Vereinbarung

nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG)

über die Pilotierung des IT-Verfahrens

elektronische Postbearbeitung (ePob)

Zwischen

der Freien und Hansestadt Hamburg - vertreten durch den Senat -

- Personalamt -

einerseits

und

dem dbb hamburg

- beamtenbund und tarifunion -

sowie

dem Deutschen Gewerkschaftsbund

- Bezirk Nord -

als Spitzenorganisationen der Gewerkschaften und Berufsverbände

des öffentlichen Dienstes

andererseits

wird Folgendes vereinbart:

Präambel

In allen Organisationseinheiten der FHH ist noch ein hoher Anteil an eingehender Papierpost zu verzeichnen. Für die Bearbeitung wird aktuell die Post manuell verteilt. Ziel der Pilotierung des IT-Verfahrens elektronische Postbearbeitung (ePob) ist es, die Digitalisierung der Papiereingänge und insbesondere die Klassifizierung der Dokumente zur weiteren Bearbeitung zur Vorbereitung des weiteren Rollouts zu erproben.

Die Partner dieser Vereinbarung sind sich einig, dass die Verteilung der eingehenden externen Post in den Pilotierungsdienststellen (vgl. unten Ziffer 2) durch das neu einzuführende IT-Verfahren ePob elektronisch unterstützt und dabei teilweise automatisiert werden soll.

Diese Vereinbarung ergänzt die bereits bestehende Vereinbarung nach § 94 HmbPersVG über den Prozess zur Einführung und Nutzung allgemeiner automatisierter Bürofunktionen und multimedialer Technik (Bürokommunikation) und zur Entwicklung von E-Government vom 10.09.2001.

Das IT-Verfahren ePob soll die Anwendenden bei der Bearbeitung von externen Posteingängen unterstützen. Durch den Einsatz von ePob wird den Anwendenden eine einfache und effiziente Lösung zur Bearbeitung der Posteingänge angeboten und gleichzeitig die Transparenz sämtlicher relevanter Bearbeitungsschritte sichergestellt. Es soll ergonomisch ausgestaltet und sinnvoll in den Gesamtprozess der Postbearbeitung integriert sein. Um dies zu gewährleisten, erfolgte die Entwicklung von ePob unter enger Einbeziehung der Behörden und Ämter im Rahmen eines Anwenderarbeitskreises. Mit der Reduktion der manuellen Tätigkeiten und einer Anbindung von ePob an die bestehenden Prozesse der DRiVe-IT soll eine höhere Akzeptanz für die Anwendung des Verfahrens ePob geschaffen werden.

Nr. 1

Gegenstand der Vereinbarung

Gegenstand der Vereinbarung ist die Pilotierung des IT-Verfahrens ePob als Teil der DRiVe-IT.

Zweck und Ziel des IT-Verfahrens sind in der Anlage 1 - Beschreibung der Verarbeitungstätigkeit - näher beschrieben. Der Prozess, den die Posteingangsstücke durchlaufen, ist in Anlage 2 dargestellt. Die Anlagen sind Bestandteil der vorliegenden Vereinbarung.

Soweit sich aus der besonderen zentralen Funktion der Kasse.Hamburg im Verfahren zusätzliche Mitbestimmungstatbestände ergeben, die von dieser Vereinbarung nicht abgedeckt sind, wird insoweit für die Kasse.Hamburg eine diese Vereinbarung ergänzende örtliche Dienstvereinbarung abgeschlossen.

Nr. 2

Geltungsbereich

Die Vereinbarung gilt für die Dienststellen Kasse.Hamburg, Bezirksamt Bergedorf, Bezirksamt Hamburg-Mitte und Behörde für Stadtentwicklung und Wohnen.

Nr. 3

Pilotierung zur Erprobung

Vor einer FHH-weiten Einführung ist eine Pilotierungsphase mit vier Pilotbetrieben vorgesehen. Es nehmen die Kasse.Hamburg, das Bezirksamt Bergedorf, das Bezirksamt Mitte und die BSW teil. Die Aufschaltung der Pilotbetriebe erfolgt in mehreren Wellen. Auch werden innerhalb eines Pilotbetriebs einzelne, durch den Pilotbetrieb selbst ausgewählte Bereiche sukzessive an ePob angebunden. Die Pilotierung dient dem Lernen und Sammeln von Erfahrungen, um die Prozesse für die hamburgweite Ausweitung zu optimieren, und Auswirkungen auf die Arbeitssituation der Beschäftigten zu beobachten.

Nr. 4

Ergonomie, Arbeitsplatzgestaltung und Barrierefreiheit

Die Gestaltung der ergonomischen Eigenschaften des IT-Verfahrens und der betroffenen Arbeitsplätze richtet sich nach den einschlägigen gesetzlichen Bestimmungen und orientiert sich an den Grundsätzen der DIN EN ISO 9241, insbesondere den Teilen -11 (Anforderung an die Gebrauchstauglichkeit) und -110 (Grundsätze der Dialoggestaltung).

Die schutzwürdigen Belange besonderer Beschäftigtengruppen (z.B. Menschen mit Behinderung) werden bei der Arbeitsplatzgestaltung berücksichtigt (z.B. Einrichtung mit Zusatzsoftware wie Bildschirmausleseprogramm, -vergrößerungsprogramm o.ä.), so dass ein barrierefreies Arbeiten möglich ist.

Das Verfahren wird auf Grundlage des §11 Hamburgischen Gesetz zur Gleichstellung von Menschen mit Behinderungen (HmbBGG) nach den Anforderungen der EN 301 549 V 3.2.1 als Expertenprüfung auf Barrierefreiheit geprüft. Als Standard wird der BITi BITV-Softwaretest genutzt. Es entsteht ein Prüfbericht mit den gefundenen Mängeln und Empfehlungen. Die Prüfung erfolgt durch Dataport A.ö.R. Im Rahmen des Austausches ePob (SK - Kasse.Hamburg) am 01.02.2023 wurde als Zeitpunkt für eine Prüfung der Barrierefreiheit sowie der Ergonomie das Ende der Pilotierung (April 2023) anvisiert.

Die betroffenen Arbeitsplätze sind mit Endgeräten ausgestattet, die der Fachaufgabe angemessen sind und dem Stand der Technik entsprechen.

Soweit sich aus einer Anwendung neue technische Anforderungen ergeben, wird eine Anpassung vorgenommen. Die Freie und Hansestadt Hamburg als Arbeitgeberin, vertreten durch die jeweils zuständige Behörde bzw. Dienststelle, wird dabei die sich aus den §§ 3-14 Arbeitsschutzgesetz und Anlage 6 der Verordnung über Arbeitsstätten ergebenden Pflichten erfüllen[1].

[1] Näheres regelt die Vereinbarung zu der Vereinbarung nach § 94 HmbPersVG zur betrieblichen Gesundheitsförderung in der hamburgischen Verwaltung hier: Regelung zur Gefährdungsbeurteilung der physischen und psychischen Belastungen am Arbeitsplatz

Nr. 5

Arbeitsplatz- und Einkommenssicherung

Die Einführung und der laufende Betrieb des neuen IT-Verfahrens werden nicht zu Kündigung oder Änderungskündigung von Arbeitsverhältnissen mit dem Ziel der tariflichen Herabgruppierung führen. Bei notwendigen Versetzungen oder Umsetzungen werden vorrangig gleichwertige Arbeitsplätze bzw. Dienstposten angeboten, sofern im bisherigen Tätigkeitsbereich eine gleichwertige Tätigkeit nicht weiter möglich ist.

Bei Versetzungen oder Umsetzungen werden alle Umstände angemessen berücksichtigt, die sich aus der Vor- und Ausbildung, der seitherigen Beschäftigung und persönlicher und sozialer Verhältnisse der bzw. des Betroffenen ergeben.

Gleiches gilt, wenn notwendige personelle Maßnahmen im Einzelfall unvermeidlich sein sollten, weil Beschäftigte auch nach den erforderlichen Fortbildungs- oder Schulungsmaßnahmen den sich aus dem neuen Verfahren ergebenden Anforderungen nicht entsprechen. Auch in diesen Fällen finden betriebsbedingte Kündigungen oder Änderungskündigungen mit dem Ziel der tariflichen Herabgruppierung nicht statt.

Die Arbeitsplatz- und Einkommenssicherung für die Tarifbeschäftigten richtet sich ferner nach dem Tarifvertrag über den Rationalisierungsschutz für Angestellte vom 09.01.1987.

Soweit sich aus dem Beamtenrecht nichts anderes ergibt, gilt die Vereinbarung nach § 94 HmbPersVG über den Rationalisierungsschutz für Beamte vom 09.05.1989.

Auf die Belange der Kolleginnen und Kollegen mit Behinderung wird besonders Rücksicht genommen.

Nr. 6

Datenschutz, Schutz vor Leistungs- und Verhaltenskontrolle

Es werden nur diejenigen personenbezogenen Daten verarbeitet (hierunter fallen auch Auswertungen, vgl. Artikel 4, Ziffer 1 und 2 Verordnung (EU) 2016/679, DSGVO), die für die Erledigung der Fachaufgabe erforderlich sind.

Die erforderlichen personenbezogenen Daten werden zu folgenden Zwecken genutzt:*

- Identifikation und Aufruf des Verfahrens,
- Aufzeichnung der Zugriffe und Veränderungen sowie
- die Identifikation der den Genehmigungsworkflow durchführenden Personen sowie der das Verfahren administrierenden Personen.

Im Einzelnen handelt es sich um folgende personenbezogene Daten der Beschäftigten:*

- Name, Vorname
- Benutzer-Kennung
- Dienstliche E-Mail-Adresse
- Dienstliches Telefon sowie Fax

Das Posteingangsbuch protokolliert Arbeitsschritte an einem Dokument. Diese Information hängt nicht an dem Digitalisat, sondern wird in der Datenbank gespeichert. Nach einer Frist von einem Jahr, ab dem das Dokument in das Posteingangsbuch gelangt ist, werden die Daten zu den Arbeitsschritten anonymisiert bzw., die Arbeitnehmerdaten aus der Datenbank gelöscht. Es kann danach keine Schlussfolgerung, wer an einem Poststück gearbeitet hat, gezogen werden. Dieser Prozess wird automatisch durch das Posteingangsbuch angestoßen.

Folgende Schnittstellen sind implementiert:

- Schnittstelle vom Posteingangsbuch zur ELDORADO-Instanz der DRiVe-IT: Aufruf der gescannten Dokumente (Poststücke) über die DOK-ID zur Anzeige im Posteingangsbuch
- Schnittstelle vom Posteingangsbuch zu ELDORADO 2.0: Als elektronisches Archiv-System wird ELDORADO 2.0 für die Verwaltung von elektronischen Schriftstücken in Akten verwendet. Bei einer positiven Archivierungsentscheidung seitens der Sachbearbeitenden werden die Poststücke in den Mandanten der jeweiligen Behörde/ des jeweiligen Amtes verfügt.

Die personenbezogenen Daten werden gemäß der Vereinbarung nach § 94 HmbPersVG über den Prozess zur Einführung und Nutzung allgemeiner automatisierter Bürofunktionen und multimedialer Technik und zur Entwicklung von E-Government vom 10.09.2001 nicht zur Leistungs- und Verhaltenskontrolle der Anwenderinnen und Anwender genutzt. Dies gilt sowohl unmittelbar über das IT-Verfahren als auch mittelbar über andere IT-Verfahren.

Die im Zusammenhang mit diesem Verfahren verarbeiteten personenbezogenen Daten der Anwenderinnen und Anwender dürfen grundsätzlich nicht zur Begründung dienst- und/oder arbeitsrechtlicher Maßnahmen verwendet werden. Ausnahmsweise ist dies bei einem (auch zufällig entstandenen) konkreten Verdacht zur Aufklärung von Missbrauchstatbeständen (Dienstvergehen, Verletzung arbeitsvertraglicher Pflichten oder strafbare Handlungen) zulässig. Der auslösende Sachverhalt ist zu dokumentieren. Der zuständige Personalrat ist möglichst[2] vorher zu unterrichten. Die bzw. der betroffene Beschäftigte ist zu unterrichten, sobald dies ohne Gefährdung des Aufklärungsziels möglich ist. Daten, die ausschließlich zum Zwecke der Aufklärung erhoben wurden, sind zu löschen, sobald der Verdacht ausgeräumt ist oder sie für Zwecke der Rechtsverfolgung nicht mehr benötigt werden.

