KoPers

Verfahrensbeschreibung und Risikoanalyse

Anlage 1

Inhaltsverzeichnis

1 Verfahrensbeschreibung nach § 9 HmbDSG

1.1 Verarbeitende Stelle

Name und Anschrift der Daten verarbeitenden Stellen:

Behörden, Ämter, Hochschulen und Landesbetriebe der Freien und Hansestadt Hamburg

1.2 Verfahren

Bezeichnung

KoPers – Kooperation zur Neuausrichtung der IT-Unterstützung von Personalmanagementaufgaben in der FHH und in SH – Einführung des neuen Personalmanagementsystems KoPers durch die Firma P&I in der Personalverwaltung für die Freie und Hansestadt Hamburg.

Zweckbestimmung

Bewirtschaftung der Tarifbeschäftigten und Beamten der oben genannten Einrichtungen, Abrechnung und Zahlbarmachung der Gehälter und Bezüge, Abführung von Sozialversicherungsbeiträgen und Steuern, Pfändungssachbearbeitung, Sachbearbeitung der Familienkasse und Nachversicherung sowie das Führen und Übermitteln gesetzlich vorgegebener Statistiken an die zuständigen Stellen.

1.3 Daten und Rechtsgrundlage

Art der verarbeitenden Daten

Daten zur Person der Tarifbeschäftigten und Beamten, sowie deren Ehepartnern und Kindern; Daten zur Sozialversicherung, Steuerdaten und weitere abrechnungsrelevante Daten; Daten im Rahmen des gesetzlichen Meldewesens; verbuchungsrelevante Daten; Arbeitgeberdaten; Pfändungsdaten. Die einzelnen Daten sind im Datenkatalog aufgeführt.

Rechtsgrundlage

§ 85 Abs.1 HmbBG i. V. m. § 28 Abs. 2, 3 HmbDSG

1.4 Kreis der Betroffenen

Alle Tarifbeschäftigten und Beamten der Freien und Hansestadt Hamburg. Auch deren Familienangehörige können betroffen sein (z. B. bei der Beihilfe, Gewährung familienbezogener Bezügebestandteile, Festsetzung Kindergeld).

1.5 Empfänger/innen der Daten

Empfangende dritte Stellen

Familien- und Sozialgerichte, Gläubiger, Sozialversicherungen, Krankenkassen, Kasse Hamburg, Finanzämter, ZfA/Riester, Institutionen für vermögenswirksame Leistungen, Hamburger Verkehrsverbund. ZPD für Zwecke der Abrechnung von Dienstleistungen, der Erstellung von Auswertungen und Berichten, Versicherungsmathematiker für die Erstellung versicherungsmathematischer Rückstellungsgutachten

Auftragsdatenbearbeitung

Dataport verarbeitet Daten im Auftrag nach § 3 HmbDSG (u. a. dadurch, dass von Dataport einen Großteil der Technik für die Verarbeitung zur Verfügung gestellt wird).

Andere Empfänger/innen
Empfänger/innen innerhalb des ZPD, die andere Aufgaben wahrnehmen: Beihilfe, Pfändung, Familienkasse, Haushalt, Nachversicherung, Dienstunfallbearbeitung.

1.6 Datenübermittlung

Datenübermittlung nach § 17 Abs. 2 und 3 HmbDSG (Übermittlung an Drittländer): Keine.

1.7 Fristen

Fristen Datensperrung
Fristen für die Sperrung der Daten: Keine.

Fristen Datenlöschung
Fristen für die Löschung der Daten: Siehe Löschkonzept

1.8 Technische und organisatorische Maßnahmen

Die einzelnen technisch-organisatorischen Maßnahmen sind in der Risikoanalyse aufgeführt.

1.9 Geräte und weitere Verfahren

Art der Geräte
Die Art der Geräte ist bei den technisch-organisatorischen Maßnahmen in der Risikoanalyse aufgeführt.

Weitere Verfahren
Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benachrichtigung.

Zur Löschung und Sperrung wird auf das Löschkonzept verwiesen, zur Datenübermittlung auf die Risikoanalyse.

Auskunftserteilung: Auskünfte nach § 18 HmbDSG erteilen die Personalbereiche der Behörden und Einrichtungen der FHH.

2 Risikoanalyse

Das Verfahren KoPers wird in den Behörden, Ämtern, Hochschulen und Landesbetrieben der Freien und Hansestadt Hamburg eingeführt. Die von jeder datenverarbeitenden Stelle im Rahmen dieser Risikoanalyse bereitzustellenden Unterlagen, werden als Anhang zu dieser Risikoanalyse aufgenommen.

