person eine eindeutige, nach einer einheitlichen Nomenklatur aufgebaute Benutzerkennung zugeteilt.

Aus der Benutzerkennung muss zweifelsfrei erkennbar sein, um welche natürliche Person es sich handelt. Eine organisationsbezogene Benutzerkennung ist datenschutzrechtlich ein Pseudonym, das als alleiniges Identifikationsmerkmal nicht ausreicht, da dadurch im Verfahren kein Bezug zur natürlichen Person hergestellt werden kann. Eine zusätzliche papiermäßige Dokumentation, welche Person in welchem Zeitraum mit welcher Kennung gearbeitet hat, reicht ebenfalls nicht aus, die Dokumentation muss revisionssicher innerhalb des Verfahrens erfolgen.

Benutzerkennungen müssen daher personenbezogen systemweit einheitlich aufgebaut werden und dürfen maximal eine Länge von zwölf Zeichen erreichen. Benutzerkennungen werden in Kleinbuchstaben erstellt.

Es ist technisch nicht auszuschließen, dass einer Person mehrere Benutzerkennung zugeordnet werden können. Zur Vermeidung, dass einer Person versehentlich mehrere Kennungen eingerichtet werden, hat die Fachliche Leitstelle vor Einrichtung einer neuen Kennung diesen Sachverhalt zu prüfen. Hierfür steht die Auswertung BER Profile/Benutzer zur Verfügung.

2.5.1.1 Arbeitskennungen

Für die tägliche Arbeit im System und die Teilnahme an Mitzeichnungsverfahren erhalten die Teilnehmer Arbeitskennungen mit acht Buchstaben mit dem Aufbau sechs Buchstaben Nachname plus zwei Buchstaben Vorname, Beispiel: Aus Jens Mustermann wird „musterje“.

Bei kürzeren Nachnamen wird ggf. aus den Vornamen aufgestockt.

Beispiel: Aus Anton Berg wird "berganto".

Reichen beide Namen nicht aus, kann die Kennung auch aus weniger Buchstaben bestehen.

Beispiel: Aus Olaf Ton wird "tonolaf".

Bei Namensgleichheit wird an neunter Stelle hochnummeriert.

Durch den einheitlichen Aufbau wird vermieden, dass einer Person versehentlich mehrere Kennungen zugeteilt werden.

2.5.2 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.

Die betroffenen Fachbereiche Versorgung, Zusatzversorgung, Pfändung und Familienkasse haben sich innerhalb Ihrer Fachbereiche für eine permanente Vertretungsregelung ausgesprochen, z. B. haben die Beschäftigten der Versorgung Zugriff auf alle Personalfälle der Versorgung.

Gleichwohl wird die Einhaltung des 4-Augen-Prinzips sichergestellt. Durch die technischen Einstellungen in den Mitzeichnungsverfahren ist ausgeschlossen, dass jemand mit der eigenen Benutzerkennung die eigenen Eingaben prüfen und freigeben kann (auch nicht als Vertreter).

Die Personalverwaltungen der Aktiven verwenden ebenfalls die permanente Vertretung in den Personalstellen.

2.6 Ausgestaltung und Umsetzung der Satzebenenberechtigung

2.6.1 Allgemeine Funktionsweise

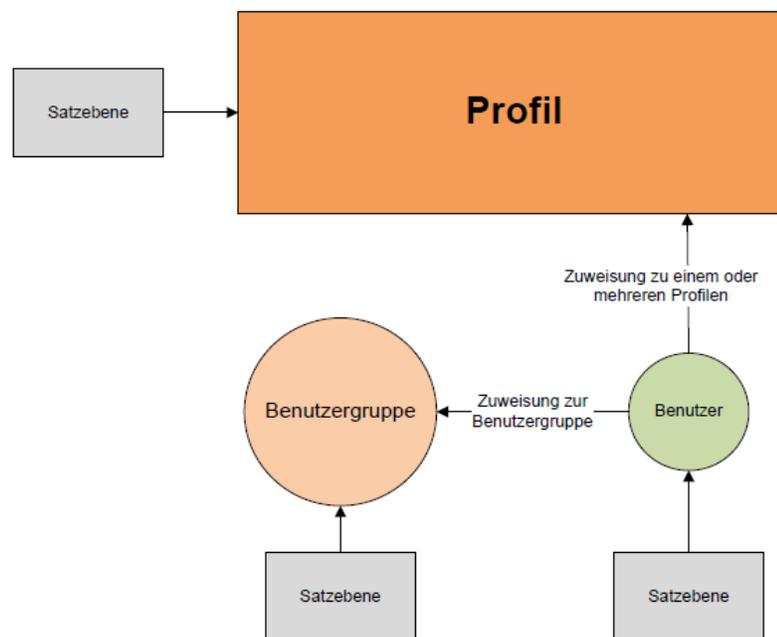
Die Satzebenenberechtigung definiert auf Feldebene Kriterien für den Zugriff auf Datensätze, z. B. nur Zugriff auf Personen eines bestimmten Status. Diese Berechtigung wirkt beim Aufruf einer Suchfunktion (Lupe-Button) oder einer Auswertung zusätzlich zu den dort bereits vorhandenen