Die Erteilung von Berechtigungen erfolgt auf der Grundlage eines Berechtigungs- und Rollenkonzepts, in dem die für die verschiedenen Funktionen/Mitarbeitergruppen erforderliche Berechtigungen festgelegt werden um mandantenspezifische (d. h. separat für jede Organisationsstruktur geltende) Berechtigungsstrukturen abzubilden. Das Rechte- und Rollenkonzept wird in der Anlage 3 näher beschrieben.

[2] Von der vorherigen Information des Personalrats darf nur abgewichen werden, wenn andernfalls das Ziel der Auswertung nicht erreicht werden kann. Gründe dafür können sich im Einzelfall ergeben, z.B. bei Gefahr im Verzuge oder einer Gefährdung des Ermittlungszwecks. Erfolgt die Unterrichtung des Personalrats erst nachträglich, sind ihm die dafür maßgeblichen Gründe zu benennen.

Nr. 7

Qualifizierung der Anwenderinnen und Anwender

Mit der Einführung dieses Verfahrens ändern sich die Arbeitsbedingungen der Anwenderinnen und Anwender. Die dafür erforderlichen Qualifizierungsmaßnahmen verfolgen das Ziel, die Anwenderinnen und Anwender entsprechend ihrer Rolle zu einer selbstständigen und sicheren Erledigung ihrer fachlichen neuen Aufgaben zu befähigen. Diese Qualifizierungsmaßnahme soll zeitnah vor Einführung des IT-Verfahrens erfolgen. Nach ca. 4 – 6 Monaten Arbeit mit dem IT-Verfahren wird den Anwenderinnen und Anwendern Gelegenheit gegeben, durch eine Ergänzungsqualifizierung selbst empfundene Defizite aufzuarbeiten. Für die Qualifizierungsmaßnahmen trägt die zuständige Behörde oder Dienststelle in Verbindung mit der fachlich zuständigen Stelle die Verantwortung.

Bei der Entwicklung des Qualifizierungskonzepts wird geprüft, ob bei mittelbar von dem IT-Verfahren betroffenen Beschäftigten ein Qualifizierungsbedarf besteht. Die Einzelheiten werden in einem Qualifizierungskonzept dargestellt, das als Anlage 4 beigefügt ist.

Den Anwenderinnen und Anwendern werden Hilfen zum Umgang mit dem IT-Verfahren bereitgestellt, die sich über das IT-Verfahren oder an zentraler Stelle (z.B. im FHHportal) aufrufen lassen. Es wird außerdem gewährleistet, dass für alle Anwenderinnen und Anwender im Falle auftretender Probleme eine versierte Ansprechstelle zur Verfügung steht.

Es wird gewährleistet, dass auch Menschen mit Behinderung qualifiziert werden können, ggf. werden individuell angepasste Qualifizierungsmaßnahmen entwickelt.

Die Spitzenorganisationen und die Personalräte erhalten Gelegenheit an den Qualifizierungsmaßnahmen teilzunehmen.

Nr. 8

Schlussbestimmungen

Soweit durch diese Vereinbarung Mitbestimmungstatbestände nicht geregelt werden, bleibt die Mitbestimmung der Personalvertretung unberührt.

Diese Vereinbarung tritt *am … /mit sofortiger Wirkung in Kraft*. Sie gilt bis zum Abschluss einer Vereinbarung nach § 93 HmbPersVG zur Einführung des IT-Verfahrens elektronische Postbearbeitung (ePob).

Hamburg, den 17. Feb. 2023

Freie und Hansestadt Hamburg

für den Senat

Volker Wiedemann

dbb hamburg

beamtenbund und tarifunion

Rudolf Klüver

Deutscher Gewerkschaftsbund

-Bezirk Nord-

Olaf Schwede

Anlagen:

1. Beschreibung der Verarbeitungstätigkeit
2. Prozessdarstellung
3. Berechtigungs- und Rollenkonzept
4. Qualifizierungskonzept

.

Hamburg

Beschreibung der Verarbeitungstätigkeit

(Bitte an die Verzeichnisführende Stelle absenden!)

Blatt-Nr.:

Von der Verzeichnisführenden Stelle auszufüllen!

Nur auszufüllen, wenn personenbezogene Daten[1] verarbeitet werden!

Anmerkung: Soweit der Platz dieses Formulars nicht ausreicht fügen Sie bitte zusätzliche Anlagen bei!

Allgemeines			
	Datum:	Klicken Sie hier, um ein Datum einzugeben.	
	Ausfüllende Person:		
	Telefonnummer:		
	Bezeichnung des Verfahrens:	Elektronische Postbearbeitung (ePob) allg.	
	Bezeichnung der Verarbeitung[2]:	☐ Erheben ☐ Erfassen ☐ Organisieren ☐ Ordnen ☐ Speichern ☐ Anpassen oder Verändern ☐ Auslesen ☐ Abfragen ☐ Verwenden ☐ Offenlegen durch Übermittlung, Verbreitung oder andere Form der Bereitstellung ☐ Abgleichen oder die Verknüpfen ☐ Einschränken ☐ Löschen ☐ Vernichten	
	Beginn der Verarbeitung[3]:	20.02.2023 – 30.04.23 (voraussichtlich-Stand 08.02.2023)	
	Änderung bestehende Verarbeitung : **Überführung bestehende Verarbeitung in geltende Rechtslage nach DS-GVO:**	☐ ja ☐ ja	
	Neue Verarbeitung:	☒ ja	
	Abmeldung bestehende Verarbeitung[4]:	☐ ja	
1. Grundsätzliche Angaben zur Verantwortlichkeit			
1.1	Verantwortliche Organisationseinheit[5] (optional):	Die anwendenden öffentlichen Stellen (Während der Pilotphase Kasse.HH, Senatskanzlei, BA Bergedorf, BA Hamburg-Mitte und die BSW)	

[1] Hinweis Nr. 1 der Anlage 1
[2] Hinweis Nr. 2 der Anlage 1
[3] Hinweis Nr. 3 der Anlage 1
[4] Hinweis Nr. 4 der Anlage 1
[5] Hinweis Nr. 5 der Anlage 1

1.2	Vertreter der verantwortlichen Organisationseinheit (optional):	Klicken Sie hier, um Text einzugeben.	
1.3	Fachliche Leitstelle (bei IT-Verfahren) bzw. zuständige Stelle (bei nicht automatisierten Verfahren): Verantwortliche Führungskraft: Leitzeichen:	FL DRiVe Oelrichs, Jessica K25	
1.4	Ansprechpartner, sofern nicht verantwortliche Führungskraft: Telefonnummer:	Klicken Sie hier, um Text einzugeben.	
1.5	Name des Datenschutzbeauftragten (optional):		
1.6	Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt[6]: Auftragsnummer:	Kasse.Hamburg Bahrenfelder Straße 254-260, 22765 Hamburg	

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung[7]			

2.1	Beschreibung und Zweckbestimmung der Verarbeitung von Daten[8]	Elektronische Postbearbeitung (ePob) ist ein Service zur elektronischen Postzustellung innerhalb der FHH. Der Service besteht aus den Komponenten Scannen, Verteilen, Bearbeiten und Verakten.
		
		Vor der elektronischen Verarbeitung wird die eingehende externe Post bei den anwenden öffentlichen Stellen (Behörde/Bezirken, u.a.) zuerst gesichtet und für einen Transport zur Scanstelle in der Kasse Hamburg vorbereitet werden. Dazu gehört eine Festlegung von Kriterien zur Identifizierung des Scangutes.
		
		Post, die für einen Scanvorgang nicht geeignet ist, verbleibt in der Behörde und wird wie bisher als Papieroriginal verteilt und bearbeitet.
		
		Zur Weiterleitung an den Zentralen Rechnungseingang der Kasse.Hamburg wurden folgende Grundkriterien werden festgelegt:
		
		• Keine interne Post
		• Ausschließlich externe Post mit Ausnahme von
		  ○ Personalangelegenheiten
		  ○ Persönlich adressierten Briefen
		  ○ Werbepost
		  ○ Infomaterialien
		  ○ Sensible Daten Gem. Art. 9 DSGVO	

[6] Hinweis Nr. 6 der Anlage 1
[7] Hinweis Nr. 7 der Anlage 1
[8] Hinweis Nr. 8 der Anlage 1

		Die mit vorgesehenen grünen Boxen aus den Behörden/Bezirken gelieferten Dokumente werden mit 8-stelligen nummerischen Barcodes beklebt und von den Beschäftigten des ZRE stapelweise eingescannt. Ein Digitalisierungsprozess setzt sich aus mehreren Arbeitsschritten zusammen Scannen Verifizieren Weiterleiten Bearbeiten Verfügen -> Eine Verfügung erfolgt in ein Zielarchiv der:s jeweiligen Behörde/Amtes. (Außerhalb des Verfahrens ePob)	
2.2	Rechtsgrundlage (Zutreffendes bitte ankreuzen und ggf. erläutern):		
☐	Spezialgesetzliche Regelung außerhalb der DS-GVO	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Klicken Sie hier, um Text einzugeben.	
☐	Einwilligung des Betroffenen (Art. 6 Abs. 1 a DS-GVO):	*Bitte fügen Sie die Einwilligungsklausel und den Einwilligungsmechanismus hier ein* Klicken Sie hier, um Text einzugeben.	
☒	Kollektivvereinbarung (z.B. Vereinbarung gem. HmbPersVG, Tarifvertrag)	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Vereinbarung nach §93 nach HmbPersVG für "ePob" (in Verhandlung)	
☐	Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 4 HmbDSG n.F.)	Klicken Sie hier, um Text einzugeben.	
☐	Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§ 10 HmbDSG n.F. und national geregelt im BDSG):	Klicken Sie hier, um Text einzugeben.	
☐	Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b DS-GVO)	Klicken Sie hier, um Text einzugeben.	
☐	Interessenabwägung (Art. 6 Abs. 1 f DS-GVO)	*Bitte benennen Sie die vorrangigen Interessen:* Klicken Sie hier, um Text einzugeben.	
☒	Weitere:	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Auftragnehmer einer Auftragsverarbeitung nach Art. 28 DSGVO	

3. Beschreibung betroffener Personen- und Datenkategorien			
3.1	Beschreibung der betroffenen Personengruppen[9]:	Beschäftigte **Sonstige:** Klicken Sie hier, um Text einzugeben. **Beschreibung:**	
3.2	Beschreibung der Art der Daten[10] bzw. Datenkategorien	Identifikations- und Adressdaten Sonstige: Klicken Sie hier, um Text einzugeben. Beschreibung: Beschäftigtendaten: + Name + Vorname + FHHNET-Kennung +Telefonnummer + E-Mail-Adresse Weitere Betroffene:	
3.3	Werden besondere Kategorien[11] von Daten verarbeitet (Art. 9 Abs. 1 DS-GVO)?	☐ ja, welche? Wählen Sie ein Element aus. ☒ nein	
4. Datenweitergabe und deren Empfänger[12]			
4.1	Eine Datenübermittlung findet statt oder ist geplant.	☐ ja ☐ nein	
4.2	Interne Empfänger innerhalb der verantwortlichen Stelle	☐ ja ☐ nein	
	Interne Stelle (Organisationseinheit)	Klicken Sie hier, um Text einzugeben.	
	Art der Daten	Siehe 3.2	
	Zweck der Daten-Mitteilung	Bearbeitung und Digitalisierung der Post	
4.3	Externe Empfänger und Dritte	☒ ja ☐ nein	
	Externe Stelle	Kasse.Hamburg (Zentraler Rechnungseingang ZRE)	
	Art der Daten	Siehe Punkt 3.2.	
	Zweck der Daten-Mitteilung	Digitalisierung der eingegangenen Post	
4.4	Geplante Datenübermittlung in Drittstaaten (außerhalb der EU) bzw. internationale Organisation	☐ ja ☒ nein	
	Drittstaat bzw. internationale Organisation	Klicken Sie hier, um Text einzugeben.	
	Art der Daten	Klicken Sie hier, um Text einzugeben.	
	Zweck der Daten Mitteilung	Klicken Sie hier, um Text einzugeben.	
	Welche geeigneten Garantien gem. Art. 46 DS-GVO werden im Zusammenhang mit der Übermittlung gegeben?	Garantien bestehen durch: ☐ verbindliche interne Datenschutzvorschriften,	