2.1 Beschreibung der Soll-Prozesse

Die Produktivsetzung in KoPers hat die Ablösung des Altsystems PAISY für oben genannte Funktionalitäten zum Ziel. Dies beinhaltet die folgenden Prozesse, die in allen datenverarbeitenden Stellen angeboten werden:

- Migration der Daten der Freien und Hansestadt Hamburg aus PAISY nach KoPers.
- Laufende Bewirtschaftung der Personalfälle in dezentralen Personalprozessen:
  - Arbeitszeit
  - Ausscheiden
  - Beurlaubung Freistellung und Rückkehr

- Beurteilung
- Disziplinarverfahren
- Einstellung
- Eingruppierung
- Ernennung
- Fehlzahlungen
- HVV-GKA
- Jubiläum
- Krankheitszeiten und Kur
- Nebentätigkeit
- Personalmanagement
- Riester
- Ständige Be- und Abzüge
- Stammdatenänderung
- Unständige Bezüge
- Umsetzung/Versetzung/Abordnung
- Vertragsverlängerung
- Vermögensbildung
- Vorschuss
- Wiedereintritt nach Unterbrechung

- Laufende Bewirtschaftung der Personalfälle in unterstützenden zentralen Personalprozessen, die im ZPD ausgeführt werden:
  - Nachversicherung
  - Fehlzahlung
  - Versorgungslastenteilungs-Staatsvertrag
  - Altersvorsorge
  - Familienkasse
  - Pfändung

- Durchführung der für die Personalabrechnung und -verwaltung erforderlichen Spezialaufgaben:
  - Monatliche Abrechnung der Entgelte und Bezüge sowie Abführung von Sozialversicherungsbeiträgen und Steuern
  - Bereitstellung von Zahlungsdateien und zahlungsbegleitenden Unterlagen
  - Gesetzliche Meldeverfahren (z. B. Riester Rente)
  - Zahlbarmachung der Entgelte und Bezüge
  - Kostenkontierungen, Verbuchung und Übermittlung in die ressourcensteuernden Verfahren
  - Bereitstellung von Daten für das Personalberichtswesen
  - Führen und Übermitteln gesetzlich vorgegebener Statistiken an die zuständigen Stellen
  - Umsetzung von Tariferhöhungen
  - Mitversteuerung/Mitversicherung für Beschäftigte mit mehreren Verträgen
  - Umgang mit Über- und Nachzahlungen
  - Rückläufer aus der monatlichen und täglichen Zahlung
  - Rückrechnungen innerhalb und außerhalb der KoPers-Historik
  - Erstattungs- und Vergleichsmitteilungen

In Vorbereitung auf die Produktivsetzung KoPers wird zur Herstellung der notwendigen Abrechnungsgenauigkeit der folgende Prozess monatlich bis zum Systemstart durchgeführt:

- Laufende Migration der Daten der Tarifbeschäftigten und Beamten der Freien und Hansestadt Hamburg von PAISY nach KoPers zum Zwecke der Abrechnung von Gehältern und Besoldungen.
- Im Einzelfall und in jeweiliger Abstimmung mit dem HmbBfDI Nutzung der Daten zur Durchführung von Tests – sofern eine Nutzung von Testdaten nicht möglich oder nur mit einem unverhältnismäßig hohen Aufwand möglich ist.

2.2 Art der verarbeiteten Daten

Werden personenbezogene Daten verarbeitet?

☒ ja ☐ nein

Welche Rechtsgrundlagen bestehen?
(Nennung der Gesetze und der einschlägigen Paragraphen)

§ 85 Abs. 1 HmbBG i. V. m. § 28 Abs. 2, 3 HmbDSG

Welche Daten werden verarbeitet?

Für die Kategorisierung und fachliche Einordnung der Daten wird auf den Datenkatalog verwiesen.

Kann der Umfang der verarbeiteten Daten reduziert werden? (vgl. § 5 Abs. 4 HmbDSG)

☐ ja (ggf. erforderliche Voraussetzungen) ☒ nein (Begründung)

Für die Erfordernisse der Bewirtschaftung bzw. Sachbearbeitung sind die im vorliegenden Datenkatalog aufgeführten Daten zwingend erforderlich.

Können personenbezogene Daten anonymisiert oder pseudonymisiert werden? (vgl. § 4 Abs. 9 und 10 HmbDSG)

☐ ja (Beschreibung) ☒ nein (Begründung)
Für die Erfordernisse der Bewirtschaftung bzw. Sachbearbeitung sind die Originaldaten zwingend erforderlich. Die Inhalte der unter 4.6 und 7.5 aufgeführten Statistiken sind grundsätzlich kumulativer Art. Ein Rückschluss auf Einzelpersonen ist ausgeschlossen.