Kriterien. Die Satzebenenberechtigung wirkt dabei immer einschränkend, nie erweiternd und kann auch durch vom Anwender selbst zu definierende Kriterien nicht ausgeweitet oder umgangen werden. Prinzipiell werden diese Kriterien vor alle anderen, bereits vorhandenen Kriterien gestellt und mit diesen „und“-verknüpft.

Satzebenenberechtigungen können auf Profilebene, auf Benutzergruppenebene und auf Benutzerebene gesetzt werden.

Die Satzebenenberechtigung wirkt immer absolut. Es ist beispielsweise nicht möglich, jemandem einen Buchstabenbereich A – H zum bearbeiten zuzuweisen und ihm gleichzeitig nur sehenden Zugriff auf andere Buchstabenbereiche zu geben, z. B. für Auskünfte.

Es ist technisch sichergestellt, dass im eigenen Personalfall keine Änderungen vorgenommen werden können, indem die eigene Personalnummer für den schreibenden Zugriff gesperrt wird. Ebenso werden die durch einen Benutzer erfassten Daten für die Vier-Augen-Prüfung durch den selben Benutzer gesperrt.



2.6.2 Datei „Person-Satzebene“

Die Tabelle Person Satzebene enthält tagesaktuell zusammengefasst alle Felder, auf die üblicherweise Satzebenenbeschränkungen eingestellt werden, z. B. Name, Behörde, Organisation, Laufbahnguppe, Status ...

Hierdurch wird die Vergabe von Berechtigungen vereinfacht. Durch die Komplexität des Datenmodells kann eine direkte Abfrage auf die Tabelleninhalte bei benötigten Merkmalskombinationen aus verschiedenen Tabellen und Dateien zu Auswahlfehlern und damit zu ungewollten Ergebnissen bei der Festlegung von Zugriffsberechtigungen führen.

Die Tabelle wird täglich nachts aktualisiert. Einzelne vordefinierte Felder können in Absprache mit P&I auch sofort im Zuge der Buchung aktualisierbar geschaltet werden.

Aus den enthaltenen Datenbankfeldern werden Folgende für die Berechtigungseinstellungen benutzt:

Tabelle Person Satzebene	
Felder	Inhalt
#Person	Person (Schlüssel der Person)
Person Alphabet	Feld zur Sortierung der Datei Person Satzebene (in der ini Datei kann bestimmt werden, ob der Name oder nach dem Vornamen sortiert werden soll)
#Behörde	Enthält zum Personalfall die zugeordnete Stammbehörde/-dienststelle
#Beschäftigungsverhältnis	Enthält die Art der Beschäftigung (Beamter, Tarifbeschäftigter, Versorgung, Zusatzversorgung)
*Behörde Abordnung	Zielbehörde der Abordnung
*Organisation Abordnung	Organisation/Dienstort der Abordnung
Abordnung von	
Abordnung bis	
Steuerung	Statuskennzeichen
Steuerung Familienkasse	Behördenbezogene Zugriffsteuerung für Familienkasse
Steuerung Pfändung	Behördenbezogene Zugriffsteuerung für FPfändung
Steuerung TEUB	Behördenbezogene Zugriffsteuerung für Technikunterstützte Erfassung unständiger Bezüge
Steuerung SP-Expert	Behördenbezogene Zugriffsteuerung für SP-Expert
Steuerung Unfallfürsorge	Behördenbezogene Zugriffsteuerung für Unfallfürsorge
#Status	Differenzierte Statuskennzeichen, inbes. Laufbahnen
gültig bis	Tatsächliches Ausscheiden
Freigabe Datenzugriff Beamtenversorgung	Steuerung der Zugriffsrechte auf Aktivenfälle
Freigabe Datenzugriff Zusatzversorgung	Steuerung der Zugriffsrechte auf Aktivenfälle
Freigabe Datenzugriff Nachversicherung	Steuerung der Zugriffsrechte auf Einzelfallebene