[9] Hinweis Nr. 9 der Anlage 1
[10] Hinweis Nr. 10 der Anlage 1
[11] Hinweis Nr. 11 der Anlage 1
[12] Hinweis Nr. 12 der Anlage 1

		☐ von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln ☐ von einer Aufsichtsbehörde genehmigte Vertragsklauseln	
	Bei Nichtvorliegen eines Angemessenheitsbeschlusses nach Art. 45 Abs. 3 DS-GVO und geeigneter Garantien nach Art. 46 DS-GVO: Welcher Ausnahmetatbestand nach Art. 49 Abs. 1 DS-GVO wird erfüllt?	Wählen Sie ein Element aus.	
5. Regelfristen für die Löschung der Daten[13]			
	Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Löschungsfristen?	☐ ja, falls ausgewählt bitte benennen: Klicken Sie hier, um Text einzugeben. ☐ nein	
	Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:	**Papieroriginal** Originale werden nach der Aufbewahrungsfrist von 6 Monaten zur Vernichtung den Elbewerkstätten übergeben (gem. § 298 Abs. 2 ZPO und § 55b Abs. 6 VwGO). **Sachbearbeiterdaten** Das Posteingangsbuch protokolliert Arbeitsschritte an einem Dokument. Diese Information hängt nicht an dem Digitalisat, sondern wird in der Datenbank gespeichert. Nach einer Frist von einem Jahr, ab dem das Dokument in das Posteingangsbuch gelangt ist, werden die Daten zu den Arbeitsschritten anonymisiert bzw., die Arbeitnehmerdaten aus der Datenbank gelöscht. Es kann danach keine Schlussfolgerung, wer an einem Poststück gearbeitet hat, gezogen werden. Dieser Prozess wird automatisch durch das Posteingangsbuch angestoßen. **Digitalisat (PDF)** Das Digitalisat liegt in PDF/A Form vor. Bei der Löschung wird nur dieses betrachtet. Nicht personenbezogene Metadaten bleiben hiervon unberührt. Das Poststück kann drei Endzustände erreichen: Storniert, Erledigt (ohne Veraktung) und Erledigt (mit Veraktung). Für die ersten zwei Status gilt: Es wurde eine Aufbewahrungsfrist von 80 Tagen festgelegt. Diese beginnt ab dem Tag des Statuswechsels. Nach Ablauf der Frist wird die PDF aus dem Eldorado des Posteingangsbuches gelöscht. Für den Status Erledigt (mit Veraktung) gilt: Sofortige Löschung im Eldorado des Posteingangsbuchs. Das Poststück wechselt den Eldorado Mandanten, da eine	

[13] Hinweis Nr. 13 der Anlage 1

		Verfügung durch die Sachbearbeitung stattgefunden hat. Ab dem Export gelten die Löschregeln des jeweiligen Zielmandanten (der Behörde/des Amtes).	
6. Mittel der Verarbeitung (optional) **Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?[14]**			
	Bezeichnung: Hersteller: Funktionsbeschreibung: Bereitstellung:	IT-Verfahren ePob xSuite/ Futuresoft / Dataport AöR / Canon Siehe 2.1 ☒ Eigenentwickelte/ individuelle Software ☒ Standard-Software ☐ Cloud-Services ☐ Sonstige: Klicken Sie hier, um Text einzugeben.	
7. Zugriffsberechtigte Personengruppen (vereinfachtes Berechtigungskonzept)[15]			
	Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte Berechtigungskonzept:	Rechte- und Rollenkonzept basiert auf der Zuordnung der Mitarbeiter über entsprechende Gruppen innerhalb des Activ Directory Der Zugang der Benutzer für ePob ist allein aus dem FHH-Netz möglich und erfolgt durch eine individuelle Benutzerkennung/Rolle mit dazugehörigem Passwort. Im Rahmen des Berechtigungskonzeptes wird dargestellt, welche Personenkreise Zugriffe für die Erledigung der ihnen übertragenen Dienstaufgabe benötigen und diese ordnungsgemäß erhalten. Das Berechtigungskonzept basiert auf der Zuordnung der Beschäftigten zu eingerichteten Benutzergruppen. Durch diese Struktur wird sichergestellt, dass nur berechtigte Personen Zugriff auf die jeweils benötigten Daten haben. (siehe Berechtigungskonzept)	
8. Sicherheit der Verarbeitung (Risikoprüfung), Datenschutz-Folgenabschätzung und Technische und organisatorische Maßnahmen[16]			
8.1	Hinsichtlich der Datensicherheitsmaßnahmen wurde der Bereich IT-Sicherheit (z.B. InSiBe der OE) eingebunden?	☐ ja ☐ nein	
8.2	Die allgemeine Zielsetzung aus dem Rahmensicherheitskonzept wurde sichergestellt.	☒ ja ☐ nein, Abweichungen erläutern: Klicken Sie hier, um Text einzugeben.	RaSiKo
8.3	Werden bei der Verarbeitung die Grundsätze des Datenschutzes durch Technikgestaltung (privacy by design) gem. Art 25 Abs. 1 DS-GVO und der datenschutzfreundlichen Voreinstellungen (privacy by	☒ ja (ggf. Betriebs-/Herstellerkonzept beifügen) ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	

[14] Hinweis Nr. 14 der Anlage 1
[15] Hinweis Nr. 15 der Anlage 1
[16] Hinweis Nr. 16 der Anlage 1

	default) gem. Art 25 Abs. 2 DS-GVO eingehalten?[17]		
8.4	Es wurden die Schutzbedarfsfeststellung und die Risikoprüfung gem. Art. 32 DS-GVO mittels Datenbank (Tool Schutzbedarfsfeststellung) durchgeführt und die Ergebnisse gem. Nutzungshinweisen ausgedruckt bzw. elektronisch gespeichert. Alternativ wurde analog (auf Papier) gem. der Darstellung aus dem BSI-Standard 200-2 eine Risikoprüfung durchgeführt.	☒ ja ☐ nein Bitte Ergebnis der Risikoprüfung als Anlage beifügen.	Link zur Datenbank bzw. pdf-Format BSI-Standard
8.5	Es wurden die Erforderlichkeitsprüfung („Schwellwertanalyse“) und ggf. die Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO durchgeführt.	☒ ja, Ergebnis der Erforderlichkeitsprüfung („Schwellwertanalyse“) und ggf. die durchgeführte DSFA als Anlage beifügen ☐ nein	Schwellwertanalyse; DSFA
8.6	Bei Verfahren, die bei Dataport gehostet werden: Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMS der FHH sichergestellt (vgl. Anlage 3).	☒ Es liegt ein Verfahren vor, das bei Dataport gehostet wird.	
8.7	Bei Verfahren, die nicht bei Dataport gehostet werden: Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMs laut Anlage 2 sichergestellt.	☐ Es liegt kein Verfahren vor, das bei Dataport gehostet wird. ☐ Die Anlage 2 wurde ausgefüllt und liegt vor.	
8.8	Es liegen schriftlich vor	☐ interne Verhaltensregeln ☐ DSFA ☒ Risikoprüfung/ Schutzbedarfsfeststellung ☐ allg. Datensicherheitsbeschreibung ☐ umfassendes Datensicherheitskonzept ☒ Wiederanlauf- bzw. Notfallkonzept ☐ Sonstiges: Klicken Sie hier, um Text einzugeben.	
9. Datenübertragbarkeit[18] (Datenportabilität)			
	Nur bei - auf Grundlage einer Einwilligung- zur Verfügung gestellten Daten: Ist der Export der verarbeiteten Daten an den Betroffenen oder andere Dienste in einem gängigen, standardisierten Format möglich?	☐ ja, Format: Als csv Datei Als Datei im csv Format ☒ nein, Begründung: Keine Suchmöglichkeiten/ Keine langfristige Speicherung	

[17] Hinweis Nr. 17 der Anlage 1
[18] Hinweis Nr. 18 der Anlage 1

10. Informationen der Betroffenen[19]			
	Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?	Klicken Sie hier, um Text einzugeben.	Link zu den Formularen
11. Sonstiges			
	Anmerkungen:	Klicken Sie hier, um Text einzugeben.	

…….. …….. ……
Verantwortlicher Datum Unterschrift

[19] Hinweis Nr. 19 der Anlage 1

.

Anlage 1**:**

Hinweise zum Formular

Hinweis Nr. 1
»Personenbezogene Daten« sind nach Art. 4 Nr.1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Dies umfasst z. B. Name, Geburtsdatum, Anschrift, Einkommen, Beruf, Kfz-Kennzeichen, Konto- oder Versicherungsnummer. Auch pseudonymisierte Daten, zum Beispiel eine IP-Adresse oder Personalnummer, aus denen die betroffene Person indirekt bestimmbar wird, gelten als personenbezogene Daten. Die Verarbeitung der personenbezogenen Daten muss im IT-Verfahren der Hauptzweck sein.

Hinweis Nr. 2
Gemeint ist, welche Verarbeitungstätigkeiten durch das Verfahren berührt werden. Folgende Definitionen beschreiben die einzelnen Verarbeitungsschritte:

Erheben	Beschaffen von Daten über eine betroffene Person. Gezielte Verwandlung eines unbekannten Datums in ein Bekanntes. Setzt aktives Handeln des Verantwortlichen voraus. Gilt nicht, wenn der/dem Verantwortlichen eine Information aufgezwungen wird.
Erfassung	Technische Formgebung erhobener Daten. Arbeitsvorgang mit dem eine erstmalige Speicherung des bekannten Datums auf einem Datenträger erfolgt. Ermöglicht die weitere technische Verarbeitung. Gilt auch, wenn Datum aufgezwungen wurde.
Organisieren	Strukturelle Neuanordnung/systematische Strukturierung der gespeicherten personenbezogenen Daten auf dem Datenträger. Organisation personenbezogener Daten bezeichnet das Ergebnis des Sammelns und Ordnen von Daten. Vereinfacht das Auffinden und Auswerten.
Ordnen	Sinnvoll strukturierte Ablage der gespeicherten personenbezogenen Daten auf dem Datenträger, z.B. nach Alphabet.
Speichern	Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Umfasst nicht nur die erstmalige Speicherung, sondern auch Zwischenspeicherungen auf Datenträger oder das Umspeichern von personenbezogenen Informationen, um diese für eine weitere Verwendung aufzubewahren. Die Aufbewahrung des Speichermediums zählt ebenfalls dazu. Gegenteil von Löschen und Vernichten.
Anpassen	Beispiel für Veränderung. Aktualisierung/Angleichung der personenbezogenen Daten an die reellen Lebensumstände, z.B. Änderung der Wohnanschrift.
Verändern	Bearbeitung bzw. inhaltliche Umgestaltung gespeicherter personenbezogener Daten oder ihrer Zuordnung. Es kommt zu einer Änderung des Informationsgehalts. Sie können jedoch auch verändert werden, indem sie ergänzt, in einen neuen Zusammenhang gestellt oder für einen anderen Zweck verwendet werden.
Auslesen	Bewusste Kenntnisnahme über die auf einem Datenträger befindlichen personenbezogenen Daten/Abrufen von Informationen. Daten werden aus einem Datenträger ausgelesen, um sie einer weiteren Bearbeitung zugänglich zu machen.
Abfragen	Gezielte Informationssuche auf einem Datenträger und Kenntnisnahme dieser/Gewinnung von Daten. Zum Beispiel mithilfe der Eingabe eines Suchbegriffs.
Verwenden	Alle Beispiele außer Erheben und Erfassen sind Unterbeispiele von Verwenden. Jeder gezielte Umgang mit personenbezogenen Daten kann als Verwendung der Daten gelten. Sinngemäße Nutzung einer bereits bekannten Information.
Offenlegen	Vorgang, der dazu führt, dass Daten für andere zugänglich gemacht werden und sie diese auslesen oder abfragen können. Bekanntgabe bekannter gespeicherter Daten an Dritte.
- **durch Übermittlung**	Gezielte Weitergabe von Daten an einen oder mehrere Empfänger.

.

