Projekt KoPers

Protokollierungskonzept

Anlage 3

Inhaltsverzeichnis

1 Zusammenfassung

KoPers-Protokollarten

- Protokolldatei: Revisionssichere Nachvollziehung aller Änderungen personenbezogener oder zahlungsrelevanter Daten (Alte und Neue Feldinhalte)
- Anmeldeprotokoll: Protokollierung aller An-/Abmeldeversuche an KoPers
- Admin-Protokoll der Fachlichen Leitstelle KoPers unverändert (Benutzerkennungen, Rechte/Zugriffe)
- Protokollierung der Protokollzugriffe: Protokollierung der Zugriffe auf Protokollinformationen
- Technische Protokollierungen: Protokollierung technischer Jobs, technischer Systemereignisse und Schnittstellenübertragungen
- Protokollierung der kassenrechtlichen Verantwortung

Die sich aus den rechtlichen Rahmenbedingungen ergebenden allgemeinen Anforderungen zur Protokollierung sind in Kapitel 1 beschrieben. Anforderungen an die einzelnen KoPers-Protokolle werden in Kapitel 2 detailliert benannt. Technische Anforderungen an die Umsetzung der Protokolle in Kapitel 3. Organisatorische Vorgaben für den anlassbezogenen und anlassunabhängigen Zugriff auf die Protokolle sowie die Löschung werden in Kapitel 4 aufgezählt.

2 Anforderungen an Protokollierung

2.1 Gesetzliche Grundlagen und Richtlinien

Die Notwendigkeit für die Protokollierung ergibt sich aus den kassenrechtlichen Anforderungen zur Revisionssicherheit und dem Personalakten- und Datenschutzrecht. Spezialregelungen finden sich in den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS), im Hamburgischen Beamtengesetz (Personalaktenrecht §§ 85-92 HmbBG)[1], dem Hamburgischen Datenschutzgesetz (HmbDSG). sowie §41 Abs.1 EStG, §28f und 28p SGB IV. Das Verfahren muss sicherstellen, dass zu jedem Zeitpunkt festgestellt werden kann, welche Personen, einschließlich Administratoren und andere Systemverwalter, oder Inputschnittstellen welche Handlungen vorgenommen haben. Hierzu ist es auch erforderlich die Verwaltung von Berechtigungen, insbesondere die Identität der Personen, die die Berechtigungen zuweisen und denen die Berechtigungen zugewiesen werden, zu dokumentieren. Durch die unterschiedlichen Gesetze und Regelungen werden Kontrollziele wie Eingabekontrolle oder Verantwortlichkeitskontrolle formuliert, aus denen sich die Pflicht zur Protokollierung ableiten lässt. Teilweise ergeben sich konkretisierte Protokollierungsvorschriften aus darüber hinausgehenden Verwaltungsanordnungen.

Durch die Revisionsfähigkeit eines IT-Verfahrens wird gemäß Nr. 7 der Anlage 10 VV ZBR gewährleistet, dass über sämtliche buchführungspflichtigen Geschäftsvorfälle ein sachlicher und zeitlicher Nachweis erbracht werden kann. Dieser muss von einer sachverständigen, nicht am Verfahren beteiligten Person in angemessener Zeit dahingehend prüfbar sein, ob

[1] § 85 HmbBG findet Anwendung und zwar unabhängig davon, ob eine elektronische Personalakte bereits eingeführt ist oder nicht. Die besondere Schutzbedürftigkeit der Beschäftigtendaten (im Sinne der speziellen Vorschrift des § 85 HmbBG) ist gegeben

- die verfahrensrechtlichen Vorgaben dieser Anlage und der weiteren kassenrechtlichen Vorschriften eingehalten wurden (formelle Richtigkeit) und
- die inhaltlichen Anforderungen an eine Buchung sowie an eine Ein- oder Auszahlung, insbesondere das Vorliegen eines Rechtsgrundes, erfüllt sind (sachliche Richtigkeit) und die Transparenz bzw. Authentizität der Datenverarbeitung (§ 8 Abs. 2 Nr. 4 HmbDSG) des Verfahrens zu unterstützen.

Die Revisionsfähigkeit verlangt zudem, dass die Datenverarbeitung nachvollziehbar ist. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen oder zahlungsrelevanten Daten in welcher Weise verarbeitet hat (vgl. § 8 Abs. 2 Nr. 5 HmbDSG). Nachweisbar muss auch die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener oder zahlungsrelevanter Daten sein. Darüber hinaus ermöglicht die Revisionsfähigkeit des Verfahrens, die Erledigung von Aufgaben mit Bezug zum Haushalts- Kassen- und Rechnungswesen nachträglich auf ihre Ordnungsmäßigkeit hin zu überprüfen. Gemäß Nr. 7.2 der Anlage 10 VV ZBR sind Zugriffe auf das IT-Verfahren zu dokumentieren. Es muss jederzeit nachgewiesen werden können, welche Person zu welcher Zeit welche Aktionen ausgeführt hat. Der Nachweis muss zumindest folgende Daten enthalten:

- die Bezeichnung des Geschäftsvorfalls, auf den zugegriffen worden ist,
- das Datum, die Uhrzeit und die Benutzerkennung der Sachbearbeiterin oder des Sachbearbeiters, die bzw. der die Änderung vorgenommen hat, sowie
- die geänderten Daten mit altem und neuem Stand.

Der Grundsatz der **Vertraulichkeit** (§ 8 Abs. 2 Nr. 1 HmbDSG) bestimmt, dass nur Befugte Daten zur Kenntnis nehmen bzw. auf diese zugreifen können. Zugang zu Personalaktendaten dürfen gemäß § 85 Abs. 4 HmbBG nur Beschäftigte haben, die mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Gemäß Nr. 4.2 der Anlage 10 VV ZBR dürfen Berechtigungen im IT-Verfahren eingerichtet werden, soweit dies zur Aufgabenerfüllung zwingend erforderlich ist (Prinzip der minimalen Berechtigung). Darüber hinaus ist zu gewährleisten, dass die Daten unverfälscht, vollständig und widerspruchsfrei bzw. zurechenbar und aktuell bleiben (**Integrität**, § 8 Abs. 2 Nr. 2 HmbDSG).

Alle Protokolldaten unterliegen einer strikten **Zweckbindung** (vgl. § 13 HmbDSG), für Personalaktendaten ergibt sich die Zweckbindung aus § 85 Abs. 4 HmbBG. Die Zweckbindung ist hier besonders wichtig, weil Protokollierungsdaten einen umfassenden Einblick in die Tätigkeiten der Administratoren und Nutzer bzw. Anwender ermöglichen. Im Rahmen der Zweckbindung muss für sämtliche Protokollierungseinträge die Auswertung und Verwendung geregelt sein, z. B. für Fehleranalysen oder zur anlassbezogenen Prüfung eines Missbrauchsverdachts.

§ 28 Abs. 7 HmbDSG konkretisiert die Zweckbindung dahingehend, dass Daten, die zu Beschäftigten gespeichert werden, nicht zu anderen **Zwecken, insbesondere nicht zu Zwecken der Verhaltens- oder Leistungskontrolle**, genutzt werden dürfen. Dies gilt auch für Systemadministratoren.

2.2 Erforderlichkeit, Gebot der Datensparsamkeit und -vermeidung

Darüber hinaus gilt für IT-Systeme das Gebot der **Datensparsamkeit** und **Datenvermeidung** (§ 5 Abs. 4 HmbDSG), das bei der technischen Ausgestaltung und Auswahl der Protokollierungsverfahren zu beachten ist. Um dem Gebot der Datensparsamkeit nachzukommen,

sind insbesondere die Möglichkeiten zur **Pseudonymisierung oder Anonymisierung** zu berücksichtigen. Dabei besteht regelhaft ein Zielwiderspruch zur Integrität und Authentizität bzw. Transparenz der Datenverarbeitung (§ 8 Abs. 2 Nr. 2 und 4 HmbDSG).

Hinweise zum Umgang mit Protokolldaten, die einem Verwertungsverbot unterliegen oder aus anderen Gründen nicht vorgehalten werden dürfen, gehen aus dem Löschkonzept hervor.

3 Anforderungen an Protokollierung im P&I System

Gemäß Nr. 6 der Anlage 5 zu Nr. 4.7 der VV-ZBR sind Unterlagen, die der Dokumentation von Software und IT-Verfahren zur Berechnung, Festsetzung, Anordnung oder Zahlbarmachung dienen, wie Belege aufzubewahren.

Unterlagen, die der Dokumentation von Software und IT-Verfahren zur Haushaltsüberwachung, Buchführung oder Rechnungslegung einschließlich der Kassen- oder Haushaltsrechnung dienen, sind wie Sachbücher aufzubewahren.

Gemäß Nr. 2.1.6 sind Bücher und Rechnungsunterlagen 10 Jahre, Belege sind sechs Jahre aufzubewahren. Abweichende Aufbewahrungsfristen in Rechts- und Verwaltungsvorschriften bleiben unberührt. (Nr. 4.7.2 VV-ZBR).