Wurden bzw. werden die Betroffenen über die Erfassung ihrer personenbezogenen Daten informiert? (vgl. § 12 a HmbDSG)

☒ ja zu Beginn des Beschäftigungsverhältnisses

☐ nein

Woher kommen die Daten?
Wurden bzw. werden die Daten direkt bei den Betroffenen erhoben?

☒ ja ☐ nein

Wenn ja, in welcher Form?

Personalfragebogen manuell

Wenn keine Direkterhebung: Auf welchem Weg erfolgt die Datenübermittlung?

Fehlanzeige.

Werden Informationen/ Daten aus anderen IT-Anwendungen genutzt?

☒ ja Elektronische Zeitwirtschaftssysteme

Ist eine Altdatenübernahme erforderlich?

☒ ja ☐ nein

Migration der Daten aus PAISY nach KoPers

Der Umfang der Datenlieferung entspricht den in PAISY vorhandenen Daten für die Abrechnungsmonate.

Aus PAISY übernommen werden folgende Fallzahlen (Stand 01/2016):
Fallzahlen 44.274 Beamte, 37.518 Tarifbeschäftigte

Diese teilen sich wie folgt auf. Umstellung zum 01.04.2018:

Behörde	Anzahl Beamte	Anzahl Tarifbeschäftigte
Personalamt, Rechnungshof, HmbfDI	275	194
Senatskanzlei und Senatsämter	104	77
Behörde für Wissenschaft, Forschung und Gleichstellung	71	69
Behörde für Kultur und Medien	76	216
BASFI	610	1149
Behörde für Stadtentwicklung und Wohnen und Behörde für Umwelt und Energie	428	899
Behörde für Wirtschaft, Verkehr und Innovation	277	286
Finanzbehörde und Finanzbehörde/Steuerverwaltung	4301	717

Umstellung zum 01.07.2018:

Behörde	Anzahl Beamte	Anzahl Tarifbeschäftigte

Justizbehörde, Arbeitsgerichte, Sozialgerichte, Finanzgericht, Justizvollzugsanstalten, Amtsgerichte, Landgericht, Oberlandesgericht, Verwaltungsgericht, Oberverwaltungsgericht, Referendare am OLG, Staatsanwaltschaften	3726	2135
Behörde für Inneres, Amt für innere Verwaltung, Einwohnerzentralamt, Polizei, Feuerwehr, V., Wasserschutzpolizeischule, Feuerwehrakademie	11663	2329
Bezirksämter: Mitte, Altona, Eimsbüttel, Nord, Wandsbek, Bergedorf, Harburg	1691	5783

Umstellung zum 01.01.2019:

Behörde	**Anzahl Beamte**	**Anzahl Tarifbeschäftigte**
Bürgerschaft und LB ZPD	205	321
Behörde für Schule und Berufsbildung inkl. LB LHV	15793	6379
Behörde für Gesundheit und Verbraucherschutz	249	430
Hochschulen	1464	11326
Schulbau Hamburg, Hamburger Institut für berufliche Bildung, Landesbetrieb Erziehung u. Beratung und weitere Landesbetriebe	3065	4358
Landesbetrieb ZAF/AMD	41	107
Institut für Hygiene und Umwelt	19	312
Staats- und Universitätsbibliothek	59	216
Kasse.Hamburg, Hmb. Münze	148	126
Großmarkt	5	32
LB Rathaus-Service	2	45
Planetarium	2	12

Werden Daten an andere IT-Anwendungen bzw. Stellen übermittelt?

☒ ja, ohne automatisiertes Abrufverfahren ☐ ja, mit automatisiertem Abrufverfahren
☐ nein

Eine Datenübermittlung erfolgt im Rahmen der Meldeverfahren der Sozialversicherung, u. a.:

DEÜV

Die "Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung (kurz: Datenerfassungs- und -übermittlungsverordnung oder auch DEÜV)" umfasst die Erstellung monatlicher Meldungen an die Sozialversicherungsträger nach der Datenübermittlungsverordnung.

EEL

Seit dem 01. Juli 2011 ist es für Arbeitgeber bindend, die Entgeltbescheinigung zur Beantragung von Krankengeld, Verletztengeld, Übergangsgeld und Krankheit des Kindes sowie Mutterschaftsgeld elektronisch an die Krankenkasse zu übertragen (EEL). Damit Arbeitnehmer Entgeltersatzleistungen zügig und in korrekter Höhe erhalten, benötigt der Sozialversicherungsträger zeitnah die zur Berechnung erforderlichen Daten (z. B. Höhe des Arbeitsentgelts). Entgeltersatzleistungen sind z. B. Krankengeld, Kinderpflege-Krankengeld, Mutterschaftsfeld, Übergangsgelder etc. Darüber hinaus werden u. a. Informationen über Vorerkrankungszeiten (zur Prüfung der 6-Wochen Lohnfortzahlung) übermittelt.