- **durch Verbreitung**	Ungezielte Weitergabe an unbestimmte Adressaten z.B. Öffentlichkeit.
- **durch andere Form der Bereitstellung**	Passive Form der Offenlegung. Bereithaltung der Daten zum potenziellen Gebrauch, z.B. für eine Einsicht.
Abgleichen	Vergleich mehrerer zusammengehöriger bekannter, nicht am selben Ort gespeicherter Daten. Abweichungen oder Übereinstimmungen können festgestellt werden.
Verknüpfen	Zuordnung mehrerer zusammengehöriger bekannter, nicht am gleichen Ort gespeicherter Daten. Ziel ist die Entstehung einer neuen Datenstruktur durch Zusammenführung der Daten. (Dient z.B. der Erleichterung der Durchführung von Abfragen).
Einschränken	Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken (Art. 4 Nr. 3). Entspricht der Sperrung von Daten.
Löschen	Entfernung/Unkenntlichmachung einer gespeicherten Information von jedem Datenträger, sodass die Daten keinesfalls mehr ausgelesen bzw. wiederhergestellt werden können. Der Datenträger kann physisch erhalten bleiben. Es erfolgt kein Löschen durch Verschlüsselung oder Anonymisierung der Daten.
Vernichten	Physische Beseitigung der Daten. Vollständige Zerstörung des Datenträgers, sodass keinerlei Information mehr auslesbar ist.

Hinweis Nr. 3
Geplanter oder tatsächlicher Beginn der Verarbeitung von personenbezogenen Daten (wann ist das Verfahren in Betrieb genommen bzw. wann wird es in Betrieb gehen). Dabei ist schon die erstmalige Übertragung oder Speicherung von Daten relevant.

Hinweis Nr. 4
Nur bei Beendigung der Verarbeitung auszuwählen. Bei Auswahl kann das ursprüngliche Erfassungsformular verwendet werden. In Abstimmung mit dem Datenschutzbeauftragten der OE ist über die weitere Verwendung des Datenbestands zu entscheiden, also ob Löschung oder Migration in andere Verfahren erforderlich ist.

Hinweis Nr. 5
Gemeint ist die Behörde, das Bezirksamt oder eine sonstige Organisationseinheit (z.B. Landesbetrieb). Bei der Eintragung sollten keine konkreten Namen sondern Funktionsbezeichnungen (z.B. Präses der Behörde … , Geschäftsleitung des Landesbetriebes …) genannt werden.

Hinweis Nr. 6
Dient der Transparenz in der Auftragsverarbeitung, der Sicherstellung einer sorgfältigen Auswahl des Dienstleisters, dem Nachweis eines Vertrags und der Wahrnehmung der Kontrollpflichten.

Hinweis Nr. 7
Zieldefinition der Verarbeitung personenbezogener Daten und Nennung der darauf gerichteten rechtlichen Grundlage (Prinzip des Verarbeitungsverbots mit Erlaubnisvorbehalt).

Hinweis Nr. 8
Konkrete Beschreibung des Zwecks der Datenverarbeitung und der Datenverarbeitung selbst. Es empfiehlt sich, entsprechende Erläuterungen möglichst unter der in der Behörde bekannten Terminologie zu formulieren und in Zweifelsfällen Rücksprache mit dem Datenschutzbeauftragten der OE zu halten.

Hinweis Nr. 9
Nennung der durch die Verarbeitung betroffenen Personengruppen, z. B. Beschäftigte (Mitarbeiter(-gruppen)), Berater, Kunden, Lieferanten, Patienten, Schuldner, Versicherungsnehmer, Interessenten.

Hinweis Nr. 10
Datenkategorien werden verwendet, um die jeweiligen Metadaten kategorisiert abbilden zu können.
Beispiele für Datenkategorien: Identifikations- und Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten (z. B. Verbindungsdaten, Logging-Informationen).

Hinweis Nr. 11
Die Verarbeitung besonderer Kategorien personenbezogener Daten ist in Art. 9 Abs. 1 DS-GVO geregelt. Umfasst sind Verarbeitungen von Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Eine Verwendung dieser besonders schutzbedürftigen Daten führt zwangsläufig zu einem hohen Schutzbedarf und es ist in jedem Fall eine Datenschutzfolgenabschätzung durchzuführen.

Hinweis Nr. 12
Hier werden die Empfänger personenbezogener Daten zur Weiterverarbeitung bzw. Nutzung innerhalb der verantwortlichen Stelle oder im Rahmen einer Übermittlung an Dritte erfasst..

»Empfänger« ist jede Person oder Stelle, die Daten erhält, z. B. Vertragspartner, Kunden, Behörden, Versicherungen, ärztliches Personal, Auftragsverarbeiter (z. B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter), oder ein Verfahren, bzw. Geschäftsprozess, an den Daten weitergegeben werden.

Interne Empfänger sind jede Empfänger innerhalb des Verantwortungsbereiches bzw. innerhalb der Organisationseinheit. Organisationseinheit meint Behörde, Bezirksamt oder sonstige Organisationseinheit (z.B. Landesbetrieb).

Externe und Dritte sind jede Empfänger außerhalb des Verantwortungsbereiches, z.B. auch andere Behörden innerhalb der Verwaltung und Behörden der Bundesverwaltung und Empfänger außerhalb der Verwaltung.

Sobald Daten im Filesystem gespeichert werden, ist automatisch eine Übermittlung von Daten an Dritte, hier Dataport, gegeben.

Die Art der Daten oder Datenkategorien ist getrennt nach dem jeweiligen Drittstaat und den jeweiligen Empfängern oder Kategorien von Empfängern anzugeben.

Hinweis Nr. 13
Gemäß Art. 5 Abs. 1 lit. e DS-GVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Unter Beachtung (z.B. steuer-) gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen müssen die Daten nach Zweckfortfall unverzüglich gelöscht werden. Wird keine Löschung ausgewählt oder bei Zweifeln zu Aufbewahrungsfristen und Löschroutinen ist Rücksprache mit dem Datenschutzbeauftragten der OE zu halten.

Hinweis Nr. 14
Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur angegeben werden, um ein besseres Verständnis der Beschreibung der technischen und organisatorischen Maßnahmen zu ermöglichen.
Im Rahmen der Bürokommunikation werden verschiedene IT-Infrastrukturen (z.B. Computer Cloud Mail System, Telefonie, SharePoint) in Anspruch genommen. Diese sollen nicht extra erwähnt werden. Die entsprechenden IT-Infrastruktur-Beschreibungen müssen von den Fachlichen Leitstellen vorgenommen werden.

Hinweis Nr. 15
Skizzierung des Berechtigungsverfahrens und Nennung der berechtigten Gruppen. Sofern vorhanden kann auf ein umfassendes Berechtigungskonzept verwiesen werden.

Sollte bei zu überführenden Verfahren ein Zugriffsberechtigungskonzept bereits Teil der durchgeführten Risikoanalyse sein, dann auf dieses verwiesen werden.

Hinweis Nr. 16
Beschreibung der Schutzmaßnahmen im Hinblick auf die Kontrollziele für die jeweils verarbeiteten personenbezogenen Daten. Nähere Ausführungen zu den Anforderungen an Schutzmaßnahmen kann der Anlage 2 entnommen werden.

Ergänzend kann auf die ISO 27001 Bezug genommen werden. Die Kontrollziele zur angemessenen Sicherung der Daten vor Missbrauch und Verlust sind dabei nicht abschließend oder als in Gänze verpflichtender Maßnahmenkatalog zu sehen. So könnten aufgrund einer Spezialgesetzgebung zum Datenschutz weitere Kontrollziele und entsprechende Maßnahmen gefordert sein (z. B. aus dem Telekommunikationsgesetz, aus der Sozialgesetzgebung, oder aus den Landesdatenschutzgesetzen).

Bei nicht automatisierten Verfahren sind nur die organisatorischen Maßnahmen zu benennen.

Hinweis Nr. 17
Nach Art. 25 der DS-GVO müssen geeignete Mittel für die Verarbeitung festgelegt sowie technische und organisatorische Maßnahmen getroffen werden, die dazu ausgelegt sind, die Datenschutzvorgaben aus der Datenschutzverordnung wirksam umzusetzen und die Rechte der Betroffenen Personen zu schützen.

Hinweis Nr. 18
Bei Verarbeitungen auf Grundlage eines Vertrages oder einer Einwilligung, für die die Betroffenen den Behörden Daten bereitgestellt haben, haben sie nach Art. 20 DS-GVO das Recht, diese sie betreffenden personenbezogenen Daten, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder sie an einen anderen Verantwortlichen übermitteln zu lassen, sofern dies technisch machbar ist.

„Soweit technisch machbar“ bedeutet, dass Verantwortliche bereits über entsprechende Einrichtungen verfügen, diese aber nicht neu implementieren müssen, um ein Recht auf Datenportabilität erfüllen zu können.

Hinweis Nr. 19
Nach Art. 12 der DS-GVO müssen beim Verantwortlichen geeignete Maßnahmen getroffen werden, um den Betroffenen die in Art. 13 und 14 DS-GVO aufgeführten Angaben, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Dies kann schriftlich oder in einer anderen Form, z.B. elektronisch erfolgen.

.

Anlage 2

Übersicht und Erläuterungen zu den technischen und organisatorischen Maßnahmen

Grundwerte	ergriffene TOMs
Datenminimierung Art. 5 Abs. 1 lit.c DS-GVO	
Gewährleistung der **Integrität** Art. 32 Abs. 1 lit. b DS-GVO	
Gewährleistung der **Verfügbarkeit** Art. 32 Abs. 1 lit. b DS-GVO	
Gewährleistung der **Vertraulichkeit** Art. 32 Abs. 1 lit. b DS-GVO	
Intervenierbarkeit Art. 5 Abs. 1 lit. d,f DS-GVO	
Nichtverkettung Art. 5 Abs. 1 DS-GVO	
Transparenz Art. 5 Abs. 1 lit. a DS-GVO	
Gewährleistung der **Belastbarkeit der Systeme** Art. 32 Abs 1 lit. b DS-GVO	
Verfahren **regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** Art. 32 Abs. 1 lit. d DS-GVO	
Verfahren zur **Wiederherstellung der Verfügbarkeit** personenbezogener Daten nach einem physischen oder technischen Zwischenfall Art. 32 Abs. 1 lit. c DS-GVO	

Erläuterungen zu den Technischen und organisatorischen Maßnahmen gem. Art. 30 Abs. 1 S. 2 lit. g DS-GVO

Trotz der Formulierung „wenn möglich“ stellt die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO hier den Regelfall dar.
Art. 5 Abs. 2 DS-GVO verpflichtet den Verantwortlichen insbesondere auch zur Dokumentation der technischen und organisatorischen Maßnahmen (Art. 5 Abs. 1 lit. f DS-GVO). Zudem muss der Verantwortliche die Wirksamkeit dieser Maßnahmen regelmäßig überprüfen (Art. 32 Abs. 1 lit. d DS-GVO). Beide Forderungen kann der Verantwortliche nur erfüllen, wenn die technischen und organisatorischen Maßnahmen vollständig beschrieben sind (etwa in einem Sicherheitskonzept).

Eine Verarbeitung darf erst erfolgen, wenn der Verantwortliche seiner Pflicht nach Art. 24 DS-GVO nachgekommen ist. Darunter fallen neben den Verpflichtungen nach Art. 12 und 25 DS-GVO auch diejenigen nach Art. 32 DSGVO zur Bestimmung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das betrifft primär Fragen der Sicherheit der Verarbeitung, schließt somit aber

auch Maßnahmen zur Gewährleistung von Betroffenenrechten ein. In das Verzeichnis ist eine allgemeine, einfach nachvollziehbare Beschreibung der für diesen Zweck getroffenen Maßnahmen aufzunehmen.

Die Beschreibung der jeweiligen Maßnahme ist konkret auf die Kategorie betroffener Personen bzw. personenbezogener Daten im Sinne des Art. 30 Abs. 1 S. 2 lit. c DS-GVO zu beziehen, soweit eine entsprechende Differenzierung in ihrer Anwendung erfolgt.

Für die Bestimmung der zu treffenden Maßnahmen wird auf das Standard-Datenschutzmodell, die Leitlinien und Orientierungshilfen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und der Artikel-29-Arbeitsgruppe sowie auf die bestehenden nationalen und internationalen Standards (z. B. BSI-Grundschutz, ISO-Standards) verwiesen. Ist bei der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zu erwarten, hat die Bestimmung der Maßnahmen bereits im Rahmen einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO zu erfolgen.

Eine Verletzung der Sicherheit der Datenverarbeitung ist immer eine Verletzung des Schutzes personenbezogener Daten i. S. v. Art. 4 Nr. 12 DS-GVO.