3.1 Protokolldatei

Zielsetzung
Revisionssichere Nachvollziehung aller Änderungen personenbezogener oder zahlungsrelevanter Daten
Protokollierungszeitpunkt/ Vorhaltefrist
Mit jedem Speichervorgang in KoPers, 6 Jahre nach Abschluss des Haushaltsjahres, der Wirksamkeit der Änderung bzw. für das die Unterlagen bestimmt sind.[2] (Nr. 7.1 der Anlage 5 zu Nr. 4.7 der VV-ZBR),
Protokollierungsinhalt
Personal- und Vertragsnummer, Datum, Uhrzeit[3], Benutzer- oder Systemkennung, Geschäftsfall, Dateibezeichnung, Feldbezeichnung, vorgenommene Änderung auf Feldebene (alter Feldinhalt und neuer Feldinhalt), Art der Änderung (Neuanlage/Änderung) und ggf. Systemänderungen (Beispiel Datenänderung durch ELStAM). Die Protokollierung entspricht dem P&I Standard und ist nicht anpassbar, da hiervon alle Kunden der P&I AG betroffen wären. Die Protokollierung „Änderung“ hält den Sachverhalt fest, dass ein Sachbearbeiter, die Daten auf sachliche Richtigkeit geprüft hat. Der Eintrag

[2] Das kann bei einer zur Einstellung erfassten IBAN bedeuten, dass diese 6 Jahre nach der Beendigung der Bankverbindung protokolliert sein muss.

[3] Die Protokollierung der Uhrzeit muss erfolgen, weil sonst nicht im Rahmen der Revisionsfähigkeit nachvollzogen werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat – das „wann“ ist in § 8 Abs.2 Nr. 5 HmbDSG, ausdrücklich vorgesehen. Eine Leistungs- und Verhaltenskontrolle wird damit nicht bezweckt; sie ist nach § 28 Abs.7 HmbDSG auch nicht zulässig.

„Genehmigung“ hält den Sachverhalt fest, dass ein Prüfer die Daten geprüft und für korrekt erachtet hat und die Anordnung erfolgt ist.

Protokollzugriff

Fachliche Leitstelle (bei Stufe 1 im Auftrag der datenverarbeitenden Stelle): anlassbezogen und im Rahmen monatlicher - zunächst heuristischer - Prüfungen (vgl. Kapitel 4)

Filterung des Protokollzugriffs

Zur besseren Handhabung des Zugriff können Protokolldaten systemisch gefiltert ausgegeben werden:

- Filter auf anzuzeigenden Zeitraum
- Filter auf Art der Änderung und Datentyp
- Filter auf Geschäftsfall und Personalnummer
- Filter auf Daten einer datenverarbeitenden Stelle (Org-Einheit)

Besonderheit

Da das KoPers-System Personaldaten (vgl. § 85 Abs.1 HmbBG) enthält, müssen auch lesende Zugriffe protokolliert werden, sofern diese nicht durch die personalverwaltende Stelle selbst erfolgen. Personalaktendaten sind vertraulich zu behandeln und vor unbefugter Einsichtnahme zu schützen. Zugang zur Personalakte dürfen nur Personalsachbearbeiter haben, soweit dies zu Zwecken der Personalverwaltung und der Personalwirtschaft erforderlich ist (§ 85 Abs. 4 HmbBG).

Ausnahmsweise darf im Rahmen der Datensicherung oder der Systemwartung („Sicherung des ordnungsmäßigen Betriebes einer Datenverarbeitungsanlage“) eine Kenntnisnahme von Personalaktendaten erfolgen, soweit diese „nach dem Stand der Technik nicht oder nur mit unverhältnismäßigem Aufwand zu vermeiden ist“ (§ 85 Abs. 6 S. 2 HmbBG). Um nachprüfen zu können, ob diese Voraussetzung erfüllt ist, muss jede Kenntnisnahme von Personalaktendaten durch Administratoren bei Dataport zumindest protokolliert werden. Nur so kann auch die Revisionsfähigkeit (§ 8 Abs. 2 Nr. 5, s.o. 1.1.) gewährleistet werden.

Der folgende Screenshot ist zur besseren Lesbarkeit auf 2 Abbildungen aufgeteilt. Systemseitig handelt es sich um eine gemeinsame CSV Datei.

Systemdatum	Systemzeit	#Person	Name	Vorname	Geburtsdatum	Pers.-Nr.	Benutzername	Datenbestand	Feld
05.10.2015	10:39:10	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Sachbearbeiterzuordnung Person/(Z)VersF.	*Sachbearbeiter ID
05.10.2015	10:38:47	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV Zulage/Vst. E0	#Buchführungsart
05.10.2015	10:38:47	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV Zulage/Vst. E0	!gültig ab
05.10.2015	10:38:47	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV Zulage/Vst. E0	!gültig bis
05.10.2015	10:38:47	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV Zulage/Vst. E0	Erste Hauptverrechnungsstelle
05.10.2015	10:38:47	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV Zulage/Vst. E0	Wichtung prozentual
05.10.2015	10:38:47	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV Zulage/Vst. E0	#Verrechnungsstellen
05.10.2015	10:37:28	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV/Steuerdaten	#Steuerklasse
05.10.2015	10:37:28	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV/Steuerdaten	#Kirchensteuer Arbeitnehmer
05.10.2015	10:37:28	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV/Steuerdaten	Abw. steuerliches Geburtsdatum liegt vor
05.10.2015	10:37:28	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV/Steuerdaten	!gültig bis
05.10.2015	10:37:28	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV/Steuerdaten	!gültig ab
05.10.2015	10:37:28	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV/Steuerdaten	!berechnet bis
05.10.2015	10:36:15	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Unfallversicherung	#Berufsgenossenschaft
05.10.2015	10:36:15	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Unfallversicherung	*AG Unfallversicherung
05.10.2015	10:36:15	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Unfallversicherung	#Gefahrentarif
05.10.2015	10:36:15	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Unfallversicherung	Prozentsatz 1
05.10.2015	10:36:15	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Unfallversicherung	ID Unfallversicherung
05.10.2015	10:36:15	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Unfallversicherung	!gültig ab
05.10.2015	10:36:15	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Unfallversicherung	!gültig bis

05.10.2015	10:36:15	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Unfallversicherung	#ID Person Unfallversicherung
05.10.2015	10:27:42	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Krankenversicherung	#Krankenversicherung
05.10.2015	10:27:42	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Krankenversicherung	Sozialversicherungsnummer
05.10.2015	10:27:42	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Krankenversicherung	!gültig ab
05.10.2015	10:27:42	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Krankenversicherung	!berechnet bis
05.10.2015	10:27:42	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Krankenversicherung	Auslöser Webservice KK-Fusion
05.10.2015	10:27:42	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Krankenversicherung	Kopierfeld Name KK
05.10.2015	10:27:42	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person Krankenversicherung	!gültig bis
05.10.2015	10:25:19	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV/SV-Nummer+Meldeverfahren	#Berufsbereich
05.10.2015	10:25:19	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV/SV-Nummer+Meldeverfahren	#Berufshauptgruppe
05.10.2015	10:25:19	100147	Maus	Melitta	15.08.1969	60000377	mlueb	Person BV/SV-Nummer+Meldeverfahren	#Berufsgruppe

Geschäftsmodul	Geschäftsfall	Protokolldaten Aktion	alter Wert	neuer Wert	Abrechnungsstand Versorger
Person	SB-Zuordnung Person	Neuanlage		2816; Normannenweg; 36; 20537; Hamburg; ZPD 36	00.00.0000
Person	Finanzpositionen FHH	Neuanlage		Kameral FHH	00.00.0000
Person	Finanzpositionen FHH	Neuanlage	00.00.0000	01.03.2015	00.00.0000
Person	Finanzpositionen FHH	Neuanlage	00.00.0000	31.12.9999	00.00.0000
Person	Finanzpositionen FHH	Neuanlage	0	1	00.00.0000
Person	Finanzpositionen FHH	Neuanlage	0,00	100,00	00.00.0000
Person	Finanzpositionen FHH	Neuanlage		00.6.0680.061.02; 19500101; 99991231; 006; 0680; 06102; Statistisches Amt für Hamburg und Schleswig-Holstein; 0	00.00.0000
Person	Steuer FHH	Neuanlage		Steuerklasse IV	00.00.0000
Person	Steuer FHH	Neuanlage		Evangelisch	00.00.0000
Person	Steuer FHH	Neuanlage		Nein	00.00.0000
Person	Steuer FHH	Neuanlage	00.00.0000	31.12.9999	00.00.0000
Person	Steuer FHH	Neuanlage	00.00.0000	01.03.2015	00.00.0000
Person	Steuer FHH	Neuanlage	00.00.0000	31.12.9999	00.00.0000
Person	Unfallversicherung FHH	Neuanlage		UK Nord	00.00.0000
Person	Unfallversicherung FHH	Neuanlage		123456789	00.00.0000
Person	Unfallversicherung FHH	Neuanlage		99999999	00.00.0000
Person	Unfallversicherung FHH	Neuanlage	0,00	100,00	00.00.0000
Person	Unfallversicherung FHH	Neuanlage	0	100000000019	00.00.0000
Person	Unfallversicherung FHH	Neuanlage	00.00.0000	01.03.2015	00.00.0000
Person	Unfallversicherung FHH	Neuanlage	00.00.0000	31.12.9999	00.00.0000
Person	Unfallversicherung FHH	Neuanlage		1	00.00.0000
Person	Person Krankenkasse	Neuanlage		BKK FREUDENBERG	00.00.0000
Person	Person Krankenkasse	Neuanlage		19150869H690	00.00.0000
Person	Person Krankenkasse	Neuanlage	00.00.0000	01.03.2015	00.00.0000
Person	Person Krankenkasse	Neuanlage	00.00.0000	31.12.9999	00.00.0000
Person	Person Krankenkasse	Neuanlage		63922962	00.00.0000
Person	Person Krankenkasse	Neuanlage		BKK FREUDENBERG	00.00.0000
Person	Person Krankenkasse	Neuanlage	00.00.0000	31.12.9999	00.00.0000
Person	Meldeverfahren FHH	Neuanlage		Kaufmännische Dienstleistungen, Warenhandel, Vertrieb, Hotel und Tourismus	00.00.0000
Person	Meldeverfahren FHH	Neuanlage		Tourismus, Hotel- und Gaststättenberufe	00.00.0000
Person	Meldeverfahren FHH	Neuanlage		Tourismus und Sport	00.00.0000