AAG

Nach dem Aufwandsausgleichsgesetz (AAG) werden Arbeitgebern Aufwendungen für die Entgeltfortzahlung nach dem Entgeltfortzahlungsgesetz (EFZG) erstattet, sofern sie nicht mehr als 30 Arbeitnehmer beschäftigen. Weiterhin ist im AAG geregelt, dass alle Arbeitgeber die Aufwendungen zum Mutterschaftsgeld nach dem Mutterschutzgesetz (MuSchG) bzw. Entgeltfortzahlung im Beschäftigungsverbot durch die Einzugsstellen erhalten. Seit Januar 2011 sind diese Anträge zum Erstattungsverfahren nach EFZG und MuSchG zu erstellen und elektronisch an die Krankenkassen zu übermitteln. Im elektronischen Meldeverfahren werden die erforderlichen Informationen zur jeweiligen Arbeitsunfähigkeit, zum Beschäftigungsverbot, zum Mutterschaftsgeld-Zuschuss sowie Bankverbindungen, Name und Anschrift übergeben. Stornierungs- und Korrekturmeldungen werden ebenfalls abgesetzt.

Berufsständige Versorgungswerke

Berufsständige Versorgungswerke (BVE) sind Bestandteil der DEÜV (Anlage 5 der Gemeinsamen Grundsätze). Es handelt sich hierbei um ein Meldeverfahren für Beschäftigte, die anstelle der gesetzlichen Rentenversicherung in einer berufsständischen Versorgungseinrichtung Mitglied sind.

Elster/ELStAM – Steuern und elektronische Lohnsteuerkarte:
In Deutschland steuerpflichtige Arbeitgeber und Unternehmer sind gesetzlich verpflichtet, ihre Lohnsteueranmeldungen sowie die Lohnbescheinigungen ihrer Arbeitnehmer elektro-

nisch über das ELSTER-System abzuwickeln (vgl. BMF-Schreiben vom 16. November 2011, BStBl 2011 I S. 1063).

Mit dem Verfahren ELSTER werden die Lohnsteuer-Anmeldung und die Lohnsteuerbescheinigungsdaten an das Finanzamt maschinell und automatisiert übermittelt.

Im ELStAM Verfahren werden von den Finanzämtern die Daten der elektronischen Lohnsteuerbescheinigung an das Verfahren KoPers übertragen und hier eingelesen.

IdNr-Kontrollverfahren (Kindergeld)
Ab 1.1.2016 sind die an den Beschäftigten und dessen Kind vergebenen steuerlichen Identifikationsnummern (IdNr) gesetzlich vorgeschriebene Anspruchsvoraussetzung für das Kindergeld. Das Bundeszentralamt für Steuern (BZSt) unterhält hierzu ein verbindliches IT-Verfahren (IdNr-Kontrollverfahren Kindergeld), mit dem ungerechtfertigte Kindergeldzahlungen verhindert werden. Die Familienkassen sind verpflichtet daran teilzunehmen. Im Kontrollverfahren muss jede Familienkasse die Zuständigkeit für die von ihr bearbeiteten Kindergeldfälle unter Angabe der IdNr der Kinder an die IdNr-Datenbank des BZSt elektronisch melden. Weitere übertragene Daten (zur Ermittlung einer neuen IDNr) sind Name, Vorname, Geburtsdatum und Adressdaten.

Riester
Beamte und Empfänger von Besoldung und Amtsbezügen können gem. §10a EStG von der Riester-Rente profitieren, d. h. sie sind “riesterförderfähig“. Hierzu muss – nach schriftlichen Einwilligung zur Datenübermittlung durch den Beschäftigten – die FHH Daten mit der Zentralen Zulagenstelle für Altersvermögen (ZfA) austauschen. Die Datenübertragung dient der Ermittlung einer Zulagennummer für den förderfähigen Beschäftigten und im Anschluss der Übertragung der für die Ermittlung des Riester-Mindesteigenbeitrags und die Gewährung der Riester-Kinderzulage erforderlichen Daten.

Beihilfe-Permis-B: Beihilfe
Beamte (sowie einzelne Tarifbeschäftigte) der FHH haben entsprechend § 80 Absatz 11 HmbBG Ansprüche auf Beihilfezahlungen. Diese werden in dem Fachverfahren Permis-B geprüft und berechnet. Zuständig für den Betrieb von Permis-B ist ebenfalls das ZPD. Für die Prüfung und Berechnung der Beihilfe übermittelt das Verfahren KoPers an das Verfahren Permis-B die entsprechenden Stammdaten, sowie deren Änderungen.

Die Auszahlung der Beihilfen erfolgt mit KoPers.. Hierzu werden Zahlungsinformationen von Permis-B an KoPers zurück übermittelt, mit Buchungsinformationen angereichert und dann über KoPers ausgezahlt.