Nach Art. 32 Abs. 1 DS-GVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der mit ihr verbundenen Risiken geeignete technische und organisatorische Maßnahmen zu treffen, um insbesondere Folgendes sicherzustellen:

Maßnahmenbereiche, die sich aus Art. 32 Abs. 1 DS-GVO ergeben:

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste
- Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
- Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Nachfolgend werden den einzelnen Bereichen typische, bewährte technische und organisatorische Maßnahmen zugeordnet. Die Auflistung ist nicht vollständig oder abschließend. In Abhängigkeit von den konkreten Verarbeitungstätigkeiten können weitere oder andere Maßnahmen geeignet und angemessen sein. Auch ist die Zuordnung einzelner Maßnahmen zu einem bestimmten Maßnahmenbereich nicht in jedem Fall eindeutig.

Hinweis: Wird das Verfahren in der IT-Infrastruktur der FHH betrieben (dazu zählt auch das Dataport Rechenzentrum) greifen grundlegend die TOMs Sicherheits- und Betriebskonzept Rechenzentrum Dataport und die Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten (vgl. teilweise Tabelle Anlage 3).

Maßnahmen zur Pseudonymisierung personenbezogener Daten

Hierzu zählen u. a.:

- Festlegung der durch Pseudonymisierung zu ersetzenden identifizierenden Daten
- Definition der Pseudonymisierungsregel, ggf. anknüpfend an Personal-, Kunden- oder Patienten-Kennziffern
- Autorisierung: Festlegung der Personen, die zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind
- Festlegung der zulässigen Anlässe für Pseudonymisierungs- und Depseudonymisie-rungsvorgänge
- zufällige Erzeugung der Zuordnungstabellen oder der in eine algorithmische Pseudony-misierung eingehenden geheimen Parameter
- Schutz der Zuordnungstabellen bzw. geheimen Parameter sowohl gegen unautorisierten Zugriff als auch gegen unautorisierte Nutzung
- Trennung der zu pseudonymisierenden Daten in die zu ersetzenden identifizierenden und die weiteren Angaben

Maßnahmen zur Verschlüsselung personenbezogener Daten
(z. B. in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport)

Schlüssel können flüchtig (z. B. für die Dauer eines Kommunikationsvorgangs) oder statisch (mittel- oder langfristig)

für den Schutz personenbezogener Daten eingesetzt werden.

Es sind Festlegungen zu treffen (z. B. im Rahmen eines Kryptokonzepts) u. a. zur Auswahl geeigneter kryptografischer Verfahren und Produkte, zur Organisation ihres Einsatzes, zu Maßnahmen bei der Entdeckung von Schwächen in Verschlüsselungsverfahren oder -produkten (Um- oder Überverschlüsselung) sowie zu Schlüssellängen. Voraussetzung für effektive Verschlüsselung ist ein adäquates Schlüsselmanagement, das u. a. folgende Aspekte betrifft:

- zufällige Erzeugung der Schlüssel
- Autorisierung von Personen zur Verwaltung und zur Nutzung von Schlüsseln bzw. ihre Zuweisung zu Geräten, in denen sie eingesetzt werden
- zuverlässige Schlüsselverteilung, Verknüpfung von Schlüsseln mit Identitäten von natürlichen Personen oder informationstechnischen Geräten, ggf. Einbringen in speziell gesicherte Speichermedien (z. B. Chipkarten)
- Schutz der Schlüssel vor nicht autorisiertem Zugriff oder Nutzung
- regelmäßiger oder situationsbezogener Schlüsselwechsel, ggf. eine Schlüsselarchivierung, stets sorgfältige Schlüssellöschung nach Ablauf des Lebenszyklusses
- Verwaltung des Lebenszyklus der Schlüssel von Erzeugung und Verteilung über Nutzung bis zu ihrer Archivierung und Löschung

Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste

Die folgenden Maßnahmen sollen eine spezifikationsgerechte Verarbeitung sichern und nicht autorisierte bzw. unberechtigte Verarbeitung sowie unbeabsichtigte Änderung, Verlust oder Schädigung personenbezogener Daten ausschließen; beim Verantwortlichen selbst oder auf dem Transportweg zu Auftragsverarbeitern oder Dritten.

Hierzu zählen u. a.:

- Formulierung von verbindlichen Sicherheitsleitlinien
- Definition der Verantwortlichkeiten für das Informationssicherheitsmanagement
- Inventarisierung der zu verarbeitenden personenbezogenen Daten
- Inventarisierung der Informationstechnik
- Erarbeitung eines Sicherheitskonzepts, ggf. unter Durchführung einer Risikoanalyse
- Personalsicherheit: Überprüfung und Verpflichtung des Personals, Sensibilisierung und Training, Aufgabentrennung
- Spezifikation der Sicherheitsanforderungen an Informationssysteme und deren Konfiguration, Prüfung ihrer Einhaltung
- Schutz vor unberechtigtem physischem Zugang, einschließlich Schutz von Mobilgeräten
- Erarbeitung eines Rollen- und Rechtekonzepts
- Maßnahmen zur Autorisierung von Personen für den Zugriff auf personenbezogene Daten und die Steuerung der Verarbeitung
- Zugriffskontrolle und sicherer Umgang mit Speichermedien, einschließlich der Maßnahmen zur zuverlässigen Authentisierung von Personen gegenüber der Informationstechnik, zur Sicherung der Revisionsfähigkeit der Eingabe und der Änderung von personen- bezogenen Daten sowie ggf. der Nutzung und des Zugriffs auf diese und zur Revision dieser Prozesse
- Maßnahmen der Betriebssicherheit, insbesondere zur Spezifikation der Bedienabläufe, zur Änderungssteuerung, zum Schutz vor Malware, zum Umgang mit technischen Schwachstellen, zur kontrollierten Installation und Konfiguration neuer Software, sowie zur Ereignisüberwachung und -protokollierung, einschließlich der regelmäßigen und anlassbezogenen Auswertung dieser Protokolle
- Maßnahmen, die (berechtigte oder unberechtigte) Veränderung gespeicherter oder übertragener Daten nachträglich feststellbar machen (z. B. Signaturverfahren, Hashverfahren)
- Maßnahmen zur Kommunikationssicherheit: Netzwerksicherheitsmanagement, insbesondere zur Kontrolle und Einschränkung des Datenverkehrs (Firewalls, Application Layer Gateways), Einrichtung von Sicherheitszonen, Authentisierung von Geräten gegeneinander
- sichere Gestaltung von Informationsübertragungen, einschließlich des Abschlusses von Vereinbarungen mit regelmäßigen Übermittlern und Empfängern personenbezogener Daten und der Authentisierung der Kommunikationspartner
- Sicherung und Überprüfung der Authentizität der übermittelten Daten
- sichere Einbeziehung von externen Diensten
- Management von Informationssicherheitsvorfällen
- Aufrechterhaltung der Informationssicherheit bei ungeplanten Systemzuständen
- Durchführung von internen oder externen Sicherheitsaudits
- logische oder physikalische Trennung der Datenverarbeitung z. B. nach verantwortlichen Stellen, den verfolgten Verarbeitungszwecken und nach Gruppen betroffener Personen

.

- sicheres, rückstandsfreies Löschen von Daten bzw. Vernichten von Datenträgern nach Ablauf der Aufbewahrungsfristen, Festlegungen zu Löschverfahren und zur Beauftragung von Dienstleistern

Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste

Die folgenden Maßnahmen sollen sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden.

Hierzu zählen u. a.:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage z. B. DDOS, höhere Gewalt)
- Dokumentation von Syntax und Semantik der gespeicherten Daten
- Redundanz von Hard- und Software sowie Infrastruktur
- Umsetzung von Reparaturstrategien und Ausweichprozessen
- Vertretungsregelungen für abwesende Mitarbeiter

Maßnahmen, um nach einem physischen oder technischen Zwischenfall (Notfall) die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen rasch wiederherzustellen.

Eine besondere Ausprägung der Gewährleistung von Verfügbarkeit ist hinsichtlich möglicher Notfälle (siehe dazu auch BSI Standard 100-4) erforderlich.

Hierzu sind u. a. folgende Maßnahmen erforderlich:

- Erstellung und Umsetzung eines Notfallkonzepts
- Erarbeitung eines Notfallhandbuches
- Integration des Notfallmanagements in Geschäftsprozesse
- Durchführung von Notfallübungen
- Erprobung von Wiederanlaufszenarien

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Hierzu zählen u. a.:

- regelmäßige Revision des Sicherheitskonzepts
- Information über neu auftretende Schwachstellen und andere Risikofaktoren, ggf. Überarbeitung der Risikoanalyse und -bewertung
- Prüfungen des Datenschutzbeauftragten und der IT-Revision auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme
- externe Prüfungen, Audits, Zertifizierungen

Weitere Maßnahmenbereiche, die sich aus der DS-GVO ergeben und deren Darstellung im Verzeichnis empfohlen wird:

Die Formulierung in Art. 32 Abs. 1 DS-GVO „diese Maßnahmen schließen unter anderem Folgen des ein“ verdeutlicht, dass die dort vorgenommene Aufzählung nicht abschließend ist. Die Sicherheit der Verarbeitung ist u. a. auch Voraussetzung dafür, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden (Zweckbindung), dass Betroffene, Verantwortliche und Kontrollinstanzen u. a. erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden (Transparenz) und dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden (Intervenierbarkeit). Entsprechend sind auch die Maßnahmenbereiche zu berücksichtigen, die vorrangig der Minimierung der Eingriffsintensität in die Grundrechte Betroffener dienen.

Maßnahmen zur Gewährleistung der Zweckbindung personenbezogener Daten (Nichtverkettung) – Art. 5 Abs. 1 lit. b) DS-GVO:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten

.

- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
- Trennung nach Organisations-/Abteilungsgrenzen
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten
- geregelte Zweckänderungsverfahren

Maßnahmen zur Gewährleistung der Transparenz für Betroffene, Verantwortliche und Kontrollinstanzen – Art. 5 Abs. 1 lit. a) DS-GVO:

- Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren
- Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren
- Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen
- Dokumentation von Einwilligungen und Widersprüchen
- Protokollierung von Zugriffen und Änderungen
- Nachweis der Quellen von Daten (Authentizität)
- Versionierung
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts
- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept

Maßnahmen zur Gewährleistung der Betroffenenrechte – Art. 13 ff. DS-GVO (Intervenierbarkeit):

- differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte
- Einrichtung eines Single Point of Contact (SPoC) für Betroffene
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten

.
Anlage 3

Darstellung der ergriffenen Technischen und Organisatorischen Maßnahmen (TOMs) der FHH im Vergleich zu den TOMS nach BDSG und Grundwerten nach Grundschutz und DS-GVO

Grundwerte nach DS-GVO	Definierte Technische und Organisatorische Maßnahmen (TOMs) nach § 64 BDSG	Ergriffene Technische und Organisatorische Maßnahmen (TOMs) der FHH
Datenminimierung Art. 5 Abs. 1 lit.c DS-GVO	-	Verwaltungsvorschrift IT-Projekte (bei kleineren IT-Projekten wird diese VV sinngemäß angewendet) Richtlinie über Mindestanforderungen an die Sicherheit der Datenverarbeitung auf UNIX-Rechnern (UNIX-Richtlinie)
Gewährleistung der **Integrität** Art. 32 Abs. 1 lit. b DS-GVO	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)
	Datenintegrität (§ 64 Abs. 3 Nr. 11 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Geschäftsbestimmungen der Behörden (Revisionfähige Prozessbeschreibungen, Überprüfbarkeit des Verwaltungshandelns)
	Datenträgerkontrolle (§ 64 Abs. 3 Nr. 2 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich Entsorgungs-Richtlinie
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich

	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzepte der jeweiligen Fachverfahren Grundsätze des Verwaltungshandelns nach Beamtenstatusgesetz bzw. Tarifvertrag (Verschwiegenheitspflicht)
	Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)	Betriebskonzept des jeweiligen Fachverfahrens Geschäftsordnungsbestimmungen der Behörden
	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO
	Zugangskontrolle (§ 64 Abs. 3 Nr. 1 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Datatport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept)
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
Gewährleistung der **Verfügbarkeit** Art. 32 Abs. 1 lit. b DS-GVO	Verfügbarkeitskontrolle (§ 64 Abs. 3 Nr. 13 BSDG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden Richtlinie Regelwerk ELDORADO
	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO

	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL)Rahmen-Sicherheitskonzept der FHH (RaSiKo)Sicherheits- und Betriebskonzept Rechenzentrum DataportGeschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
Gewährleistung der **Vertraulichkeit** Art. 32 Abs. 1 lit. b DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	Freigabe-Richtlinie Service-Level-Agreements Richtlinie zur Datensicherheit im IuK-Bereich
	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzepte der jeweiligen Fachverfahren Grundsätze des Verwaltungshandelns nach

		Beamtenstatusgesetz bzw. Tarifvertrag (Verschwiegenheitspflicht)
	Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)	Betriebskonzept des jeweiligen Fachverfahrens Geschäftsordnungsbestimmungen der Behörden
	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
Intervenierbarkeit Art. 5 Abs. 1 lit. d,f DS-GVO	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO
Nichtverkettung Art. 5 Abs. 1 DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	Freigabe-Richtlinie Service-Level-Agreements Richtlinie zur Datensicherheit im IuK-Bereich
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzepte der jeweiligen Fachverfahren Grundsätze des Verwaltungshandelns nach Beamtenstatusgesetz bzw. Tarifvertrag (Verschwiegenheitspflicht)
	Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)	Betriebskonzept des jeweiligen Fachverfahrens Geschäftsordnungsbestimmungen der Behörden
Transparenz Art. 5 Abs. 1 lit. a DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	Freigabe-Richtlinie Service-Level-Agreements Richtlinie zur Datensicherheit im IuK-Bereich

	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum DataportVorgaben für das Haushalts- und KassenrechtRichtlinie zur Verwaltung von PasswörternGeschäftsordnungsbestimmungen der Behörden
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
Verfahren **regelmäßiger Überprüfung**, **Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** Art. 32 Abs. 1 lit. d DS-GVO	-	turnusmäßige Überarbeitung der Richtlinien der FHH (PDCA-Modell im RaSiKo, IS-LL) turnusmäßige Überarbeitung des Sicherheitskonzeptes durch Dataport
Verfahren zur schnellen **Wiederherstellung der Verfügbarkeit** personenbezogener Daten nach einem physischen oder technischen Zwischenfall Art. 32 Abs. 1 lit. c DS-GVO	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO

Gewährleistung der **Belastbarkeit der Systeme** Art. 32 Abs. 1 lit. b DS-GVO	Verfügbarkeitskontrolle (§ 64 Abs. 3 Nr. 13 BSDG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden Richtlinie Regelwerk ELDORADO
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)

Definitionen der Grundwerte nach DS-GVO:

Datenminimierung:	Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.
Vertraulichkeit:	Gewährleistung, dass Informationen ausschließlich Berechtigten zugänglich sind
Verfügbarkeit:	Gewährleistung, dass Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang und in angemessener Zeit nutzbar sind
Integrität:	Gewährleistung, dass die Unverfälschtheit und Vollständigkeit von Informationen, Anwendungen und IT-Systemen überprüfbar sind
Nichtverkettung:	Erhobene personenbezogene Daten werden nur für den Zweck verarbeitet, zu dem sie erhoben wurden.
Transparenz:	Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.
Intervenierbarkeit:	Gewährleistung von Betroffenenrechten zu Berichtigung, Löschen, Widerspruch und zur Einschränkung der Verarbeitung sowie zur Datenportabilität..

Definitionen der TOMs gem. § 64 BDSG:

Zugangskontrolle:	Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte
Datenträgerkontrolle:	Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern
Speicherkontrolle:	Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten
Benutzerkontrolle:	Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte
Zugriffskontrolle:	Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben

Übertragungskontrolle:	Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können
Eingabekontrolle:	Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind
Transportkontrolle:	Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden
Wiederherstellbarkeit:	Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können
Zuverlässigkeit:	Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden
Datenintegrität:	Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können
Auftragskontrolle:	Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können
Verfügbarkeitskontrolle:	Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind
Trennbarkeit	Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

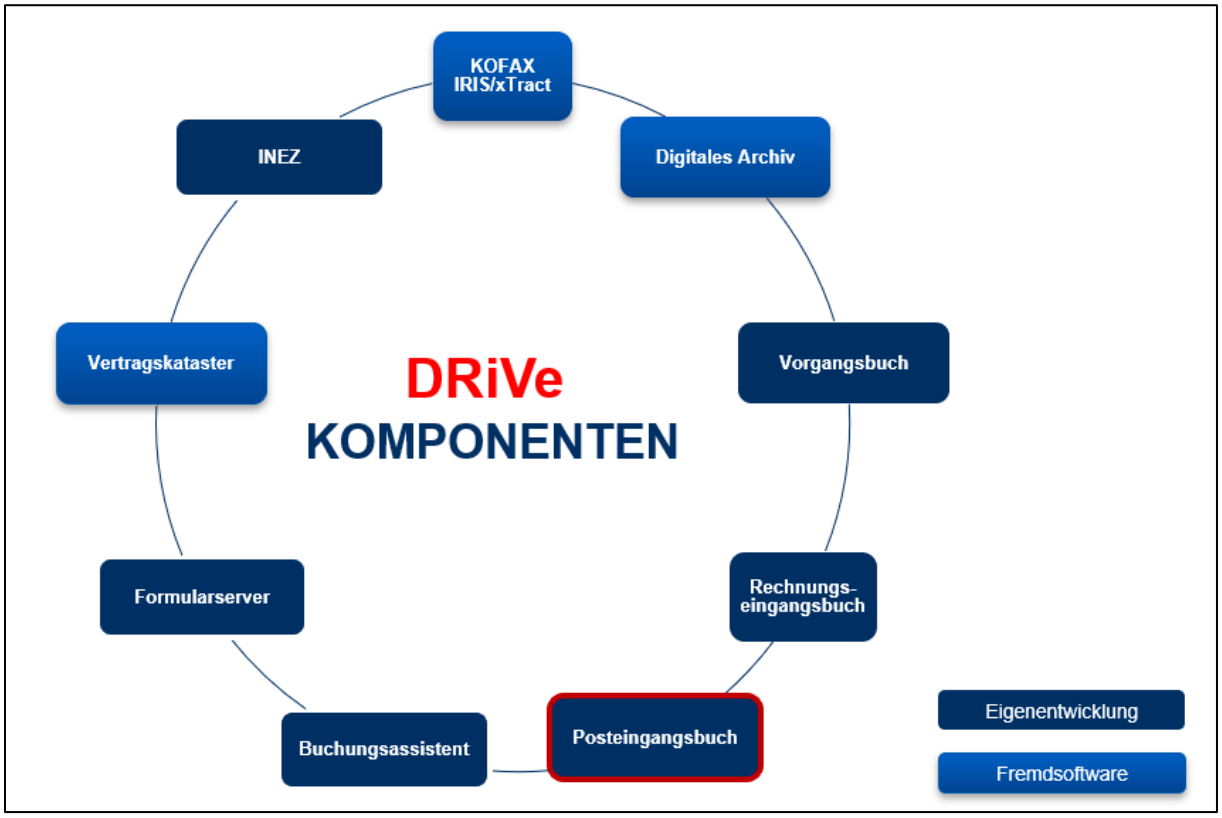
Anlage 2

zur Dienstvereinbarung zur Pilotierung des IT-Verfahrens elektronische Postbearbeitung (ePob)

Fachverfahren ePob als neue Verfahrenskomponente der DRiVe-IT[1]

Das Fachverfahren ePob stellt einen neuen Verfahrensteil innerhalb der DRiVe-IT-Landschaft dar und wurde auf Basis bereits vorhandener DRiVe-Funktionalitäten konzipiert und bereitgestellt.

Abbildung 1: Übersicht der DRiVe-IT



Digitalisierungsprozesse in der DRiVe-IT

Im Folgenden werden die Parallelen zwischen den bereits etablierten Prozessen der DRiVe-IT und dem neuen Verfahren ePob hervorgehoben.

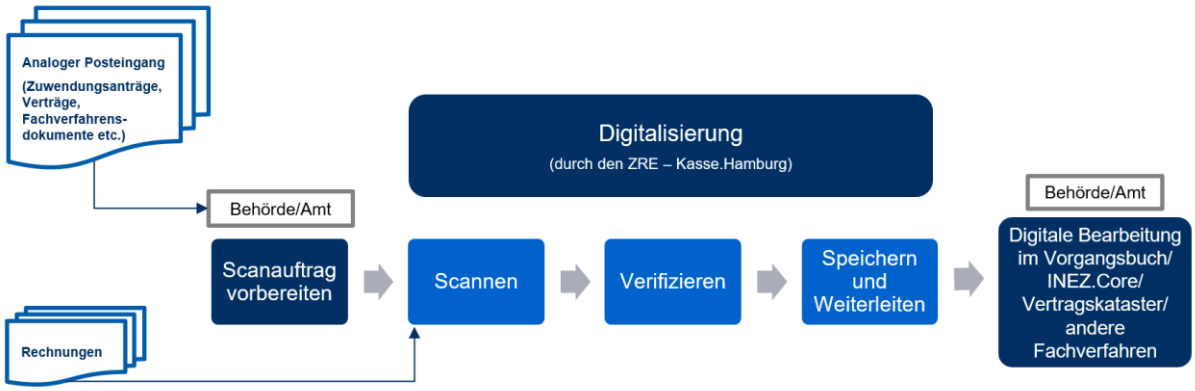
Die Abbildung 2 zeigt den Prozess, welcher für die Digitalisierung der im ZRE (Zentraler Rechnungseingang der Kasse.Hamburg) eingehenden Dokumente (z.B. Rechnungen, Zuwendungsanträge) bereits seit Jahren eingesetzt wird.

Nach der Digitalisierung der Dokumente im ZRE erfolgt eine Weiterleitung in die jeweiligen Zielsysteme der DRiVe-IT (und ggf. weitere angebundene Fachverfahren), in denen eine

[1] DRiVe IT: Digitales Rechnungswesen in der Verwaltung (ehemals Herakles-IT)

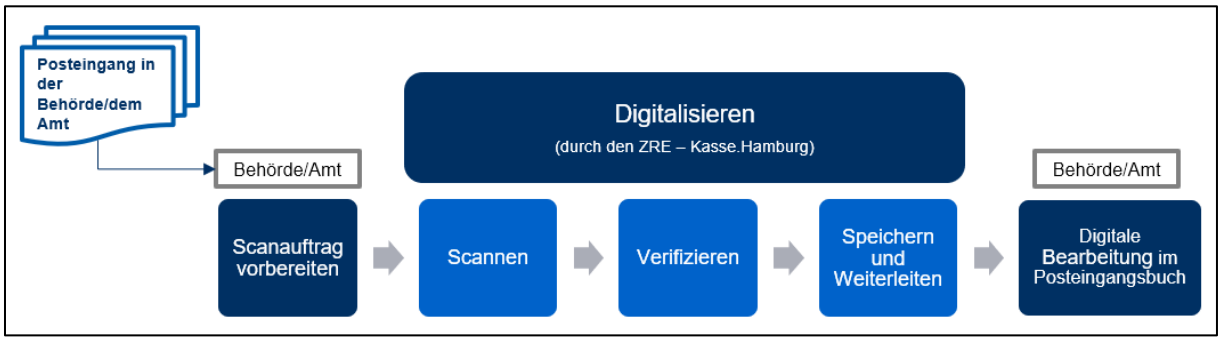
Weiterverarbeitung durch die zuständigen Sachbearbeitungen in den Behörden und Ämtern erfolgt.

Abbildung 2: Übersicht der bereits etablierten Digitalisierungsprozesse der DRiVe-IT



In der Abbildung 3 sowie in der nachfolgenden Tabelle wird der Prozess, wie er zukünftig mit dem neuen Fachverfahren ePob ablaufen wird, dargestellt. Hierbei wird deutlich, dass das neue Verfahren auf die bereits ausgiebig erprobte Komponenten bzw. Prozesse der DRiVe-IT zurückgreift. Primär unterscheiden sich lediglich der Eingangskanal und die dazuzählende Vorbereitung sowie das Zielsystem (Posteingangsbuch), in dem die anschließende Sachbearbeitung erfolgt.