Das Feld „Person Alphabet“ beinhaltet hierbei nicht den kompletten Namen einer Person, um eine „leichte“ Form der Anonymisierung zu erreichen. Über eine Konfigurationsdatei kann seitens der Technischen Leitstelle eingetragen werden, ob Daten aus dem Vornamen oder aus dem Nachnamen und wie viele Zeichen überhaupt gespeichert werden sollen. Derzeit enthält das Feld die ersten fünf Buchstaben des Nachnamens.

Anpassungen können nach Maßgabe der Fachlichkeit über die Technische Leitstelle/P&I vorgenommen werden.

Die Tabelle Person Satzebene enthält nur tagesaktuelle Datenbestände über Personen, die an dem Tag in einem Beschäftigungsverhältnis stehen oder in Zukunft stehen werden. Ausgeschiedene werden nach Ausscheiden nur noch sechs Monate berücksichtigt und anschließend nicht mehr berücksichtigt. Damit stehen Ausgeschiedene für die Sachbearbeitung nicht mehr im Zugriff. Im Falle einer Reaktivierung oder für erforderliche Nacharbeiten stehen Sonderfunktionalitäten zur Verfügung, die ggf. den Zugriff wieder ermöglichen.

2.6.3 Parallelzugriffe auf Daten aus verschiedenen Zuständigkeiten

KoPers verwendet ein relationales Datenbankmodell, welches redundante Datenhaltung weitgehend vermeidet. Dies führt allerdings auch zu geänderten Bedingungen in der Zugriffssteuerung. Bestimmte, nur einmalig im System vorhandene Daten können nicht mehr eindeutig nur einer datenverarbeitenden Stelle zugeordnet sein. Arbeitsanlässe bei mehreren Beschäftigungsverhältnissen, z. B. Arbeitsvertrag bei einer Behörde in Verbindung mit einer Nebentätigkeit bei einer anderen desselben Arbeitgebers, erfordern teilweise den Zugriff auf die gleichen Stammdaten wie Name, Adressdaten, Steuernummer und andere. Diese Daten sind unmittelbar der Person zugeordnet. Daten, die unabhängig vom Beschäftigungsverhältnis an der Person hängen, dürfen von allen Sachbearbeitern auch unterschiedlicher Stellen gepflegt werden. Ab Ebene Beschäftigungsverhältnis stehen dann nur die das jeweilige Beschäftigungsverhältnis betreffenden Angaben im Zugriff.

Nähere Informationen zur Definition und Behandlung von Mehrvertragsfällen ergeben sich aus dem Konzept Mehrvertragsfähigkeit.

3 Sicherheitskonzept KoPers

3.1 Kennwortregeln

Für die Vergabe der Passwörter gelten die Regeln der Passwort-Richtlinie der FHH. Unbeschadet der dortigen Regelungen 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 in KoPers beträgt 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. (Die Änderung wird systemseitig erzwungen, indem die Administratoren die Restgültigkeit des des zentral vergebenen neuen Kennworts auf 0 Tage setzen.).

3.2 Sperrung von Kennungen nach langer Inaktivität

Kennungen sollen nach einer Inaktivität von 45 Tagen gesperrt werden. Eine automatische Sperrung wird von KoPers nicht unterstützt. Auf der Basis von wöchentlichen Auswertungen wird die Fachliche Leitstelle des ZPD zentral eine manuelle Sperrung der ermittelten Arbeitskennungen vornehmen.

3.3 Einschränkungen der Administratoren

Im Rahmen der Benutzeradministration steht für die zentrale Benutzerverwaltung auf Produktion durch die Service-Line im ZPD das Profil ADM_BEN_PROD zur Verfügung. Rechte von Benutzerprofilen und Benutzergruppen können nicht angepasst werden. Das Profil dient der reinen Benutzerverwaltung hinsichtlich

- Anlegen von Kennungen, Passwortfreischaltung, Sperren und Entsperren von Kennungen,
- Zuordnung von Profilen und Benutzergruppen
- Setzen von weiter einschränkenden Rechten auf Satzebene an der Benutzerkennung

Für die dezentrale Administration steht das Profil ADM_BEN_DEZ zur Verfügung. Die Zugriffsrechte beschränken sich hier auf

- das Sperren und Entsperren von Benutzerkennungen,
- die Passwortfreischaltung,
- die Eingabe von Vertretungsregelungen.