Verbuchung:
Für die Landesbetriebe und Hochschulen (alle in der Umstellung zum 01.01.2019) gibt es eine Änderung im Verbuchungsprozess mit der Einführung von KoPers. Zukünftig erfolgt keine Zahlung der Bezüge mehr durch das ZPD, sondern direkt von Konten der Landesbetriebe und Hochschulen. Dies trifft auf alle Bezügezahlungen und Zahlungen an Dritte (z. B. HVV, Gläubiger etc.) zu. Steuern und Sozialversicherungsbeiträge werden von den Landesbetrieben und Hochschulen an den Kernhaushalt der FHH abgeführt, damit die FHH ihre

einheitlichen Arbeitgeberaufgaben wahrnehmen kann und diese wiederrum selbst abführen kann. In diesem Zusammenhang stellt KoPers SEPA-Dateien zu Lasten des jeweiligen Kontos sowie diverse Auswertungen für Abstimmung und Nachweisung (CO-Buc) sowie zahlungsbegleitende Unterlagen zur Verfügung.

Abschläge und andere tägliche Zahlungen sollen ebenfalls über SEPA-Dateien abgewickelt werden.

2.3 Sperrung und Löschung (vgl. § 19 HmbDSG)

Welche Fristen, Zuständigkeiten, Abläufe gelten?

- Siehe Löschkonzept.

2.4 Berechtigungskonzept

Nutzerzahlen:

Zahl der voraussichtlichen Nutzer (insgesamt): ca. 626, davon:

In den Behörden und Ämtern zum 01.04.2018:	ca. **85**
In den Behörden und Ämtern zum 01.07.2018:	ca. **205**
In den Behörden, Ämtern, Landesbetrieben und Hochschulen zum 01.07.2018:	ca. **336**

Grundsätzlich sollen die gleichen Zugriffsmöglichkeiten gewährleistet sein wie in der täglichen Praxis mit dem Altsystem PAISY. Das weitere ist im Berechtigungskonzept festgelegt.

2.5 IT-Konzept

Einbindung in die Infrastruktur: Der Betrieb des Systems KoPers erfolgt vollständig im Dataport Rechenzentrum (RZ²). Das System besteht aus einem Entwicklungssystem, Qualitätssicherungssystemen (Stage) und dem Produktivsystem. Es gibt getrennte Qualitätssicherungssysteme für den Betrieb KoPers sowie das Projekt (Stufe 2). Das Entwicklungssystem ist ein gemeinsames, dieses teilen sich die beteiligten Länder auf Systemebene (Datenbankinstanz). Die Länder werden hier über Mandanten abgebildet. Das Produktivsystem sowie das QS-System bestehen aus zwei unabhängigen Datenbankinstanzen je Land.

Bis zur Einführung der Stufe 2 ergibt sich die folgende Systemlandschaft für den Betrieb KoPers sowie die projektvorbereitenden Aktivitäten Stufe 2:

Produktion

Mandant **430**: Produktivmandant Passive
(releaseunabhängig SH) (Echtdaten)

Mandant **431**: Produktivmandant QuickWin Bewerbungsmanagement sowie künftig Versorgungsfestsetzung
(releaseunabhängig SH) (Echtdaten)

Stage/QS

Mandant **330**: Qualitätssicherung im Projekt

Mandant **333**: Qualitätssicherung Passive
(releaseunabhängig SH)

Mandant **630**: Qualitätssicherung Monatsabschluss
(releaseunabhängig SH) (Echtdaten)

Entwicklung

Mandant **030**: Entwicklung Betrieb Passive und Projekt

Schulung

Mandant **150**: Schulungsumgebung

Mandant **334**: Produktionsnahe Schulung
(releaseunabhängig SH)

Migration

Mandant **230**: Monatliche Migration und Abrechnungsanalyse (Echtdaten)

Mandant **231**: Migration und Abrechnungsanalyse, Aufbau Rückrechnungshistorie (Echtdaten)

Systemtechnisch besteht das System aus Web-Server (Zugriff der Nutzer über das Web/Linux-Server), Applikationsservern (Linux), Datenbankservern (Linux/Oracle), Payroll-Server (Linux) sowie den Druckservern (Windows/Office). Die Details sind der bereits verschickten IT-Sicherheits-Dokumentation von Dataport zu entnehmen (CD).

Die Länder Schleswig-Holstein und Hamburg teilen sich jeweils eine gemeinsame systemtechnische Umgebung für die Entwicklung, für den Test der Software im Projekt sowie für Schulungen. Die Daten werden hier in einer gemeinsamen Datenbankinstanz verwaltet. Die logische Trennung der Datenhaltung wird durch Mandanten realisiert, d. h. für die jeweiligen Länder wird eine disjunkte, mandantenorientierte Datenhaltung gewährleistet.