Abbildung 3: Übersicht des Digitalisierungsprozesses für ePob



Prozessschritt	**Beschreibung**
Posteingang in der Behörde/ dem Amt **und** Scanauftrag vorbereiten	Die externe Post erreicht die Behörde/ das Amt. In der Poststelle soll eine Vorsortierung der Post nach den vorgegebenen Kriterien stattfinden. Zusammenhängende Poststücke werden getackert. Es sollen maximal zwei Stapel gebildet werden 1. Poststücke, die in der Kasse.Hamburg verwahrt werden sollen 2. Poststücke, die zurück an den Besitzer gehen sollen Pro Stapel **ein** Scanvorblatt. Die Bündel werden in grüne Boxen gelegt und an die Behördenpost Topas übergeben. Empfänger Kasse.Hamburg
Scannen	Durchzuführen durch Mitarbeitende des ZRE.

	Vorbereitung pro Stapel: 1. Tackernadel entfernen 2. Pro Poststück: erste Seite mit dem Scanbarcode bekleben Die Stapel werden gescannt und die Scanqualität wird überprüft - ggf. Nachscannen.
Verifizieren	Systemseitige Kontrolle der Scanqualität sowie das Auslesen von Metadaten.
Speichern und Weiterleiten	Das Poststück, in Form einer PDF/A, wird in dem Eldoradomandanten des Posteingangsbuches gespeichert. Übergabe der Metadaten und der zugehörigen digitalen Dokumente zur weiteren Bearbeitung zum Posteingangsbuch.
Digitale Bearbeitung	Anzeige des Poststücks und der Metadaten. Eine Veraktung in Eldorado 2.0 kann ggf. durch die Sachbearbeitung vorgenommen werden

Anlage 3

zur Vereinbarung nach § 93 HmbPersVG über die Einführung des Fachverfahrens ePob

Berechtigungs- und Rollenkonzept

im Fachverfahren ePob

Version 1.0

Stand 10.11.2022

Inhalt

1 Ausgangslage

In allen Organisationseinheiten der FHH ist noch ein hoher Anteil an eingehender Papierpost zu verzeichnen. Für die Bearbeitung wird aktuell die Post manuell verteilt. Ziel von ePob (elektronische Postbearbeitung) ist es, die Papiereingänge zu digitalisieren und als strukturierte Dokumente zur weiteren Bearbeitung zu übertragen.

Für die notwendigen Systemzugriffe in ePob werden analog zu den übrigen Verfahren der DRiVe-IT-Verfahren systematische und strukturierte Berechtigungen vergeben.

Im Rahmen des Berechtigungskonzeptes wird dargestellt, welche Personenkreise Zugriffe für die Erledigung der ihnen übertragenen Dienstaufgabe benötigen und diese ordnungsgemäß erhalten. Das Berechtigungskonzept basiert auf der Zuordnung der Mitarbeiter und Mitarbeiterinnen[1] zu eingerichteten Benutzergruppen. Durch diese Struktur wird sichergestellt, dass nur berechtigte Personen Zugriff auf die jeweiligen Daten haben.

2 Ziele

Mit der Einrichtung der Nutzerverwaltung wird eine einheitliche und strukturierte Verwaltung der Berechtigungen auf der Basis des Active Directory umgesetzt. Damit wird sichergestellt, dass die notwendigen Berechtigungen nur einmal hinterlegt und verwendet werden.

3 Zugriff auf ePob im Posteingangsbuch

3.1 Zugriff mittels Single Sign On

Der Zugang der Benutzer auf ePob im Posteingangsbuch ist allein aus dem FHH-Net möglich und erfolgt durch eine individuelle Benutzerkennung mit dazugehörigem Passwort. Hierfür wird der FHH-Account im Active Directory (AD) verwendet. Alle Anwendungen werden mittels Single-Sign-On (SSO) gestartet.

[1] Im weiteren Verlauf des Textes wird zur Vereinfachung der Lesbarkeit bei Begriffen, die sich auf personengruppen beziehen, die männliche Form verwendet, die weibliche Form ist mitgemeint.

Für die Authentifizierung der Benutzer wurde das AD über das LDAP (Lightweight Directory Access Protocol) integriert. Die Passwortprüfung gegen das Passwort des FHH-Netzes und das Auslesen benutzerrelevanter Daten erfolgt immer mit Hilfe von LDAP. Die dazugehörigen Berechtigungen werden durch die Zuordnung zu den entsprechenden Benutzergruppen im Active Directory gesteuert.

3.2 Schutz vor Zugriffen nicht autorisierter Personen

Der Schutz vor Zugriffen durch nicht autorisierte Personen erfolgt vor allem durch den Schutz der Benutzerkennungen mittels Passwörtern. Die erforderlichen Maßnahmen für diesen Schutz ergeben sich aus der Passwort-RL. Da nur ein Zugriff im FHH-Netz möglich ist und dies nur dann erfolgen kann, wenn Benutzer in einer Benutzergruppe im Active Directory gepflegt sind, liegt die Verantwortlichkeit außerhalb von Posteingangsbuch, und es wird sichergestellt, dass die Passwort-RL erfüllt ist.

4 Verwendung der Benutzergruppen

Die Anwender der Behörden und Bezirksämter bearbeiten im Rahmen ihrer Aufgabenwahrnehmung die der Dienststelle obliegenden Posteingänge im Posteingangsbuch. Hierfür werden die zu verwendenden Berechtigungen durch die Fachliche Leitstelle ePob im Posteingangsbuch hinterlegt. Über die Berechtigungen wird gesteuert, inwiefern welche Eingaben und Prüfungen im Rahmen einer systemseitig hinterlegten Prozesskette oder sonstige Eingaben außerhalb der Prozesskette innerhalb der Organisation und der Rollenzugehörigkeit vorgenommen werden dürfen. Gleichermaßen kann eine Einschränkung der Bearbeitungsmöglichkeit durch Vergabe von lediglich Sichtberechtigungen vorgenommen werden.

Die über Posteingangsbuch ablaufenden Prozesse und die organisatorische Einordnung in die jeweiligen Vor- und Genehmigungsstufen werden in der Verfahrensbeschreibung ePob detailliert dargestellt.

5 Notwendige Berechtigungen für das Posteingangsbuch

5.1 Übersicht über die Berechtigungen

Im Rahmen der Berechtigungsverwaltung werden Benutzergruppen festgelegt, die in ePob und den hinterlegten Prozessketten mit unterschiedlichen Aufgaben ausgestattet sind.

Name	**Einsicht**
Art der Aufgabe	Einsichtnahme
Verwendung	Einsichtnahme in die Prozessstufen
Aufgabenbeschreibung:	Leserecht im Bearbeitungsbereich. Die Einsichtnahme erfolgt über die Recherchefunktion und kann grundsätzlich in alle Prozessschritte des Posteingangsbuches genommen werden.
Mögliche Mitarbeitergruppen:	Mitarbeitende der Behörden/ Ämter, die Sichtrechte in die zu bearbeitenden eingescannten Poststücke erhalten sollen.
Berechtigungsprofil	Lesen
Benutzergruppe	ROL-Behördenkürzel-ePob-Sicht Beispiel: ROL-FB-ePob-Sicht

Name	**Postworkflow**
Art der Aufgabe	Postweiterleitung
Verwendung	Weiterleitung der eingescannten Poststücke an die zuständige Sachbearbeitung
Aufgabenbeschreibung:	Innerhalb der Aufgabe sollen die Dokumente feingesteuert werden
Mögliche Mitarbeitergruppen:	Mitarbeitende in den Poststellen der Behörden/ Ämter
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	ROL-Behördenkürzel-Abteilung/Referat-ePob-Poststelle Beispiel: ROL-FB-ePob-Poststelle

Name	**Fachworkflow**
Art der Aufgabe	Sachbearbeitung
Verwendung	Fachliche Bearbeitung im Fachworkflow

Aufgabenbeschreibung:	Innerhalb der Aufgabe soll die Fachliche Bearbeitung anhand des vorliegenden Dokumentes durchgeführt werden
Mögliche Mitarbeitergruppen:	Sachbearbeitende in den Behörden/ Ämtern
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	ROL-Behördenkürzel-Abteilung/Referat-ePob-Fachaufgabe Beispiel: ROL-BWF-ePob-Dichtigkeitspruefung

5.2 Verwaltung von Berechtigungen

Die Berechtigungen werden entweder zentral in der Fachlichen Leitstelle ePob oder dezentral in den jeweiligen Fachbehörden und Bezirksämtern verwaltet.

Folgende Berechtigungen werden zentral in der Fachlichen Leitstelle ePob verwaltet:

- Berechtigungen für die Administration
- Berechtigung für die Geschäftspartnersuche

Folgende Berechtigungen werden dezentral durch die Behörden und Bezirksämter gesteuert:

- Benutzerpflege und Erteilung der Zugriffsrechte über Benutzergruppen
- Antrag auf Hinzufügung und Änderung von Benutzergruppen einschließlich Berechtigungen

5.2.1 Bildungsregel in Posteingangsbuch

Die eigentliche Benutzerverwaltung erfolgt in den Behörden / Ämtern selbst. Die Benutzer werden in den Behörden / Ämtern den eingerichteten Benutzergruppen zugeordnet.

Ebenso wie die Benutzergruppen der DRiVe-IT werden die Benutzergruppen von ePob dezentral über das Active Directory abgebildet. Nach Meldung der Behörden / Ämter an die Fachliche Leitstelle ePob werden diese in der Benutzerverwaltung freigegeben und danach automatisch über eine Schnittstelle im Posteingangsbuch hinterlegt und täglich aktualisiert. Die Pflege der Gruppen erfolgt dezentral über die jeweilige IT-Abteilung einer Behörde oder eines Amtes. Die Fachliche Leitstelle ePob erteilt dann im Rahmen ihrer Administratorenzuständigkeit die gemäß der Rollenzuteilung zustehenden Lese- und/oder Schreibrechte für das Posteingangsbuch.

Das Ziel der ordnungsgemäßen Berechtigungsverwaltung ist, dass auf das IT-Verfahren ePob lediglich Personen Zugriff haben sollen, die den Zugriff für die Erledigung der ihnen übertragenen Dienstaufgabe benötigen und denen der Zugriff ordnungsgemäß übertragen worden ist.

Abweichungen von den Vorgaben der Musterrollen bei der Berechtigungsvergabe sind nicht zulässig. Die Pflege und Änderung der Musterrollen obliegen der Fachlichen Leitstelle ePob. Änderungen erfolgen nur, wenn eine ordnungsgemäße Aufgabenerledigung mit den vorhandenen Musterrollen nicht möglich ist. Änderungen der Musterrollen werden schriftlich dokumentiert und laufend fortgeschrieben sowie bei Bedarf angepasst.

Im Unterschied zu den Benutzergruppen der DRiVe-IT-Verfahren setzen sich die ePob-Benutzergruppen folgendermaßen in ihrer Bezeichnung zusammen:

- Präfix „ROL“ für die Benutzergruppe,
- Kurzbezeichnung der Behörde / des Amtes,
- Bezeichnung des verwendeten Fachverfahrens: ePob
- Organisationseinheit oder Aufgabengruppe in der Behörde/ dem Amt
- Maximale Zeichenlänge: 40, Trennung mit Bindestrich innerhalb des Namens

5.2.2 Übernahme der Berechtigungen / Aufgabenabgrenzung in ePob

Die möglichen Prozessketten und die Bildungsregeln für die Benutzergruppen werden durch die Fachliche Leitstelle ePob vorgeschlagen und die Umsetzung in den Behörden / Ämtern mit der Fachlichen Leitstelle ePob abgestimmt.

Die Einrichtung der Gruppen und Festlegung auf die jeweiligen Berechtigungen im Posteingangsbuch erfolgt entsprechend der Verfahrensweise der DRiVe-IT in Absprache mit dem jeweiligen Ansprechpartner in der Behörde. Die Fachliche Leitstelle überprüft nach Mitteilung der Benutzergruppen, ob diese sich in die Organisationsstruktur der beantragenden Stelle sinnvoll einbinden und für das Posteingangsbuch hinterlegen lassen.

Aufgabe	Behörde/ Amt	Fachliche Leitstelle ePob
Festlegung Prozesskette	V	B
Einrichtung der Benutzergruppen im Active Directory	V	B
Pflege der Benutzergruppen	V	B
Übernahme der Benutzergruppen in die Benutzerverwaltung		V

B = Beratung ***V = Verantwortung***

5.3 Verwaltung der Admin-Berechtigungen

Die Berechtigungen der Administratoren werden über eine Anbindung an das Active Directory verwaltet. Die Berechtigungen sollen - je nach Aufgabendefinition - mehrstufig vergeben werden können.