Abbildung 1: Abbildungen zu Protokolldaten / Protokolldatei

3.2 Anmeldeprotokoll

Zielsetzung
Auswertung der erfolgreichen und nicht erfolgreichen Anmeldeversuche; gemäß Nr. 5 der Anlage 10 VV ZBR ist sicherzustellen, dass eine Zugriffskontrolle gewährleistet ist und in den Arbeitsablauf nicht unbefugt eingegriffen werden kann. Der Zugriff auf das Verfahren wird durch ein Passwort geschützt, das die Vorgaben der Passwortrichtlinie in der jeweils

geltenden Fassung einhält.
Protokollierungszeitpunkt / Vorhaltefrist
Die Protokollierung erfolgt zu jedem Anmeldeversuch, Vorhaltefrist: 3 Monate
Protokollierungsinhalt
IP-Adressen der Clients mitsamt Datum und Zeit der Anmeldung, Anmeldekennung und Hinweis ob die Anmeldung erfolgreich war. Darüber hinaus muss mandantenspezifisch konfiguriert werden können, inwieweit die Protokollierung der Anmeldung und/oder Abmeldung durchgeführt werden soll. (Auswertung „Anmeldeprotokoll“)
Protokollzugriff
Fachliche Leitstelle, Technische Leitstelle (bei Stufe 1 im Auftrag der datenverarbeitenden Stelle): anlassbezogen und anlassunabhängig (vgl. Kapitel 4). Erfolgreiche Anmeldeversuche werden nur anlassbezogen, d. h. im Verdachtsfall, ausgewertet.
Filterung des Protokollzugriffs
Zur besseren Handhabung des Zugriff können Protokolldaten systemisch gefiltert ausgegeben werden: • Filter auf anzuzeigenden Zeitraum • Filter auf Benutzernamen (Anmeldekennung) und IP-Adresse • Filter auf Daten einer datenverarbeitenden Stelle (Org-Einheit)

!Systemdatum	!Systemzeit	!Ben-Name	!Pro-Name	IP-Adresse	Text	Versuch
05.10.2015	11:45:14	xxx1	ADM_AUSWERT	10.62.35.136	Benutzer: 'xxx1' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	11:35:35	xxx2	Anwender	10.109.69.167	Benutzer 'xxx2' hat zum Profil 'Anwender' gewechselt.	erfolgreich
05.10.2015	11:35:35	xxx2	Anwender	10.109.69.167	Benutzer 'xxx2' hat zum Profil 'Anwender' gewechselt.	erfolgreich
05.10.2015	11:34:29	xxx2	SB_PERSONAL	10.109.69.167	Benutzer 'xxx2' hat zum Profil 'SB_PERSONAL' gewechselt.	erfolgreich
05.10.2015	11:34:29	xxx2	SB_PERSONAL	10.109.69.167	Benutzer 'xxx2' hat zum Profil 'SB_PERSONAL' gewechselt.	erfolgreich
05.10.2015	11:34:06	xxx2	SB_ZUVERS	10.109.69.167	Benutzer: 'xxx2' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	11:28:53	xxx4	ADM_AUSWERT	10.62.35.136	Benutzer 'xxx4' hat zum Profil 'ADM_AUSWERT' gewechselt.	erfolgreich
05.10.2015	11:28:44	xxx4	Anwender	10.62.35.136	Benutzer: 'xxx4' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	11:23:45	xxx1	Anwender	10.109.69.43	Benutzer 'xxx1' hat zum Profil 'Anwender' gewechselt.	erfolgreich
05.10.2015	11:23:45	xxx1	Anwender	10.109.69.43	Benutzer 'xxx1' hat zum Profil 'Anwender' gewechselt.	erfolgreich
05.10.2015	11:23:40	xxx1	ADM_AUSWERT	10.109.69.43	Benutzer: 'xxx1' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	11:20:08	xxx3	ADM_PROTOKOL	10.62.35.136	Benutzer 'xxx3' hat zum Profil 'ADM_PROTOKOL' gewechselt.	erfolgreich
05.10.2015	11:19:31	xxx3	Anwender	10.62.35.136	Benutzer: 'xxx3' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	11:19:25	xxx6	Anwender	10.109.69.177	Benutzer: 'xxx6' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	11:06:33	xxx1	ADM_AUSWERT	10.62.35.136	Benutzer: 'xxx1' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	10:40:07	DP_Reltest	PUI_SYSTEM	10.62.35.136	Benutzer 'DP_Reltest' hat zum Profil 'PUI_SYSTEM' gewechselt.	erfolgreich
05.10.2015	10:40:00	DP_Reltest	ADM_DP_PROD	10.62.35.136	Benutzer: 'DP_Reltest' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	10:32:13	DP_Reltest	PUI_SYSTEM	10.78.22.168	Benutzer 'DP_Reltest' hat zum Profil 'PUI_SYSTEM' gewechselt.	erfolgreich
05.10.2015	10:32:13	DP_Reltest	PUI_SYSTEM	10.78.22.168	Benutzer 'DP_Reltest' hat zum Profil 'PUI_SYSTEM' gewechselt.	erfolgreich
05.10.2015	10:32:06	DP_Reltest	ADM_DP_PROD	10.78.22.168	Benutzer: 'DP_Reltest' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	10:10:44	DP_Reltest	PUI_SYSTEM	10.62.35.136	Benutzer 'DP_Reltest' hat zum Profil 'PUI_SYSTEM' gewechselt.	erfolgreich
05.10.2015	10:10:38	DP_Reltest	ADM_DP_PROD	10.62.35.136	Benutzer: 'DP_Reltest' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	10:06:18	xxx5	ADM_BENUTZER	10.109.67.253	Benutzer 'xxx5' hat zum Profil 'ADM_BENUTZER' gewechselt.	erfolgreich
05.10.2015	10:06:18	xxx5	ADM_BENUTZER	10.109.67.253	Benutzer 'xxx5' hat zum Profil 'ADM_BENUTZER' gewechselt.	erfolgreich
05.10.2015	10:06:07	xxx5	Anwender	10.109.67.253	Benutzer: 'xxx5' hat sich erfolgreich angemeldet !	erfolgreich

05.10.2015	10:02:36	xxx3	Anwender	10.109.69.92	Benutzer: 'xxx3' hat sich erfolgreich angemeldet !	erfolgreich
05.10.2015	10:02:13	xxx3		10.109.69.92	Benutzer: 'xxx3' hat sich mit dem falschen Kennwort angemeldet. Anmeldung abg	fehlgeschlagen
05.10.2015	10:02:07	xxx3		10.109.69.92	Benutzer: 'xxx3' hat sich mit dem falschen Kennwort angemeldet. Anmeldung abg	fehlgeschlagen
05.10.2015	09:57:35	DP_Reltest		10.62.35.136	Benutzer: 'DP_Reltest' hat sich zu oft vergeblich angemeldet. Kennung gesperrt !	fehlgeschlagen

Abbildung 2: Anmeldeprotokoll

3.3 Admin-Protokoll

Zielsetzung
Revisionssichere Nachvollziehbarkeit der Arbeit derFachlichen Leitstelle gemäß Nr. 4.2 der Anlage 10 VV ZBR dürfen Berechtigungen im IT-Verfahren nur eingerichtet werden, soweit dies zur Aufgabenerfüllung zwingend erforderlich ist (Prinzip der minimalen Berechtigung). Es ist ein Verfahren für die Verwaltung der Berechtigungen (Einrichtung, Veränderung, Entzug) festzulegen. Das Verfahren muss sicherstellen, dass zu jedem Zeitpunkt festgestellt werden kann, welche Personen, einschließlich Administratoren und andere Systemverwalter, zu welchem Zeitpunkt mit welchen Berechtigungen ausgestattet gewesen sind. Die Verwaltung von Berechtigungen, insbesondere die Identität der Personen, die die Berechtigungen zuweisen und denen die Berechtigungen zugewiesen werden, ist zu dokumentieren.
Protokollierungszeitpunkt / Vorhaltefrist
Mit jeder Speicherung in KoPers, 6 Jahre nach Abschluss des Haushaltsjahres der Wirksamkeit der letzten Änderung des Benutzers (Nr. 7.1 der Anlage 5 zu Nr. 4.7 der VV-ZBR)
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 (Auswertungen „Historische Berechtigungen“ und „Formatprotokoll“)
Protokollzugriff
Technische Leitstelle (für Stufe 1 im Auftrag der datenverarbeitende Stelle, für Stufe 2 im Auftrag des HR IT-AG): 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 Daten einer datenverarbeitenden Stelle (Org-Einheit) • Filter auf Zugriffsart (schreibend/lesend) • Filter auf Berechtigungsobjekt (z. B. Geschäftsfälle / Kataloge)
Besonderheit
Zusätzlich ist es möglich, jederzeit eine Liste zu erstellen über alle Benutzerkennungen, Benutzerprofile und Berechtigungen (siehe auch 2.6).

Der folgende Screenshot ist zur besseren Lesbarkeit auf 2 Abbildungen aufgeteilt. Systemseitig handelt es sich um eine gemeinsame CSV Datei.