Das allumfassende Masterprofil Pul_SYSTEM wird in Produktion keinem Anwender zugeordnet und wird allein für Notfalleingriffe bei Gefährdung des Produktionsbetriebs vorgehalten. Über den Einsatz entscheidet der HR-IT-Auftraggeber bzw. gesondert beauftragte Personen. Die Entscheidung ist schriftlich zu begründen und die Vergabe und Verwendung schriftlich zu dokumentieren. Die Dokumentation ist für Revisionszwecke sechs Jahre aufzubewahren. Der Zugriff erfolgt im Vier-Augen-Prinzip.

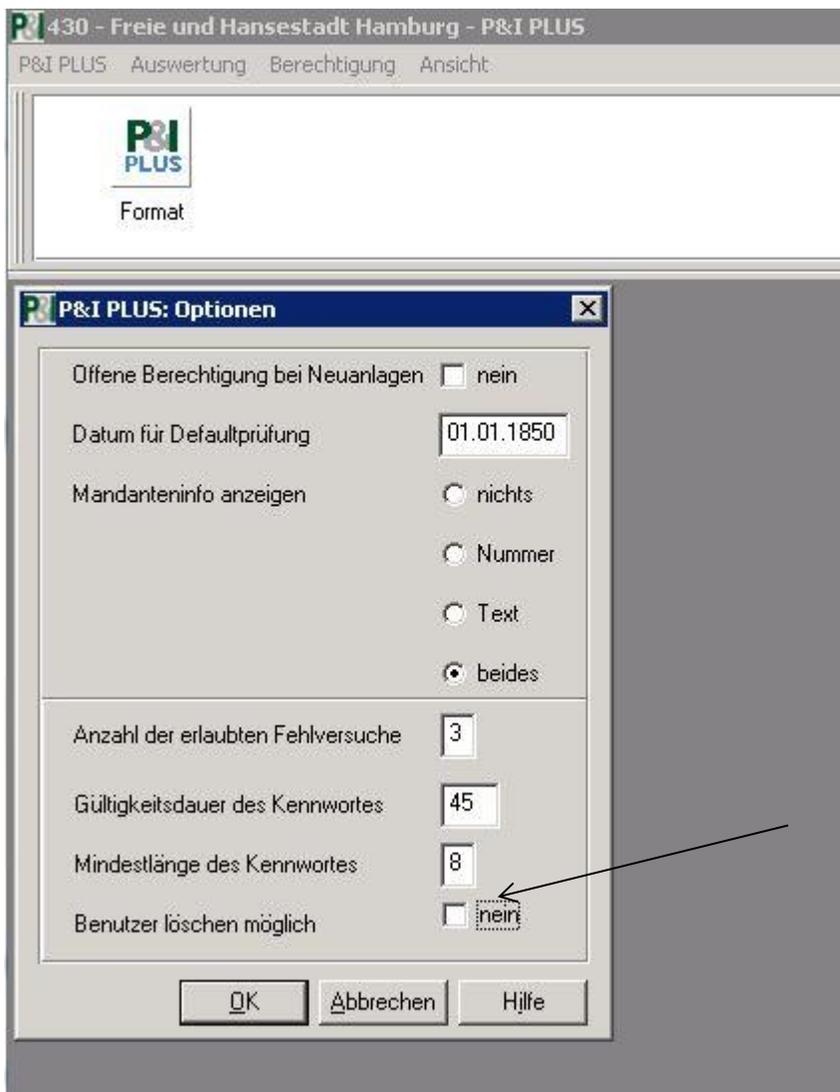
Die Protokolldatei wird monatlich ausgewertet, wann und durch wen im Produktionssystem die Profile

- ADM_AUSWERT
- ADM_BENUTZER
- ADM_KATALOGE
- ADM_MZV
- PUI_SYSTEM

- Anwender
- Mitarbeiter
- Vorgesetzter
- (SSC)
- ESS

vergeben wurden. Die Auswertung wird durch den HR-IT-Beauftragten geprüft und revisions sicher aufbewahrt.