Die Produktion beider Länder erfolgt auf zwei getrennten systemtechnischen Umgebungen. Die Länder können somit unterschiedliche Versionen der Software betreiben (oben gekennzeichnet als releaseunabhängig). Für jedes Land ist eine eigenständige Datenbankinstanz eingerichtet. Die Verwaltung der Datenbankinstanzen erfolgt über ein zentrales Datenbankmanagementsystem. Der Zugriff erfolgt ebenfalls über dedizierte Web-Server. Die Trennung des Datenstromes erfolgt getrennt nach Landesnetzen. Die Trennung übernehmen die LOAD-Balancer. Somit ist auf Darstellungsebene, Applikationsebene und Datenbankebene eine durchgehende Trennung gewährleistet. Eine Anmeldung eines Nutzers aus SH mit SH-Account bei einem FHH Mandanten ist somit technisch ausgeschlossen. Dieser könnte nur erfolgreich vorgenommen werden, wenn:

- Der SH-Nutzer Kenntnis von Benutzernamen und Passwort eines FHH Accounts hätte,
- Der Zugriff aus dem FHH Netz erfolgen würde.

Hinsichtlich der Trennung der Beschäftigtendaten der einzelnen Daten verarbeitenden Stellen zueinander wird auf das Berechtigungskonzept verwiesen. Der Zugriff auf KoPers erfolgt per Webzugriff innerhalb des FHH-Netzes. Verwendet wird das https Protokoll und der Internetexplorer in der jeweils aktuellen Version.

Art der Clients (Arbeitsplatzrechner/mobile Geräte): Es werden grundsätzlich Standard-Arbeitsplatzrechner von Dataport verwendet. Dies sind Arbeitsplatzrechner mit Internetzugriff. Das FHH-Netz (auch Intranet und Internet) wird standardmäßig verwendet. (Abweichungen hiervon sind in den jeweiligen behördenspezifischen Anlagen zu dieser Risikoanalyse aufgeführt).

Das Verfahren nutzende Organisationseinheiten, Standorte und Außenstellen sind in den jeweiligen behördenspezifischen Anlagen zu dieser Risikoanalysen aufgeführt..

Server inkl. Standort: Applikationsserver und Pay-Roll-Server KoPers Standort Dataport RZ Altenholz Netzeinbindung innerhalb des Dataport RZ über verschlüsselte Leitungen (SSL).

Für die Verfügbarkeit der bereitgestellten Umgebungen sowie Notfallvorsorgemaßnahmen ist zwischen KoPers und Dataport ein SLA (Anlage 2a zum Vertrag V4992 und V5003) geschlossen. Zur Sicherstellung der Informationssicherheit ist ein SSLA (Vertrag V4992 und V5003) geschlossen.

2.6 Feststellung des Schutzbedarfs

Schutzziel	Schutzbedarf	Begründung
Vertraulichkeit Es ist zu gewährleisten, dass nur Befugte Personen bezogene Daten zur Kenntnis nehmen können.	☐ normal ☒ hoch ☐ sehr hoch	Da es sich um Personal-daten mit teil-weise hohem Schutzbedarf handelt
Integrität Es ist zu gewährleisten, dass personenbezogene Daten während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben.	☐ normal ☒ hoch ☐ sehr hoch	
Verfügbarkeit Es ist zu gewährleisten, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.	☐ normal ☒ hoch ☐ sehr hoch	
Authentizität Es ist zu gewährleisten, dass Daten ihrem Ursprung zugeordnet werden können.	☒ normal ☐ hoch ☐ sehr hoch	
Revisionsfähigkeit Es ist zu gewährleisten, dass festgestellt werden kann wer wann welche Daten in welcher Weise verarbeitet hat.	☒ normal ☐ hoch ☐ sehr hoch	

2.7 Tolerierbare Ausfallzeit

Wie hoch ist die tolerierbare Ausfallzeit (Maximum) einzuschätzen?