!Systemdatum	!Systemzeit	!Ben-Name	!Pro-Name	Aktion	Abr. Alt	Abr. Neu	Ans. Alt	Ans. Neu	Bea. Alt	Bea. Neu	Mzv Alt	Mzv Neu	Wdv Alt	Wdv Neu	Kriterien Alt
29.09.2015	15:40:24	xxx1	ADM_BENUTZER	Änderung	Nein	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	
29.09.2015	15:39:41	xxx1	ADM_BENUTZER	Änderung	Nein	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	
29.09.2015	15:39:41	xxx1	ADM_BENUTZER	Änderung	Nein	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	
29.09.2015	15:39:41	xxx1	ADM_BENUTZER	Änderung	Nein	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	
29.09.2015	15:39:41	xxx1	ADM_BENUTZER	Änderung	Nein	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	

29.09.2015	15:39:41	xxx1	ADM_BENUTZER	Änderung	Nein	Ja	Nein	Ja	Nein	Nein		Nein	Nein	Nein	Nein
29.09.2015	15:39:41	xxx1	ADM_BENUTZER	Änderung	Nein	Ja	Nein	Ja	Nein	Nein		Nein	Nein	Nein	Nein
29.09.2015	15:39:41	xxx1	ADM_BENUTZER	Änderung	Nein	Ja	Nein	Ja	Nein	Nein		Nein	Nein	Nein	Nein
29.09.2015	15:39:41	xxx1	ADM_BENUTZER	Änderung	Nein	Ja	Nein	Ja	Nein	Nein		Nein	Nein	Nein	Nein

Berechtiger	Berechtigungsprotokoll Neu Kriterien	Berechtiger Name	Be.Nr.	Berechtigungsmodul	Objekt Art	Objekt Name	O-Nr.
Profile		SB_AGFUNKT	23		Geschäftsfälle	Versorgungsverhältnis /Stammorg FHH	800626
Profile		SB_AGFUNKT	23		Geschäftsfälle	Vorbehalte FHB	100779
Profile		SB_AGFUNKT	23		Geschäftsfälle	Vorschuss NRW	800606
Profile		SB_AGFUNKT	23		Geschäftsfälle	Vortätigkeiten Tarifbeschäftigte FHB	100780
Profile		SB_AGFUNKT	23		Geschäftsfälle	Vorweggewährung Erfahrungsstufe	100766
Profile		SB_AGFUNKT	23		Geschäftsfälle	Wertigkeit pflegen	800612
Profile		SB_AGFUNKT	23		Geschäftsfälle	Wiedervorlage HB	81
Profile		SB_AGFUNKT	23		Geschäftsfälle	ZfA Ruhelohn	800605
Profile		SB_AGFUNKT	23		Geschäftsfälle	Zusatzurlaub FHB	100781
Profile		SB_AGFUNKT	23		Geschäftsfälle	cmu BEW Personaldaten Löschen	300268

Abbildung 3: Abbildungen zu historischen Berechtigungen

Der folgende Screenshot ist zur besseren Lesbarkeit auf 2 Abbildungen aufgeteilt. Systemseitig handelt es sich um eine gemeinsame CSV Datei.

!Systemdatum	!Systemzeit	!Ben-Name	Aktion	Alt-Wert	Neu-Wert	Datenbestand Name
05.10.2015	11:49:01	xxx1	Änderung			
05.10.2015	11:49:01	xxx1	Änderung			
05.10.2015	11:49:01	xxx1	Änderung			
05.10.2015	11:49:01	xxx1	Änderung			
05.10.2015	11:49:01	xxx1	Löschung	Anspruchsberechnung (aus Anspruchsberechnung) wurde entfernt.		Anspruchsberechnung
05.10.2015	11:49:01	xxx1	Löschung	Automatische Urlaubsberechnung (aus Person Urlaub) wurde entfernt.		Person Urlaub
05.10.2015	11:49:01	xxx1	Löschung	RestAktJahr (aus Person Urlaub) wurde entfernt.		Person Urlaub
05.10.2015	11:49:01	xxx1	Löschung	RestVorjahr (aus Person Urlaub) wurde entfernt.		Person Urlaub
05.10.2015	11:49:01	xxx1	Löschung	Schwerbehindertenurlaub (aus Person Urlaub) wurde entfernt.		Person Urlaub
05.10.2015	11:49:01	xxx1	Löschung	Urlaub genommen (aus Person Urlaub) wurde entfernt.		Person Urlaub
05.10.2015	11:49:01	xxx1	Löschung	Urlaubsanspruch (aus Person Urlaub) wurde entfernt.		Person Urlaub
05.10.2015	11:49:01	xxx1	Löschung	Urlaubsberechnung in Std. (aus Person Beschäftigungsverhältnis) wurde entfernt.		Person Beschäftigungsverhältnis
05.10.2015	11:49:01	xxx1	Löschung	Urlaubsjahr (aus Person Urlaub) wurde entfernt.		Person Urlaub

Feld Name	Format Name	Art	Nr.	Formatart-Name	Objekt
wfZusatzUrlaubsanspruch_in_TagenSGB1	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Konstanten-Zuordnung
wfZusatzUrlaubsanspruch_in_TagenSGB2	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Konstanten-Zuordnung
wfSchwerbehindertenurlaub_in_TagenSGB1	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Konstanten-Zuordnung
wfSchwerbehindertenurlaub_in_TagenSGB2	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Konstanten-Zuordnung
Anspruchsberechnung	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Feld-Zuordnung
Automatische Urlaubsberechnung	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Feld-Zuordnung
RestAktJahr	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Feld-Zuordnung
RestVorjahr	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Feld-Zuordnung
Schwerbehindertenurlaub	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Feld-Zuordnung
Urlaub genommen	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Feld-Zuordnung
Urlaubsanspruch	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Feld-Zuordnung
Urlaubsberechnung in Std.	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Feld-Zuordnung
Urlaubsjahr	PV_Einstellungsverfuegung_Beschaeftigte	SB	107116	Serienbriefformat	Feld-Zuordnung

Abbildung 4: Abbildungen Formatprotokoll

3.4 Protokollierung der Protokollzugriffe

Zielsetzung
Revisionssichere Nachvollziehbarkeit der Arbeit aller Protokollzugriffe
Protokollierungszeitpunkt / Vorhaltefrist
Die Protokollierung erfolgt zu jedem lesenden Zugriff auf die Protokolldatei und Anmeldeprotokoll. Vorhaltefrist: 3 Monate
Protokollierungsinhalt
Anmeldekennung, gewählte Filter- und Selektionskriterien zum Zugriff auf das Protokoll
Protokollzugriff
Technische Leitstelle (für Stufe 1 im Auftrag der datenverarbeitenden Stelle, für Stufe 2 im Auftrag des HR IT-AG) anlassbezogen und anlassunabhängig (Auswertung „Benutzerprotokoll“)
Filterung des Protokollzugriffs
Zur besseren Handhabung des Zugriff können Protokolldaten systemisch gefiltert ausgegeben werden: • Filter auf anzuzeigenden Zeitraum • Filter auf Benutzernamen (Anmeldekennung)

3.5 Technische Protokollierungen

Zielsetzung
Monitoring, Nachweis der Administration des Verfahrens
Protokollierungszeitpunkt, Vorhaltefrist
Start und Ende technischer Jobs (Jobsteuerung) sowie das Betriebshandbuch, Vorhaltefrist: 6 Jahre nach Abschluss des Haushaltsjahres für die der Job/die Systemänderung zahlungsrelevant[4] ist (Nr. 7.1 der Anlage 5 zu Nr. 4.7 der VV-ZBR), Rest 3 Monate
Protokollierungsinhalt

[4] Dieser Zeitraum umfasst insbesondere die Zahlungsrelevanz der in der Systemumgebung verarbeiteten Daten.

Nachweis der durchgeführten Tätigkeiten:

- Betriebshandbuch/Verfahrensdokumentation: Durchgeführte Änderungen an der Systemkonfiguration (Beginn, Ende, Beteiligte Mitarbeiter, Art der Änderung, z. B. Release bereitgestellt, Patch etc.)
- Durchgeführte Datensicherungen gemäß SLA über eigene Gruppe bei Dataport im Bereich Technik (Datum, Verantwortlicher Mitarbeiter, Bandnummer, Ablageplatz)
- Ungewöhnliche Systemereignisse, mit Hilfe des Incidentmanagementtools Remedy (Datum, System, Ereignisbeschreibung)
- Protokollierung von Datenübertragungen (Datum, Quellsystem, Zielsystem, Übertragungsstatus, Inhalt der Übertragung)
- Zu den Datenübertragungen gehören:
    - Transportaufträge, die mit Hilfe Verteiltool durchgeführt werden. Diese sind in in-Step sowie LOG Dateien des Verteiltool dokumentiert. Die Dateien liegen in der KoPers Umgebung und unterliegen den „normalen“ Sicherungsprozessen;
    - Manuelle Transportaufträge von einer in eine andere KoPers Umgebung werden als Change in unserem Changemanagementtool Remedy erfasst und protokolliert;
    - Filetransfer von KoPers Dateien aus der KoPers Area zu Fremdsystemen werden mittels der Filetransfersoftware openFT durchgeführt. Diese Software erstellt im Rahmen des FT-Prozesses ebenfalls Protokolle und LOGs, diese liegen in der KoPers Umgebung und unterliegen den „normalen“ Sicherungsprozessen (vgl. Abschnitt 3)

Protokollzugriff

Technische Leitstelle (für Stufe 1 im Auftrag der datenverarbeitenden Stelle, für Stufe 2 im Auftrag des HR IT-AG)anlassbezogen und anlassunabhängig funktional zu trennen von der Durchführung der kontrollierten Tätigkeiten.