Aus Revisionsgründen muss jederzeit ein Rückschluss auf die tatsächliche Person hinter der verwendeten Kennung möglich sein. Aus Transparenzgründen sind nicht mehr benötigte Kennungen nicht zu löschen, sondern nur zu sperren. Daher wird das Löschen von Kennungen auf Produktion durch die Systemeinstellungen in den Optionen unterbunden. Damit ist das Anlegen von Phantomkennungen mit anschließender Löschung nicht möglich. Auf diese grundlegende Einstellung hat die Benutzeradministration keinen Zugriff.



3.4 Grundlegende Einstellungen

Zur Sicherstellung eines rechtskonformen Systembetriebes sind bei der Berechtigungsvergabe nachstehende Einstellungen vorzunehmen:

- Eine Sachbearbeitung des jeweils eigenen Personalfalls durch Personalsachbearbeiter ist auszuschließen.
- Eine zahlungsrelevante vom Sachbearbeiter gebuchte Information darf nicht durch ihn selbst freigegeben werden.
- Die Versorgung hat umfassenden Zugriff auf alle Daten der Versorgung und für Auskunftszwecke auf eine Infomaske der Zusatzversorgung. Die Zusatzversorgung hat umfassenden Zugriff auf alle Fälle der Zusatzversorgung und auf eine Infomaske der Versorgung für Auskunftszwecke.
- Die Sonderbereiche Pfändungen und Familienkasse haben einen Zugriff auf für die Aufgabenerfüllung wesentliche Daten der Passiven und Aktiven.
- Die Personalabteilungen der Aktiven haben jeweils nur einen Zugriff auf ihre eigenen Personalfälle und Organisationsstrukturen.

3.5 Standardberechtigungs-einstellungen für neue Objekte bei Releasewechsell

Die Hauptentwicklungsarbeit findet nicht auf Hamburger Systemen statt, sondern erfolgt auf Systemen der P&I in Wiesbaden und Iserlohn. Neue Objekte wie Felder, Kataloge, Auswertungen, Geschäftsfälle und Ähnliches werden regelmäßig im Rahmen von Releases und Patches vom Hersteller ausgeliefert und in KoPers-Verfahren eingespielt. Für die Standardeinstellungen wurden dabei Vorgaben festgelegt, die Systemseitig über die Datei verteil.ini gesteuert werden. Nachstehend ein Auszug aus der verteil.ini des Produktionsmandanten 430:

--- Berechtigungen ---

[Feldberechtigung_Benutzer]

Selektion=j

Ausgabe=j

Anzeigen=j

Aendern=j

[Feldberechtigung_Profile]

Selektion=j

Ausgabe=j

Anzeigen=j

Aendern=j

[Katalogberechtigung_Profile]

Loeschen=n

Neuanlage=n

Abrufen=j

[Auswertungsberechtigung_Benutzer]

Abrufen=j

Bearbeiten=j

[Auswertungsberechtigung_Profile]

Abrufen=j

Bearbeiten=j

[Geschäftsfallberechtigung_Benutzer]

Abrufen=j

Bearbeiten=j

nur_ansehen=n

Wiedervorlagen=j

MZV_anzeigen=j

[Geschäftsfallberechtigung_Profile]

Abrufen=n

Bearbeiten=n

nur_ansehen=n

Wiedervorlagen=n

MZV_anzeigen=n

Unterschieden wird dabei wie ersichtlich nach der Objektart (Felder, Kataloge, Auswertungen, Geschäftsfälle) sowie nach Berechtigungsebene (Benutzer, Profil).

Felder:

Neue Felder sind für alle Benutzer und Profile berechtigt. Evtl. Einschränkungen müssen manuell vorgenommen werden.

Kataloge:

Kataloge werden generell berechtigt.

Geschäftsfälle:

Neue Geschäftsfälle sind für alle Benutzer berechtigt und für alle Profile entrechtet. Zugriffsrechte auf Profilebene müssen nach fachlicher Prüfung durch Beauftragung über das Auftragsmanagementsystem in-Step ergänzt werden.

Auswertungen:

Neue Auswertungen sind für alle Benutzer und Profile berechtigt. Evtl. Einschränkungen müssen manuell auf Basis eines im Auftragsmanagementsystems zu dokumentierenden Auftrags vorgenommen werden.

Die Rangfolge von Berechtigungseinstellungen am Benutzer und am Profil ist systemseitig so geregelt, dass die Profileinstellungen höherrangig sind und den Rahmen vorgeben. Am Benutzer können lediglich weitere Einschränkungen erfolgen. Es ist nicht möglich, dem Benutzer über die Profilberechtigungen hinaus weitergehende Rechte einzuräumen.