- 8 Stunden / 1 Arbeitstag

2.8 Bedrohungsanalyse/Risikobewertung

Tabelle der Risikobewertung

Bedrohtes Objekt	**Darstellung der Bedrohung zu den notwendigen technisch-organisatorischen Maßnahmen siehe die unter 2.9. aufgeführten Einzelmaßnahmen zu den**	**Bedrohtes Schutzziel**	**Schutz-bedarf**

	jeweiligen bedrohten Objekten.		
Arbeitsplatzrechner (PC) mit Daten	Diebstahl bzw. Verlust durch höhere Gewalt	Vertraulichkeit, Verfügbarkeit	2
	Unberechtigter Zugriff z. B. bei Sitzungspausen	Vertraulichkeit, Integrität	2
	Ausspähen des Bildschirminhalts durch Dritte	Vertraulichkeit	2
	Kopie der Daten auf externen Speicher (z. B. USB-Stick)	Vertraulichkeit	2
	Einschleusen eines Keyloggers	Vertraulichkeit	2
	Zugriff auf Daten über das Internet	Vertraulichkeit, Integrität	2
	Infektion mit Viren und Trojaner	Vertraulichkeit, Integrität	2
	Missbräuchlicher Zugriff durch berechtigte Person	Vertraulichkeit, Integrität	2
LAN/WAN innerhalb DP RZ	Missbräuchlicher Zugriff durch Administratoren	Vertraulichkeit, Integrität	2
	Zerstörung durch höhere Gewalt (Feuer, Wasser, Blitz, ...)	Verfügbarkeit	1
	Missbräuchlicher Zugriff durch Beschäftigte	Vertraulichkeit, Integrität	2
	Missbräuchlicher Zugriff durch betriebsfremde Personen	Vertraulichkeit, Integrität	2
Server	Ausfälle und Störungen	Verfügbarkeit, Integrität	1
	Vandalismus Diebstahl	Verfügbarkeit, Vertraulichkeit, Integrität	2
	Höhere Gewalt	Verfügbarkeit	1
	Unberechtigter Zugriff	Vertraulichkeit, Verfügbarkeit, Integrität	2
	Datenverlust/-veränderung durch Bedienungsfehler	Verfügbarkeit, Integrität	1
	Einschleusen von Schadsoftware	Verfügbarkeit, Integrität	1
	Angriff von außen	Verfügbarkeit	1
	Fehlerhafte Software u. a. bei Versionswechsel	Verfügbarkeit	1
Benutzer	Ausspähen von Eingaben	Vertraulichkeit	2
	Missbrauch von Zugangs-kennungen	Vertraulichkeit, Integrität	2
	Weitergabe von Zugangskennungen	Vertraulichkeit Integrität	2

	Kopie der Daten auf externe Speichermedien	Vertraulichkeit	2
Drucker	Einsicht oder Diebstahl von Ausdrucken	Vertraulichkeit	2
	Unberechtigte Nutzung interner Speicherdaten	Vertraulichkeit	2
	Vervielfältigen von Bildschirmausdrucken	Vertraulichkeit	2

Liegt bei einzelnen Objekten erhöhte Eintrittswahrscheinlichkeit für mögliche Schäden vor?

- ☐ ja (Beschreibung) ☒ nein (Begründung)

Wenn ja, welche Objekte und welche Bedrohungen?

- Fehlanzeige.

2.9 Beschreibung technischer und organisatorischer Maßnahmen

Arbeitsplatzrechner
Die technischen und organisatorischen Maßnahmen zum Schutz der Arbeitsplatzrechner (Clients) sind in den dezentralen behördenspezifischen Anlagen zu dieser Risikoanalyse aufgeführt.

LAN / WLAN

- RZ-Betrieb für PAISY und KoPers.
- Das Verfahren erfolgt vollständig im Dataport LAN, die bestehenden Anforderungen an die Verfügbarkeit erübrigen weitere Maßnahmen.
- WLAN: Aus dem WLAN ist kein Zugriff auf die KoPers Produktionsumgebung (430, 431) möglich.
- Über eine VPN Verbindung ist kein Zugriff auf die KoPers Produktionsumgebung(430, 431) möglich.

Server

- Server-Betrieb im gesicherten Rechenzentrum von Dataport (Datenverarbeitung im Auftrag).
- Vor der Installation von Software bzw. Softwareänderungen werden diese entsprechend des Anforderungsprozesses des Systems KoPers und des HR-Systemhauses (entspricht der Freigaberichtlinie der FHH) einem Funktions- u. Abnahmetest unterzogen.
- Die Zugangsverfügbarkeit des FHHNET beträgt lt. Dataport etwa 98 %.
- Protokollierungen im Fachverfahren:
    - fehlerhafte Logins (vgl. Passwortrichtlinie),
    - Schreibende Zugriffe durch Benutzer und Administratoren, (unter Angabe der Benutzerkennung und des Datums),
    - Anlegen, Löschen von Benutzern, Änderungen von Zugriffsrechten,
    - Technische Protokollierungen (durchgeführte Datensicherungen.
- Im Migrationstool erfolgt keine Protokollierung.
- Verschlüsselung der Datenbank mit Oracle TDE.

Dezentrale Infrastruktur

Die technischen und organisatorischen Maßnahmen zum Schutz der dezentralen Infrastruktur (z. B. Drucker) sind in den dezentralen behördenspezifischen Anlagen zu dieser Risikoanalyse aufgeführt.