Filterung des Protokollzugriffs

Zur besseren Handhabung des Zugriff auf die einzelnen Protokolle ist eine systemische Filterung möglich:

- Filter auf anzuzeigenden Zeitraum
- Filter auf Benutzernamen (Anmeldekennung) und IP-Adresse

Besonderheit

Die Form der Protokollierung hängt von den Inhalten ab:

- Administrationsaktivitäten/Durchgeführte Änderungen an der Systemkonfiguration im Betriebshandbuch
- Durchgeführte Datensicherungen im Betriebshandbuch
- Ungewöhnliche Systemereignisse im Monitoring-Werkzeug (z. B. Nagios)
- Metainformationen zu Schnittstellenläufen als LOG-Dateien
- Inhalt von Datenübertragungen als LOG-Dateien

Grundsätzlich ist sicherzustellen, dass die kontrollierte Tätigkeit funktional zu trennen ist von der Kontrolle.

3.6 Rollen-Berechtigungsliste

Zielsetzung

Auswertung der im Verfahren eingerichteten Berechtigungen. Zweck ist die Prüfung der im KoPers Zugriffsmanagement eingerichteten Berechtigungen und Abgleich mit dem definierten SOLL

Protokollierungszeitpunkt / Vorhaltefrist

Kein Protokoll im eigentlichen Sinn; Auswertung die zum Prüfzeitpunkt aus dem System erzeugt wird, entsprechend keine Vorhaltefrist

Auswertung: BER Profil/Benutzer
Profil-Nummer
Profil-Name
Profil-Kommentar
Benutzer-Nummer
Benutzer-Kennung
Benutzer-Name
Benutzer-Funktion
Aktiv Datum
Fehllogins
Rest Gültigk. Dauer
Gruppennummer
Aendern Datum
Aendern Benutzer-Name
Aendern Profil-Name
Benutzer-Kommentar

Auswertung: BER Profil/Formate
Format-Art
Profil-Nummer
Profil-Name
Format-Nummer
Format-Name
Abruf-Berechtigung
Bearbeit-Berechtigung

Auswertung: BER Benutzergruppen
Benutzergruppen-Nummer
Benutzergruppen-Name
Benutzergruppen-Kommentar
Benutzer-Nummer
Benutzer-Kennung
Benutzer-Name
Benutzer-Funktion
Aktiv Datum
Fehllogins
Rest Gültigk. Dauer
Gruppennummer
Aendern Datum
Aendern Benutzer-Name
Aendern Profil-Name
Benutzer-Gesperrt
Benutzer-Kommentar

Protokollierungsinhalt

Eingerichtete Benutzerkennungen mit den zugeordneten Profilen. Berechtigungen der Profile für die einzelnen Formate (z. B. Masken, Auswertungen etc.) sowie eingerichtete Benutzerkennungen mit Benutzergruppen.

Protokollzugriff

Fachliche Leitstelle, für Stufe 1 im Auftrag der datenverarbeitende Stelle: anlassbezogen und anlassunabhängig

Filterung des Protokollzugriffs
• Ausgabe in Excel mit den verbundenen Filtermöglichkeiten • Filter auf Daten einer datenverarbeitenden Stelle (Org-Einheit)
Besonderheit
Die Profil-Berechtigungsliste wird im Zuge der anlassbezogenen und anlassunabhängigen Kontrolle der Berechtigungen erzeugt. Hierzu wird die Rolle mit den im System eingerichteten IST-Berechtigungen gegen die in der FL vorgehaltenen Dokumentation der SOLL-Berechtigungen geprüft und Abweichungen dargestellt. Darüber hinaus kann eine Liste erzeugt werden über alle Änderungen (alter und neuer Wert) in Profilen und Berechtigungen. Die Auswertung dient darüber hinaus der Bereinigung nicht mehr benötigter Profile.

Profil	Profil-Name	Profil-Kommentar	Benutzer-I	Benutzer-Kenn	Benutzer-Name	Benutzer-Funktion	Aktiv Datum	Fe	Res	Grup	Aendern Dat	Aendern Benut	Aendern Profil-Name
029	ADM_AUSWE	Erstellung und Einbindung von Au	000305			Dataport	16.01.2014	9	372	000	21.07.2014		ADM_BENUTZER
			000054				08.07.2014	0	545	000	09.09.2014		PUI_SYSTEM
			000069				14.09.2015	0	978	000	21.07.2014		ADM_BENUTZER
			000120			ZPD 34	16.06.2015	0	888	000	04.09.2015		ADM_BENUTZER
			000121			HR Systemhaus	28.07.2014	0	565	000	29.08.2014		ADM_BENUTZER
			000304				15.11.2013	0	310	000	21.07.2014		ADM_BENUTZER
			000285			ZPD 6	29.10.2011	0	0	000	24.07.2014		ADM_BENUTZER
			000089			HR Systemhaus	30.07.2014	0	567	000	21.07.2014		ADM_BENUTZER
030	ADM_BENUTZ	Administrationsprofil für das Anle	000436			ZPD 36	16.04.2015	0	827	000	29.05.2015		ADM_BENUTZER
			000240			HR Systemhaus	27.06.2014	0	534	000	21.07.2014		ADM_BENUTZER
			000146			HR Systemhaus / ZPD 33	25.06.2015	0	897	000	25.06.2015		ADM_BENUTZER
			000199			ZPD ePers TP Technik	05.07.2012	0	0	000	31.03.2015		ADM_BENUTZER
			000113				17.09.2015	0	981	000	03.03.2015		ADM_BENUTZER
			000248			HR Systemhaus	03.09.2014	0	602	000	03.09.2014		ADM_BENUTZER
			000307			HR Systemhaus / ZPD 33	25.06.2015	0	897	000	25.06.2015		ADM_BENUTZER
			000275			ZPD 36	17.03.2015	0	797	000	12.03.2015		ADM_BENUTZER
			000117			HR Systemhaus / ZPD 33	28.09.2015	0	992	000	25.06.2015		ADM_BENUTZER
088	ADM_BEN_PR	Benutzerverwaltung auf Produktio	000436			ZPD 36	16.04.2015	0	827	000	29.05.2015		ADM_BENUTZER
			000199			ZPD ePers TP Technik	05.07.2012	0	0	000	31.03.2015		ADM_BENUTZER
			000113				17.09.2015	0	981	000	03.03.2015		ADM_BENUTZER
			000307			HR Systemhaus / ZPD 33	25.06.2015	0	897	000	25.06.2015		ADM_BENUTZER
086	ADM_DATAPC	Profil für DP-Mitarbeiter der Technischen Leitstel											
087	ADM_DP_PRC	Profil für DP-Mitarbeiter in Produk	000012	DP_Reltest	DP_Reltest		09.01.2013	0	0	000	05.10.2015	peinth	ADM_BENUTZER
031	ADM_KATALO	Erstellung und Einbindung von Ka	000054				08.07.2014	0	545	000	09.09.2014	aharwart	PUI_SYSTEM
			000069				14.09.2015	0	978	000	21.07.2014	schachho	ADM_BENUTZER
			000121			HR Systemhaus	28.07.2014	0	565	000	29.08.2014	horstmjo	ADM_BENUTZER
			000310			ePers TP Test	19.12.2014	0	709	000	19.12.2014	horstmjo	ADM_BENUTZER
			000126			HR Systemhaus	22.05.2015	0	863	000	21.05.2015	horstmjo	ADM_BENUTZER

Abbildung 5: Abbildung BER Profil/Benutzer

3.7 Bearbeitungsschritte in den Geschäftsfallmasken

Die in einem Geschäftsfall durch unterschiedliche Sachbearbeiter im Laufe der Zeit an den Daten vorgenommenen Änderungen werden protokolliert. Sie sind aus dem Geschäftsfall heraus aufrufbar und weisen die Informationen / Felder der Protokolldatei auf. Es greift das KoPers Berechtigungskonzept, so dass nur Protokollinformationen zu Daten eingesehen werden können, für deren lesenden Zugriff die Sachbearbeiter selbst berechtigt sind. Eine automatische Auswertbarkeit ist nicht gegeben. Für Hamburg ist über die Protokollierung in der Protokolldatei hinausgehend die Protokollierung am Geschäftsfall nicht vorgesehen.

Wichtig ist die Abgrenzung der hier beschriebenen Protokollinformationen im Vergleich zu **historischen Daten im Datenmodell**:

Während historische Daten im Datenmodell fachliche Informationen mit Zeitbezug liefern (z. B. welche Kontoverbindung war zu welchem Zeitpunkt die zu verwendende), liefern Protokollierungsinformationen Aussagen darüber wie die fachlichen Informationen mit Zeitbezug im System entstanden sind (z. B. wer hat wann welche Informationen über ein zu einem Zeitpunkt zu verwendendes Konto eingegeben).