Ausgenommen hiervon sind die Satzebenenberechtigungen. Diese gelten sowohl am Profil als auch am Benutzer sowie in der Benutzergruppe uneingeschränkt.

3.6 Nachweis der Verwaltung von Berechtigungen

3.6.1 Dokumentation der Verwaltung von Zugriffsrechten

Die Revisionsfähigkeit eines IT-gestützten Verfahrens setzt voraus, dass die Verwaltung der Berechtigungen nachvollzogen werden kann. Daher werden folgende Regelungen getroffen:

Die Vergabe von Berechtigungen erfolgt im Produktivsystem nur auf Basis eines schriftlichen Auftrages (mit handschriftlicher Unterschrift). Die Verifizierung der Auftragsberechtigungen erfolgt durch den Vergleich mit hinterlegten Unterschriftsproben nach Augenschein. Weitere Wege sind nicht ausgeschlossen, wenn nach Stand der Technik eine Verifizierung der antragstellenden Personen gewährleistet ist.

Die Auftragstellung erfolgt durch die Vorgesetzten der zuständigen Fachbereiche im ZPD (Versorgung, Zusatzversorgung, Familienkasse, Pfändung, HR Systemhaus, HR-Service-Center) und der am Verfahren teilnehmenden Dienststellen. Die Übermittlung kann per Post oder durch persönliche Übergabe erfolgen. Andere Übermittlungswege können je nach Stand der Technik in Frage kommen, wenn Absender und Auftragsberechtigte eindeutig zu identifizieren sind.

Ausnahme: Für die Beantragung eines neuen Passworts reicht ein schriftlicher Auftrag des betroffenen Benutzers aus.

Die Umsetzung der Aufträge wird von der Fachlichen Leitstelle mit geeigneten Mitteln dokumentiert. Geeignet sind alle Mittel, die nachvollziehbar beschreiben, wer (Person) welche Änderungen (Einstellungen im System) wann (Datum – keine Uhrzeit!) vorgenommen hat.

Die Originale der Aufträge und die Umsetzungsdokumentationen sind für sechs Jahre für Revisionszwecke aufzubewahren. Die Aufbewahrungsfrist beginnt mit der Sperrung bzw. Löschung einer Berechtigung. Passwortänderungen sind ein Jahr aufzubewahren und anschließend zu vernichten/zu löschen.

3.6.1.1 Das Admin-Protokoll (Historische Berechtigungen)

Für die Nachvollziehbarkeit der Tätigkeiten der Berechtigungsverwaltung werden alle vorgenommenen Anpassungen im Admin-Protokoll vorgehalten. Dies betrifft sowohl die Einstellungen an Profilen und Benutzergruppen als auch konkret die Änderungen bei der Einrichtung und Pflege von Benutzerkennungen.

Zielsetzung
Kontrollfunktion der Fachlichen Leitstelle
Protokollierungszeitpunkt/Vorhaltefrist
Mit jeder Speicherung in KoPers, sechs Jahre nach Abschluss des Kalenderjahres der Wirksamkeit der Änderung
Protokollierungsinhalt
Jede Änderung in der Benutzerverwaltung, an Benutzerprofilen, in der Berechtigungs- und Zugriffsverwaltung auf Feldebene (alter Feldinhalt und neuer Feldinhalt), Art der Änderung (Neuanlage/Änderung), Benutzerkennung, Datum, Uhrzeit

Protokollzugriff
Fachliche Leitstelle, datenverarbeitende Stelle: anlassbezogen und anlassunabhängig
Filterung des Protokollzugriffs
Zur besseren Handhabung des Zugriff können Protokolldaten systemisch gefiltert ausgegeben werden: - Filter auf anzuzeigenden Zeitraum - Filter auf Benutzernamen (Anmeldekennung) - Filter auf Zugriffsart (schreibend/lesend) - Filter auf Berechtigungsobjekt (z. B. Benutzerkennung/Auswertungen/Geschäftsfälle/Kataloge)

Sofern eine mandantenbezogene (jede datenverarbeitende Stelle einzeln) Protokollierung technisch nicht möglich ist, muss über eine entsprechende Filterfunktion gewährleistet sein, dass die Bereitstellung von Protokollinformationen mandantenbezogen von der Fachlichen Leitstelle erfolgen kann.