Clients
Austausch defekter Workstations kann von Dataport innerhalb von 24 Stunden gewährleistet werden. An dem Migrationsprojekt sind nur fachlich geschulte Personen beteiligt.

Benutzer / Zugriffe
Die technischen und organisatorischen Maßnahmen zum Schutz der Benutzer / Zugriffe sind in den dezentralen behördenspezifischen Anlagen zu dieser Risikoanalyse aufgeführt.

2.10 Datenschutz-/datensicherheitsrelevante Aspekte

Welche datenschutz-/datensicherheitsrelevanten Aspekte sind vertraglich zu regeln? (z. B. Fernwartung, Datenaustausch, Datenschutzverpflichtung, Fehlerbehebung, Auftragsdatenverarbeitung durch Dataport, Auftragsdatenverarbeitung durch andere Dritte).

Die Auftragsdatenverarbeitung erfolgt durch Dataport und ist geregelt durch das Kooperationsabkommen sowie die Ergänzung zum Kooperationsabkommen zwischen der FHH und dem Land Schleswig-Holstein sowie durch den Rahmenvertrag zwischen der FHH und dem Land Schleswig-Holstein einerseits und Dataport andererseits. Das Verfahren wird im RZ² Rechenzentrum von Dataport betrieben. Der technische Verfahrensaufbau und -betrieb ist in der Dataport Sicherheitsdokumentation beschrieben. Die FHH schließt mit den in der Stufe 1 beteiligten Anstalten des öffentlichen Rechts Kontrakte zur Einführung des KoPers-Verfahrens. Der Kooperation ist die Freie Hansestadt Bremen beigetreten, welche ihre Projektaktivitäten im Rahmen eines Moratoriums derzeit nicht verfolgt.

2.11 Änderung von Programmfunktionalitäten

Wie ist das Änderungsverfahren geregelt?

Zur Anwendung kommt das freigegebene HR-IT-Anforderungsmanagement - mit dem implementierten Freigabeprozess. Dieser sieht folgende Prozessschritte vor:

- Anforderungserhebung,
- Bewertung der Anforderung,
- Länderübergreifende Abstimmung,
- Freigabe der Anforderung,
- Umsetzung der Anforderung,
- Test der Umsetzung,
- Freigabe der Anforderung.

Der gesamte Prozess wird vom HR-IT Auftraggeber als Teil des HR-Systemhauses beim ZPD gesteuert und überwacht. Die Umsetzung von Anforderungen erfolgt nach der Aufgabenverteilung wie folgt:

- Die Pflege von fachlichen Objekten und Tabellen (Customizing) erfolgt in der Fachlichen Leitstelle KoPers (HR-Systemhaus).
- Die Pflege von technischen Objekten und Tabellen erfolgt in der technischen Leitstelle bei Dataport.
- Programmierungen und Systemerweiterungen werden von der P&I AG vorgenommen. Pro Kalenderjahr sind 4 Releases plus 1 Jahresendrelease vorgesehen.

Die Freigabe des Verfahrens durch den HR-IT Auftraggeber entspricht immer einer Gesamtfreigabe des Systems nach der Freigaberichtlinie der FHH.

Wo liegt die Verantwortung?

- Für Änderungen in KoPers liegt die Verantwortung bei dem HR-Systemhaus, bzw. der Fachlichen Leitstelle und dem HR-IT Auftraggeber.

Wer betreut die Anwendung?

- Die technische Betreuung von KoPers wird durch die Technische Leitstelle bei Dataport sichergestellt. Die fachliche Betreuung KoPers ist im HR-Systemhaus angesiedelt, die programmierende Betreuung von KoPers nimmt P&I wahr.

Wie und durch wen erfolgt die Abnahme und Freigabe der IT-Anwendung?

- Eine Freigabe gemäß der Freigabe-RL für das Verfahren KoPers Stufe 2 ist für den 28.02.2018 vorgesehen. Nach erfolgreichem Freigabetest erfolgt seitens des ZPD die Empfehlung der Freigabe durch den HR-IT-Auftraggeber. Die Freigabe der Anwendung für den Produktionsbetrieb erfolgt durch die Daten verarbeitenden Stellen.

Wie und durch wen erfolgt die Schulung, Einweisung oder Unterrichtung und die Betreuung der betroffenen Anwender?

- Siehe hierzu das beiliegende Schulungskonzept.

2.12 Zusammenfassende Bewertung

☒ Die mit dem Verfahren verbundenen Gefahren werden durch die beschriebenen technischen und organisatorischen Maßnahmen wirksam beherrscht.

☐ Die mit dem Verfahren verbundenen Gefahren werden durch die beschriebenen technischen und organisatorischen Maßnahmen nicht wirksam beherrscht.