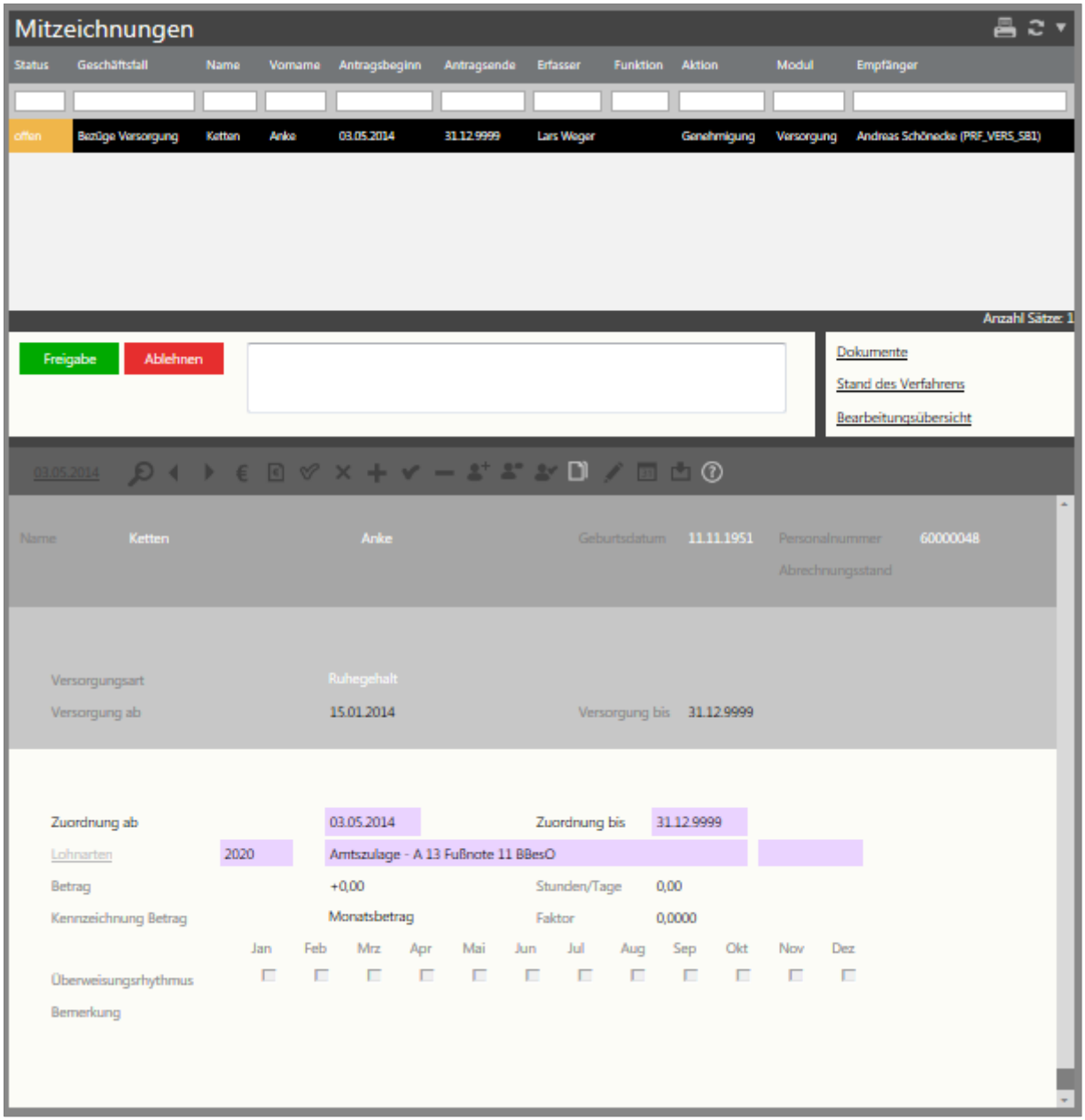
3.8 Bearbeitungsschritte in der Workflowengine

Die Statusverfolgung einer Mitzeichnung erlaubt das Nachvollziehen der einzelnen Bearbeitungsschritte mitsamt der Änderungen (alter und neuer Feldinhalte), die Mitarbeiter im Rahmen des Mitzeichnungsverfahrens getätigt haben. Die Statusverfolgung geht aus den folgenden Screenshots hervor, in denen die Erteilung einer Amtszulage gezeichnet wird und

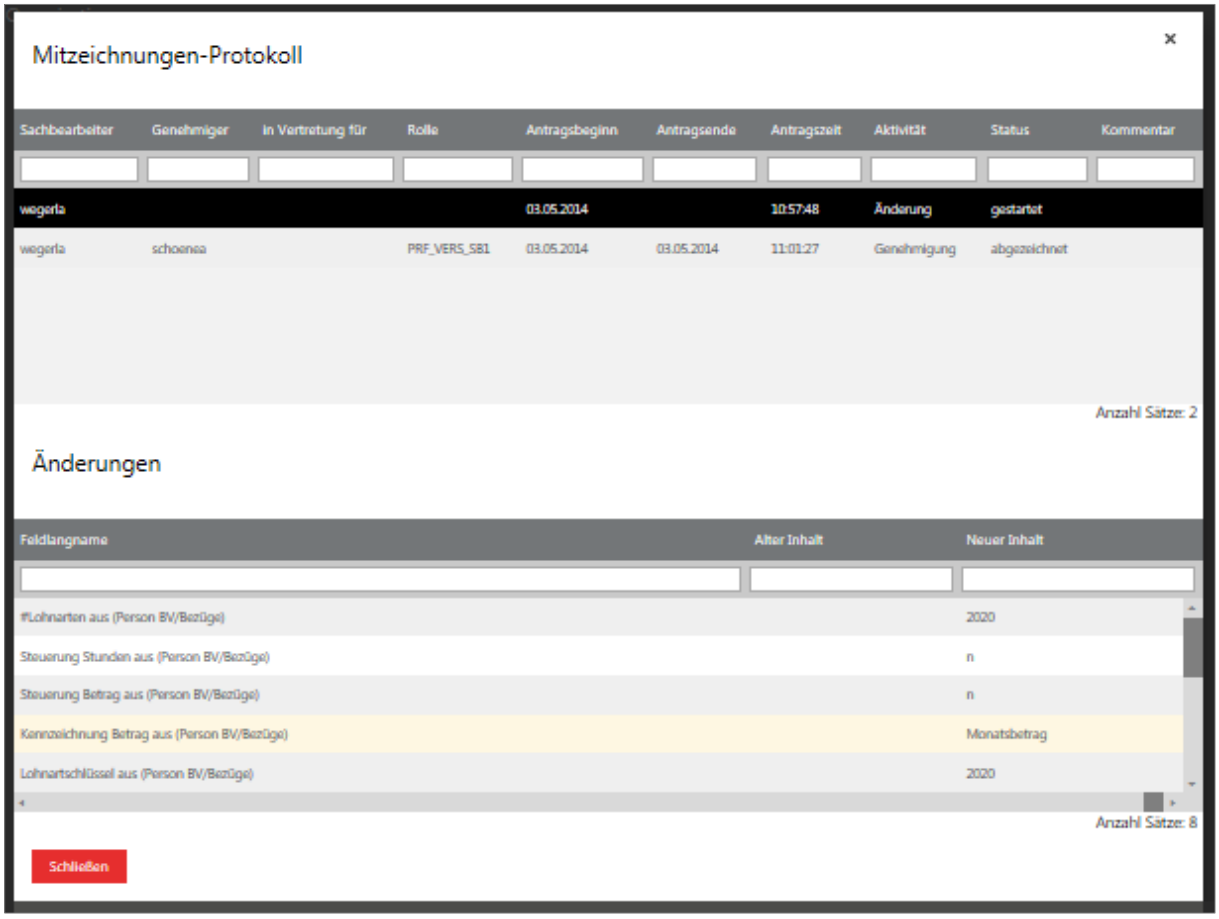
anschließend aus dem Protokoll hervorgeht. Es muss jederzeit erkennbar sein, wer mit dem Bescheinigungsfenster „sachlich und rechnerisch richtig“ gezeichnet hat und wer über die Mitzeichnung kassenrechtlich angeordnet hat.

Da auch diese Informationen nur über den Einzelfall zugänglich sind, unterliegen sie dem KoPers Rollen und Berechtigungsmodell. Eine automatische Auswertbarkeit ist nicht gegeben. Insbesondere werden die erfassten Uhrzeiten nicht zur Leistungsmessung- oder Kontrolle herangezogen.

Prüfung einer Mitzeichnung:



Anschließendes Mitzeichnungsprotokoll:



Die Protokollierung „Änderung“ hält den Sachverhalt fest, dass ein Sachbearbeiter, wie oben beschrieben, die Daten auf sachliche Richtigkeit geprüft hat. Der Eintrag „Genehmigung“ hält den Sachverhalt fest, dass ein Prüfer die Daten geprüft und für Korrekt erachtet hat und die Anordnung erfolgt ist. Das Mitzeichnungsprotokoll wird nur an Geschäftsfällen mit aktivierter Mitzeichnung erstellt. Es handelt sich dabei um die im Konzept Stichprobenverfahren mit einem Prüfworkflow hinterlegten Geschäftsfälle.

Zielsetzung
Revisionssichere Nachvollziehung der Zahlungsanordnung
Protokollierungszeitpunkt / Vorhaltefrist
Mit jedem Speichervorgang in KoPers, 6 Jahre nach Abschluss des Haushaltsjahres, der Wirksamkeit der Änderung bzw. für das die Unterlagen bestimmt sind.[5](Nr. 7.1 der Anlage 5 zu Nr. 4.7 der VV-ZBR),
Protokollierungsinhalt
Personal- und Vertragsnummer, Datum, Uhrzeit, Benutzer- oder Systemkennung, Geschäftsfall, Art der übernommenen kassenrechtlichen Verantwortung (wer mit dem Bescheinigungsfenster „sachlich und rechnerisch richtig“ gezeichnet hat und wer über die Mitzeichnung kassenrechtlich „angeordnet“ hat)
Protokollzugriff
Der Zugriff erfolgt durch die Anwender über einen Geschäftsfall. Der Zugriff erfordert das vorherige Laden eines Datensatzes und erlaubt nur Einblick in die geänderten Informatio-

[5] Das kann bei einer zur Einstellung erfassten IBAN bedeuten, dass die kassenrechtliche Verantwortung 6 Jahre nach der Beendigung der Bankverbindung protokolliert sein muss.

nen des geladenen Geschäftsfalls.
Filterung des Protokollzugriffs
Alle angezeigten Spalten können gefiltert und sortiert werden.