Alle zu einem Zeitpunkt gültigen Berechtigungseinstellungen können bei Bedarf über Auswertungen abgefragt werden. In Verbindung mit der Admin-Protokoll lässt sich so nachvollziehen, welche Berechtigungen einem Anwender zu einem Zeitpunkt zur Verfügung standen.

Folgende Auswertungen stehen in KoPers zu diesem Zweck zur Verfügung:

Bezeichnung der Auswertung	Kurzbeschreibung
BER Profil/Benutzer	Übersicht über alle im System vorhandenen Profile (Rollen) mit zugeordneten Benutzerkennungen
BER Profil/Benutzer/Satzebene	Übersicht über alle im System erteilten Satzebenenberechtigungen je Profil und je Benutzer
BERP Profile/Felder	Übersicht über alle Feldberechtigungen je Profil
BERP Profil Formate Ausw	Übersicht über alle im System vorhandenen Berechtigungen auf Auswertungen
BERP Profile Formate GF	Übersicht über alle im System vorhandenen Berechtigungen auf Geschäftsfälle
BERP Profil Kataloge	Übersicht über alle im System vorhandenen Berechtigungen auf Kataloge
BER Vertreter	Übersicht über alle eingerichteten Vertretungsregelungen
BER Vergabe kritischer Profile	Monatliche Prüfliste, ob nicht berechtigte Profile im Produktivsystem vergeben worden sind.

Diese Auswertungen sind für Revisionszwecke regelmäßig einmal Monatlich für alle Systemumgebungen zu erzeugen und elektronisch revisionssicher aufzubewahren. Näheres regelt die Fachliche Leitstelle. Die Ergebnisse bieten die in MS Office üblichen Recherche- und Filtermöglichkeiten.

3.6.2 Vergabe von Zugriffsrechten

3.6.2.1 Einrichtung

Für die Sicherheit der Berechtigungsvergabe ist entscheidend, dass für die Vergabe ein mehrstufiges, schriftliches Verfahren existiert. Dafür werden folgende Verfahrensregelungen getroffen:

Die Auftragsberechtigten der Fachbereiche im ZPD (Versorgung, Zusatzversorgung, Familienkasse, Pfändungen, HR Systemhaus, HR-Service-Center) sowie die Auftragsberechtigten in den am Verfahren teilnehmenden Dienststellen entscheiden über die Einrichtung von Zugriffsberechtigungen und beauftragen diese schriftlich bei der Fachlichen Leitstelle.

Für die in der Fachlichen Leitstelle Beschäftigten entscheiden die auftragsberechtigten Personen der Fachlichen Leitstelle über die Einrichtung und den Umfang der Berechtigungen. Die Entscheidungen sind ebenfalls durch Aufträge zu dokumentieren. Es ist organisatorisch auszuschließen, dass auftragsberechtigte Personen selbst Berechtigungsadministratoren sind.

Die schriftlichen Aufträge umfassen

- die zu berechtigende Person,
- das/die zuzuordnende/n Profil/e,
- die beizuordnende Benutzergruppe und
- ggf. weitere für die Umsetzung relevante Kriterien wie beispielsweise Buchstabenbereiche, Einschränkungen bei Auswertungen, Geschäftsfallbeschränkungen und Ähnliches.

Der Umfang der zu vergebenden Zugriffsrechte für die bei Ihnen Beschäftigten liegt in der Verantwortung der datenverarbeitenden Stellen. Die Fachliche Leitstelle berät bei der Einrichtung und setzt die Aufträge nach Maßgabe des Abschnitts 3.3 um.

Die schriftlichen Aufträge sind abzulegen und für Revisionszwecke sechs Jahre nach Abschluss des Kalenderjahres der Wirksamkeit der Änderung aufzubewahren.

3.6.2.2 Änderung von Zugriffsrechten

Im Kassenrecht, wie auch allgemein im Personalakenrecht (§ 85 Abs. 4 HmbBG), gilt das Prinzip der minimalen Berechtigung. Dazu muss insbesondere gewährleistet sein, dass Bedienstete Berechtigungen nicht behalten, wenn sie diese für die Erledigung einer übertragenen Aufgabe nicht mehr benötigen.