3.9 Protokollierung der Migration

Die Protokollierung der Datenmigration von PAISY nach KoPers ist nicht Gegenstand dieses Konzeptes. Sie wird im Rahmen der Kassendokumentation (Verfahrensdokumentation gemäß Anlage 10 zu den VV-ZBR) sowie im P&I Migrationskonzept dargestellt.

4 Technische Anforderungen an die Protokollierung

- Es ist sicherzustellen, dass die Zeitstempel aller an der Protokollierung beteiligten Systeme synchronisiert sind. Alle in RZ² und an KoPers beteiligten Server nutzen hierfür einen zentralen NTP Dienst. Damit sind sämtliche Zeiten und Uhren synchronisiert.

- Sämtliche aufeinander zugreifenden Teile (Maschinen, Applikationen, Personen) des gesamten Systems müssen einander vertrauen bzw. einander identifizieren. Alle an KoPers beteiligten Server und alle zugreifenden Accounts (Personen und Dienste), Ausnahme Useraccounts innerhalb der Fachanwendungen, sind Mitglieder einander vertrauender Domänen und werden hierfür über die Domaincontroller authentifiziert.

- Protokollinformationen müssen vor einer nachträglichen Änderung geschützt sein (z. B. Schutz durch Signatur); KoPers Protokolle (vgl. 2.1, 2.2, 2.3 und 2.4) werden aus diesem Grund zentral innerhalb der KoPers Datenbank verschlüsselt über Oracle TDE abgelegt. Ein lesender Zugriff ist nur unter der KoPers Berechtigungssteuerung (Zugriffsmanagement) möglich;

- Sämtliche KoPers Job-Aufrufe der technischen Leitstelle werden von Spring Batch in der Administrations-Plattform protokolliert;

- Die zeitliche und prozessbezogene Steuerung der KoPers-Jobs wird über ein Programm namens Control-M abgewickelt. In Control-M werden Protokolle in der Control-M Datenbank 30 Tage lang aufbewahrt. In Control-M werden keine personenbezogene Daten verarbeitet, dort werden lediglich Prozesse der Jobsteuerung für PuI Plus gesteuert;

- Weiterhin erfolgt eine Protokollierung der openFT-Jobs, wenn Schnittstellen verschlüsselt von A nach B übertragen werden. Die Protokolle werden für eine unbestimmte Zeit aufbewahrt. Die log-Datei ist durch die Berechtigung so geschützt, dass sie nur durch das System (openFT) und keine Benutzer modifiziert werden kann;
- Dem Berechtigungskonzept folgend werden nur personenbezogene Kennungen verwendet. Damit ist sichergestellt, dass der Nutzer tatsächlich derjenige ist, für den die Protokoll-Einträge erfolgen (Authentisierung);

- Die ordnungsgemäße Funktion des Protokollierungsverfahrens und die Gültigkeit von Protokolldaten werden durch geeignete Tests der Fachlichen Leitstelle im Rahmen der Testzyklen sichergestellt. Diese Tests erfolgen insbesondere, wenn die protokollierenden

Systeme oder Systemteile verändert werden. Für die Freigabe von KoPers sind derzeit folgende Testfälle in Verbindung mit der Protokollierung vorgesehen:

- TST-000069 Kasse - Migration - Protokollierung Altdatenübernahme
- TST-000112 Protokollierung - Zugriff auf Protokolldateien (KP-001298)
- TST-000161 Migration - Protokollierung der Benutzerkennung 'Migration'
- TST-000242 Protokollierung - Protokollinformationen dürfen nach Erstellung nicht mehr verändert werden können
- TST-000243 Protokollierung - Inhalt, Filterung und Sortierung von Protokollen
- TST-000244 Protokollierung - Protokollierung des Zugriffs auf Protokolle
- TST-000245 Protokollierung - Protokollierung von Schnittstellenläufen
- TST-000246 Protokollierung - Rückstandsloses Löschen von Protokolleinträgen
- TST-000248 Protokollierung - Protokollierung der Migration
- TST-000291 Protokollierung - Abgleich der Migrationsprotokolle gegen PAISY (Abrechnung und Verwaltung)
- TST-000292 Protokollierung - Abgleich der Migrationsprotokolle gegen KoPers Felder (Abrechnung und Verwaltung)
- TST-000293 Protokollierung - Abgleich der Migrationsprotokolle gegen eine in KoPers durchgeführte Abrechnung
- TST-000294 Protokollierung - Revisionsfähigkeit und Manipulationssicherheit des Migrationsprozesses

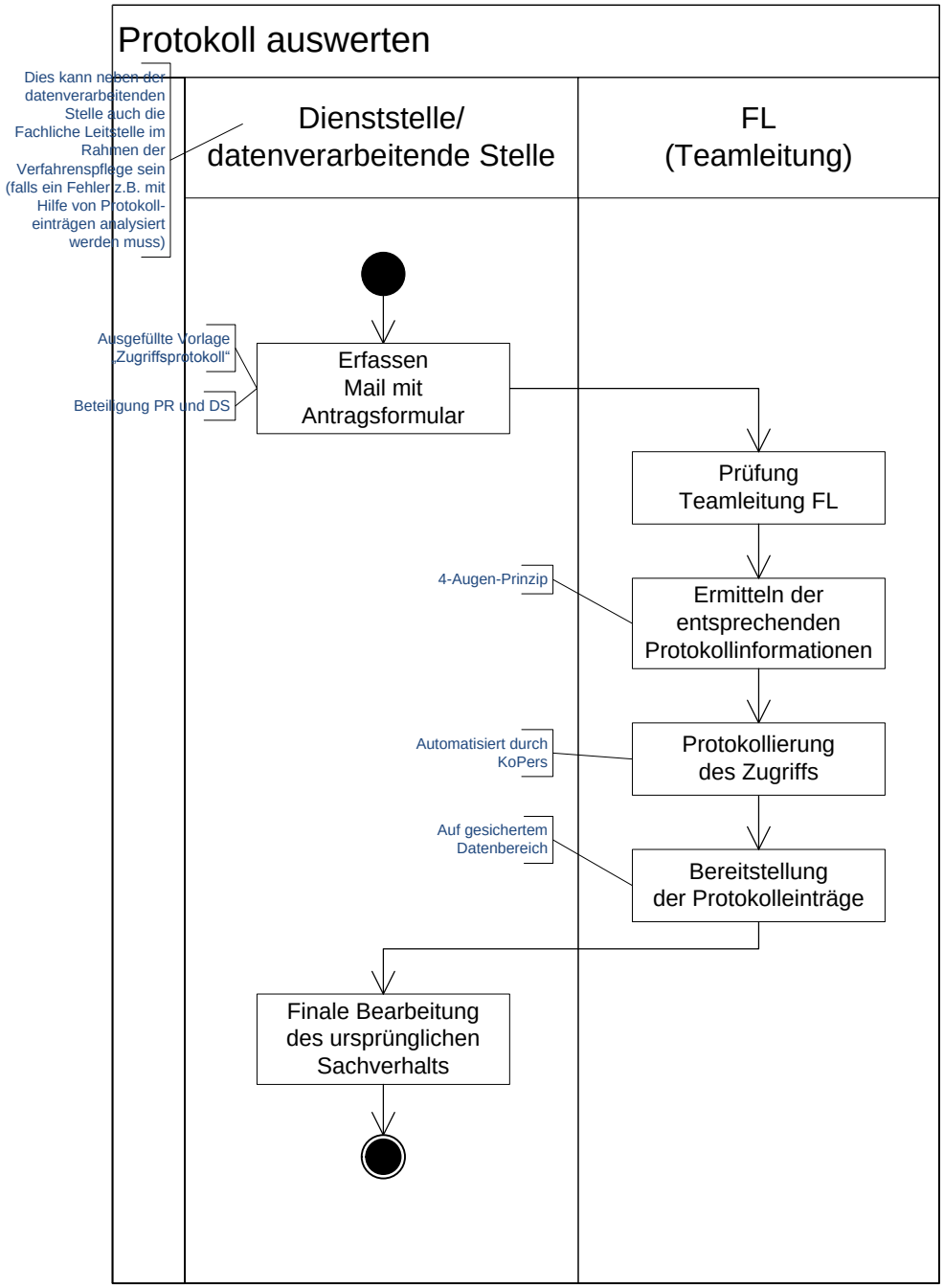
5 Zugriff auf Protokollinformationen

Der Zugriff auf Protokolldaten erfolgt entweder anlassbezogen oder nicht anlassbezogen. In jedem Fall ist der Einblick in Protokolldaten – je nach Protokollart – nur einem ausgewählten

Nutzerkreis der Technischen oder Fachlichen Leitstelle, Revisoren und der datenverarbeitenden Stelle möglich. Die Berechtigten mit Zugriff auf Protokollinformationen aus der Fachlichen Leitstelle werden gemäß der aktuell gültigen Freigaberichtlinie durch den IT-Beauftragten des ZPD benannt. Die Berechtigten mit Protokollzugriff auf Seiten des Dienstleisters Dataport werden durch Dataport benannt. Die Berechtigten mit Protokollzugriff auf Seiten der datenverarbeitenden Stellen werden durch diese benannt. Im Verfahren KoPers wird zum Zugriff durch die Fachliche Leitstelle ein eigenes Berechtigungsprofil, welches ausschließlich den Zugriff auf das Berechtigungsprotokoll erlaubt, erstellt (ADM_PROTOKOL). Gemäß Nr. 7.4 Anlage 10 VV-ZBR werden Berechtigungen (z. B. eine vordefinierte Prüferrolle) eingerichtet, die durch direkte Zuordnung zu einer Person einen lesenden Zugriff auf alle Daten und Systemeinstellungen des IT-Verfahrens ermöglichen (z. B. Revisoren, Rechnungshof).

5.1 Anlassbezogene Auswertung

Für den anlassbezogenen Zugriff auf **fachliche Protokolle** (in Kapitel 2 mit Zugriff durch die Fachliche Leitstelle gekennzeichnet, die Protokollierung der Bearbeitungsschritte an Geschäftsfallmasken und der Workflowengine gehört nicht hierzu) greift der nachfolgende Prozess.



Die eigentliche Auswertung personenbezogener oder zahlungsrelevanter Protokolldaten sollte unter Beachtung der personalrechtlichen Beteiligungspflichten und unter Einbeziehung des jeweils zuständigen behördlichen Datenschutzbeauftragten erfolgen. Ausgenommen hiervon ist die Verwendung für die Wahrnehmung von Aufsichts- und Kontrollbefugnissen sowie der Rechnungsprüfung nach § 13 Abs. 3 HmbDSG.

In den übrigen Fällen wird das Antragsformular zum Einblick in die Protokolldaten neben dem lokal zuständigen Anwendungsbetreuer auch durch den behördlichen Datenschutzbeauftragten gezeichnet. Die Protokollinformationen werden durch die Fachliche Leitstelle ausgewertet. Zugriffe auf Protokollinformationen erfolgen im 4-Augen-Prinzip innerhalb derFachlichen LeitstelleBeide Beteiligte unterschreiben hierzu auf dem Antragsformular. Werden personenbezogene oder zahlungsrelevante Protokolldaten durch die Anwendungsbetreuer bzw. Auftraggeber in den Dienststellenbenötigt so wird individuell ein sicherer Übertragungsweg vereinbart. Der anlassbezogene Zugriff auf **technische Protokolle** erfolgt schrift-

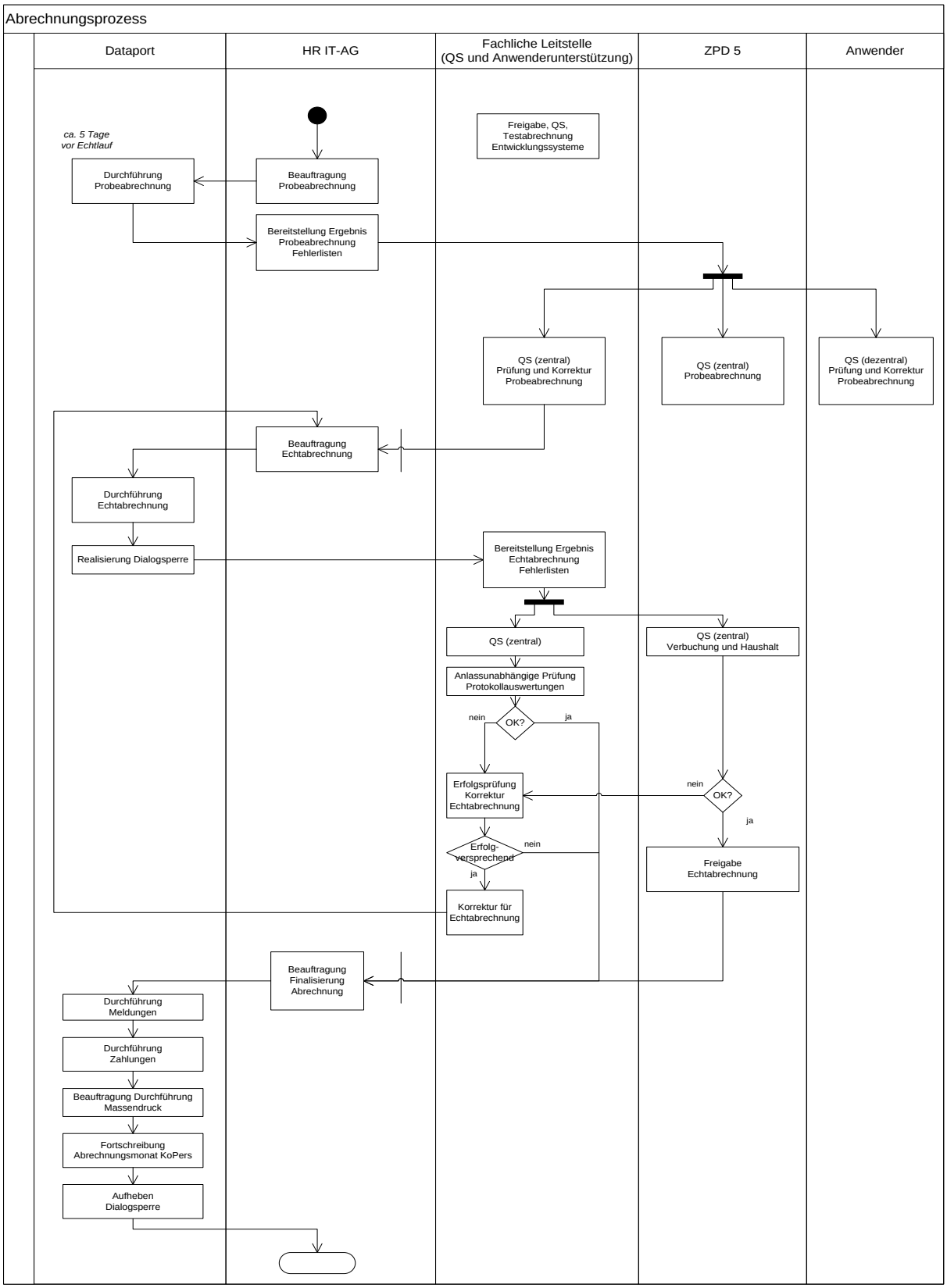
lich gegenüber Dataport. Der Auftrag ist durch eine durch den IT-Beauftragten des ZPD autorisierte Person zu zeichnen (Auftragsmanagement des ZPD).

Von dem beschriebenen Prozessablauf kann bei Prüfungen durch den Rechnungshof im Einvernehmen mit dem behördlichen Datenschutzbeauftragten abgewichen werden. In diesem Fall ist eine schriftliche Vereinbarung erforderlich in der die Protokolle, der Benutzerkreis und die Zeitdauer vereinbart wird, in der der genannte Personenkreis Zugriff auf die genannten Protokolle erhält. Die Vereinbarung ist vom Antragsteller (Rechnungshof) einer durch den IT-Beauftragten autorisierten Person, sowie dem behördlichen Datenschützer zu zeichnen.

5.2 Nicht anlassbezogene Auswertung

Im Rahmen der monatlichen Abrechnungsprüfung werden durch die Fachliche Leitstelle die im Anhang nicht abschließend beschriebenen nicht anlassbezogenen Prüfungen der Protokollinformationen durchgeführt. Die Prüfung dient dem Zweck, die monatliche Abrechnung in Bezug auf möglichen Missbrauch zu untersuchen.

Die Prüfungen erfolgen durch Ausführung der im Anhang aufgelisteten Auswertungen und Prüfung darin enthaltener Anhaltsmomente. Die Einbettung in den Abrechnungsprozess ist im Folgenden dargestellt. Dieser Abrechnungsprozess bleibt unverändert im ZPD und wird im nachfolgenden Screenshot dargestellt:



Die Ergebnisse der nicht anlassbezogenen Auswertungen werden ausschließlich ohne schützenswerte Inhalte abgelegt (z. B. „Anmeldeprotokolle wurden am XX.XX.XXXX durch XXX geprüft). Sollten sich aus der nicht-anlassbezogenen Prüfung Verdachtsmomente ergeben, werden die Protokolle bis zum Abschluss des Verfahrens aufbewahrt. In diesem Fall wird die technische Leitstelle mit der Vorhaltung beauftragt.

5.3 Löschen von Protokollinformationen

Für das Löschen von Protokollinformationen gelten die Aussagen des Löschkonzeptes.

6 Anhang Protokollauswertungen

Für die nicht anlassbezogene Prüfung der KoPers Protokolle werden Auswertungen zur Verfügung gestellt. Diese liefern Informationen über:

- Häufige nicht erfolgreiche Anmeldeversuche in einem Zeitraum von einer IP
  (> 100 an einem Tag)
- Häufige Änderungen an einem Personalfall in unterschiedlichen Geschäftsfällen durch einen Sachbearbeiter (Ausgenommen Neuzugänge)
  (> 100 in einer Woche)
- Änderungen an einem Personalfall vor einem Abrechnungslauf und Widerherstellen der Änderungen nach einem Abrechnungslauf durch den gleichen Sachbearbeiter
- Prüfung Vergebene Berechtigungen (Rollen-Berechtigungsliste) gegenüber den in der Fachlichen Leitstelle dokumentierten Berechtigungen.
  (manuelle Prüfung)

Die Einbettung in den Abrechnungsprozess ist in der Abbildung 5 (Seite 30) dargestellt.

7 Quellen

Orientierungshilfe „Protokollierung“
Herausgegeben vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
Stand 02. November 2009