Die Geschäfts- und Fachbereiche im ZPD sowie die externen Personalstellen verantworten den Umfang der eingeräumten Zugriffsrechte für die bei Ihnen Beschäftigten selbst. Bei jeder dauerhaften Veränderung von Zuständigkeiten, Aufgabenwechseln oder Aufgabenentfall hat durch die zuständigen auftragsberechtigten Personen eine Gegenprüfung gegen die erteilten Rechte zu erfolgen. Relevante Änderungen sind der Fachlichen Leitstelle anzuzeigen und die Änderung der Zugriffsrechte schriftlich zu beauftragen.

Für die in der Fachlichen Leitstelle beschäftigten Personen trifft die Fachliche Leitstelle organisatorische Regelungen, dass bei berechtigungsrelevanten Veränderungen eine Überprüfung und Anpassung der Berechtigungen erfolgt. Alle Änderungen sind durch schriftliche Aufträge zu dokumentieren.

3.6.2.3 Änderung von Zugriffsrechten bei dezentraler Berechtigungsverwaltung

Die der dezentralen Verwaltung obliegenden Vorfälle (Sperrungen/Entsperrungen, Passwortneuvergabe, Vertretungsregelungen) sind vor Ort nachvollziehbar schriftlich zu dokumentieren. Vorhanden sein müssen mindestens die Auftragserteilung/der Auslöser, der Auftraggeber, der Zeitpunkt – Datum und Uhrzeit - der Umsetzung und wer die Umsetzung vorgenommen hat. Die Dokumentationen sind sechs Jahre für Revisionszwecke vorzuhalten.

4 Kontrolle und Einhaltung des Berechtigungskonzepts

Die für das Verfahren KoPers zuständige Geschäftsbereichsleitung ZPD 3 (HR-Systemhaus) bestimmt eine verantwortliche Person, die die Einhaltung dieses Berechtigungskonzepts kontrolliert. Die benannte Person prüft stichprobenweise, ob die Vergabe von Berechtigungen inhaltlich richtig erfolgt und ordnungsgemäß dokumentiert worden ist.

Bestehen Anhaltspunkte, dass bei der Vergabe von Berechtigungen Fehler aufgetreten sind, ist die Berechtigungsvergabe unverzüglich zu korrigieren. Zuständig für die Korrektur sind die verantwortlichen Berechtigungsadministratoren.

Diese sind über die Anhaltspunkte schriftlich zu informieren. Die durchgeführten Korrekturmaßnahmen sind anschließend ebenfalls schriftlich festzuhalten und aufzubewahren. Die gewerkschaftlichen Spitzenorganisationen werden regelmäßig über wesentliche Ergebnisse von Kontrollverfahren zur Fehlerprüfung informiert.

5 Spezielle Regelungen für Mitzeichnungsverfahren (elektronische Prozesse)

In einem Mitzeichnungsverfahren können grundsätzlich beliebig viele Profile beteiligt werden. In diesem Zusammenhang besteht die Gefahr, dass in einzelnen Organisationseinheiten bestimmte Profile nicht zugeordnet wurden und das Mitzeichnungsverfahren dadurch im ungünstigsten Fall ohne geregeltes Ende blockiert wird. Dies muss durch die zusätzliche Zuweisung von Benutzern zu den „fehlenden“ Profilen gelöst werden.

Um das System administrierbar zu gestalten, sind daher die Mitzeichnungsverfahren möglichst allgemeingültig zu halten (Standardisierung). Dementsprechend muss auch die Anzahl der zugrundeliegenden Profile klein gehalten werden, was zu einer allgemeingültigen Ausgestaltung der Profile führt.

Entscheidend für Zugriffe auf Daten oder Informationen innerhalb des Mitzeichnungsverfahrens ist die Satzebenenausprägung (siehe 2.6) des zugrundeliegenden Benutzers bzw. der zugeordneten Benutzergruppe. Somit hat das teilnehmende Profil auch innerhalb eines Mitzeichnungsverfahrens nur Zugriff auf die Fälle, für die es berechtigt ist.

Bei der Verwendung der Einschränkungen der Formate (s. Ziffer 2) auf Benutzerebene muss zwingend darauf geachtet werden, dass ein funktionsfähiges Mitzeichnungsverfahren gewährleistet wird. Dies kann in der Folge zu unterschiedlichster Ausprägung auf der Benutzerebene bei identisch zugewiesenen Profilen führen.

Nicht mehr ablauffähige Mitzeichnungsverfahren (verursacht z. B. durch die Beteiligung einer Rolle(=Profil), die in einer Dienststelle nicht mit einer Person besetzt ist) können nur durch Eingriffe auf Datenbankebene entfernt werden.