5.4 Einrichtung von Info-User und Prüfberechtigungen

Für Prüfungszwecke können in den jeweiligen Behörden lesende Berechtigungen über den sog. Info-User eingerichtet werden. Dazu wird eine gesonderte Benutzergruppe eingerichtet, die lediglich einen lesenden Zugriff auf die Vorgänge der Behörde oder des Amtes erlaubt. Die Mitglieder dieser Benutzergruppe können alle für den Zuständigkeitsbereich vorhandenen eingescannten Poststücke recherchieren.

Für die Prüfzwecke des Rechnungshofes wird darüber hinaus eine eigenständige Benutzergruppe eingerichtet. Über diese Benutzergruppe wird eine lesende Berechtigung für sämtliche Dokumente der eingescannten Post innerhalb des Posteingangsbuches gesteuert. Die jeweiligen Prüfer werden für den angekündigten Prüfungszeitraum zu der Benutzergruppe zugeordnet und können somit die erforderlichen Prüfungen durchführen.

6 Betriebsorganisation/Verantwortungsabgrenzung

Der Einsatz des IT-Verfahren ePob einschließlich des Posteingangsbuches ist durch den Einsatz von Steuerungs- und Pflegeinstitutionen abzusichern.

6.1 Zuständigkeiten

Nachfolgend werden die speziellen Festlegungen zu den Zuständigkeiten für das Verfahren beschrieben. Im Übrigen gelten die Regelungen der Freigabe-Richtlinie.

6.1.1 Fachliche Leitstelle

Die Fachliche Leitstelle ePob steuert die Einsatzstrategie und betreut und berät die Verantwortlichen für eingerichtete oder zusätzliche Verfahrensteile.

Die Fachliche Leitstelle ePob ist zuständig für Beauftragung und Abnahme von Änderungen am Programmcode oder Customizing-Einstellungen. Die Abnahme umfasst sowohl den Abnahmetest wie auch die Abnahmeerklärung. Der Abnahmetest kann auch bei Dritten beauftragt werden.
Änderungen am Programmcode oder Customizing-Einstellungen müssen gegenüber dem Rechenzentrum beauftragt werden. Der Fachlichen Leitstelle ePob obliegt auch die Führung der Testdokumentation. Die Erstellung spezieller Dokumentationsteile kann gegenüber Dritten beauftragt werden.

6.1.2 Anwendende Stellen

Das IT-Verfahren ePob steht grundsätzlich an allen Arbeitsplätzen der FHH mit Intranet und Internetanschluss zur Verfügung, da es sich um eine webbasierte Anwendung handelt.
Für eine möglichst einfache Handhabung der IT-Verfahrens ePob ist sichergestellt, dass ein Benutzer nach einmaliger Authentifizierung am Arbeitsplatz mittels seines Active-Directory-Passworts auf alle dafür notwendigen Dienste, für die er berechtigt ist, ohne weitere Anmeldung zugreifen kann.
Die Anmeldung erfolgt mittels Single-Sign-On und wird durch die Zugehörigkeit zur Benutzergruppen abgesichert.

6.1.3 Programmierende Stellen

Die Programmierenden Stellen sind

- Firma xSuite Group für Scan- und Verifizierungssoftware
- Firma Futuresoft für das ELDORADO-Archiv
- Firma Dataport für die Anwendung Posteingangsbuch

Die Firmen sind für die gesamte Softwaredokumentation verantwortlich.

6.1.4 Rechenstelle

Die Komponenten von ePob werden von Dataport als Datenverarbeitung im Auftrag betrieben. Der Betrieb wird unter Anwendung der Mindestanforderungen der Standard-Sicherheitsrichtlinien von Dataport durchgeführt. Auf die einschlägigen Sicherheitsbestimmungen von Dataport wird verwiesen.

Zugang zu den genutzten Hardwarekomponenten haben nur die befugten Mitarbeiter von Dataport. Durch eine Aufgabenteilung im Rechenzentrum ist sichergestellt, dass auch intern nur befugte Personen Zugriff zu den Daten haben. Der Sicherheitsstandard des Rechenzentrums ist im Dataport Datenschutzmerkblatt beschrieben.

Das Rechenzentrum sichert den performanten Betrieb der notwendigen Anwendungskomponenten. Neben der Gewährleistung der Betriebssicherheit (7 Tage á 24 Stunden) wird während der Bürozeiten von 8 – 16 Uhr der betreute Betrieb geboten.
Zudem stellt das Rechenzentrum die Datensicherung sicher. Die Daten sollen täglich – zumindest inkrementell – gesichert werden. Zumindest einmal wöchentlich ist eine Vollsicherung durchzuführen.

Die Anwendung wird von Dataport betrieben.

6.2 Verfahrensbetreuung und Support

Im Rahmen der Verfahrensbetreuung übernimmt Dataport die Aufgaben des kompletten Supports. Im Rahmen der Verfahrensbetreuung übernimmt Dataport die Supportaufgaben im Rahmen der nachstehenden Abgrenzung.
Dataport hält qualifizierte Kenntnisse zu den Grundstrukturen der IT-Verfahren DRiVe einschließlich des Posteingangsbuches und den vorgesehenen Prozessketten vor. Die Aufgaben

des First-Level-Supports und der Störungsanalyse werden von Dataport wahrgenommen. Bei fehlerhaftem Systemverhalten kann Dataport die programmierenden Stellen einschalten.

6.3 Datenschutz und Datensicherheit

Das IT-Verfahren DRiVe einschließlich des Posteingangsbuches hält sich an die Vorgaben zum Schutz personenbezogener Daten gemäß Datenschutz-Grundverordnung (DS-GVO) i.V.m. dem Hamburgischen Datenschutzgesetz (HmbDSG). Diese verlangen, dass die Verarbeitung und Speicherung personenbezogener Daten nur im Rahmen der gesetzlichen Vorschriften oder im Einverständnis mit dem Betroffenen erfolgt. Das damit verfolgte Ziel des Schutzes des Einzelnen davor, durch Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt zu werden, wird auch durch das IT-Verfahren ePob eingehalten.

Anlage 4

zur Vereinbarung nach § 93 HmbPersVG über die Einführung des Fachverfahrens ePob

Qualifizierungskonzept

Fachverfahren ePob

Stand 10.11.2022

1. Ausgangslage

In allen Organisationseinheiten der FHH ist noch ein hoher Anteil an eingehender Papierpost zu verzeichnen. Für die Bearbeitung wird aktuell die Post manuell verteilt.
Ziel des Projektes ePob ist es, die Papiereingänge zu digitalisieren und als strukturierte Dokumente zur weiteren Bearbeitung zu übertragen.

Mit ePob soll nicht nur ein digitales Bild erzeugt, sondern gleichzeitig auch eine intelligente Steuerung der darauffolgenden Workflows erreicht werden. Damit wird eine mittelfristige Entlastung der Poststellen von manuellen Tätigkeiten angestrebt.
Darüber hinaus wurde im Projekt ein großer Wert auf Standarisierung und Wiedererkennung der eingesetzten Softwarelösung gelegt.

Für die allgemeinen Posteingänge wurde eine Lösung auf Basis der DRiVe-Funktionalitäten konzipiert und als Grundlage für eine finale Entscheidung bereitgestellt. Mit der Entscheidung der Lenkungsgruppe am 10.08.2022 wurde eine vollständige Umsetzung der ePob Workflows innerhalb des Posteingangsbuches beschlossen.

2. Zielgruppen

Die Schulungsmaßnahmen für das neue Verfahren ePob richten sich an die Mitarbeitenden der Poststellen und Sachbearbeitungen der Dienststellen in den Behörden, Ämtern, Landesbetrieben und Hochschulen.

Folgende Schulungsveranstaltungen werden angeboten

- ePob-Schulung für Mitarbeitende der Poststellen
- ePob-Schulung für die Sachbearbeitung in den Dienststellen
- ePob-Informationsveranstaltung für Führungskräfte

Die Qualifizierungsmaßnahmen verfolgen das Ziel, die Anwenderinnen und Anwender entsprechend ihrer Rolle zu einer selbstständigen und sicheren Erledigung ihrer fachlichen Aufgaben zu befähigen. Die Qualifizierungsmaßnahmen erfolgen zeitnah vor und während der Pilotierung und begleitend zur behördenweiten ePob-Einführung.

Daneben sollen für die Mitarbeitenden des DRiVe-Supports bei Dataport zu fachlich-technischen Fragestellungen ein Workshop sowie eine Einweisung in die für die Schulungen zuständigen Dozentinnen und Dozenten durchgeführt werden.

Durch den Einsatz der vorhandenen DRiVe - Komponenten im Zentralen Rechnungseingang (ZRE) ist eine erneute Schulung der Mitarbeiterinnen und Mitarbeiter im Zentralen Rechnungseingang nicht erforderlich.

3. Umfang

Das Projekt ePob richtet sich an alle Beschäftigte der FHH, die Post empfangen können. Da dieser Aspekt alle Personen in der FHH betreffen kann, wird jedem:r Beschäftigten die Möglichkeit gegeben, sich über Schulungen und Schulungsmaterialien fortzubilden.

3.1 Inhalt der Schulung

Die Schulungsbedarfe der unter 0. dargestellten Zielgruppen werden durch die nachfolgend aufgeführten Angebote abgedeckt.

3.1.1 ePob-Schulung für Mitarbeitende in den Poststellen

Inhalte der Schulungsmaßnahme für Mitarbeitende in den Poststellen der Behörden und Ämter sind die Grundlagen und die Bedienung des Posteingangsbuches:

- Definitionen und Abgrenzungen
  - ePob und HIM-Workflow
  - Postworkflow und Fachworkflow
  - Frühes und spätes Archivieren

- Digitalisierungsprozess im ZRE
  - Vorbereitung der Scanpost in der Behörde
  - Weiterleitung des Scangutes an den ZRE

- Aufbau des Posteingangsbuches und Darstellung der Dokumente

- Fachaufgaben in der Poststelle nach dem Scanvorgang

  - Umgang mit dem Postworkflow
    - Weiterleitung an den Fachbereich
    - Rückfragefunktion

- Rückgabe an ZRE

3.1.2 ePob-Schulung für die Sachbearbeitung in den Dienststellen

Inhalte der Schulungsmaßnahme für die Sachbearbeitung in den Dienststellen der Behörden und Ämter sind die Grundlagen und die Bedienung des Posteingangsbuches:

- Definitionen und Abgrenzungen
  - ePob und HIM-Workflow
  - Postworkflow und Fachworkflow
  - Frühes und spätes Archivieren

- Digitalisierungsprozess im ZRE
  - Vorbereitung der Scanpost in der Behörde
  - Weiterleitung des Scangutes an den ZRE

- Aufbau des Posteingangsbuches und Darstellung der Dokumente

- Fachaufgaben in der in der Sachbearbeitung nach dem Scanvorgang
  - Umgang mit den über die Poststelle zugewiesenen Postworkflow
  - Umgang mit den automatisch gerouteten Fachworkflow
  - Verfügung an ELDORADO

3.1.3 ePob-Informationsveranstaltung für Führungskräfte

Die Informationsveranstaltung für Führungskräfte der Dienststellen der Behörden und Ämter soll der allgemeinen Information zur Umsetzung von ePob dienen und weist folgende Inhalte auf:

- Definitionen und Abgrenzungen
  - ePob und HIM-Workflow
  - Postworkflow und Fachworkflow
  - Frühes und spätes Archivieren

- Digitalisierungsprozess im ZRE
  - Vorbereitung der Scanpost in der Behörde

- Weiterleitung des Scangutes an den ZRE

- Aufbau des Posteingangsbuches und Darstellung der Dokumente

- Unterscheidung zwischen Post- und Fachworkflow

- Informationen zum Verlauf der Pilotierung und zum Rollout in den Behörden

3.1.4 Innenrevisionen und Rechnungshof

Für Prüfinstanzen werden im Bedarfsfall eigene Workshops konzipiert und angeboten.

3.1.5 DRiVe-Supportpersonal

Für den DRiVe-Support bei Dataport wird zu fachlich-technischen Fragestellungen ein adressatenorientierter Workshop durchgeführt. Dieser richtet sich ebenfalls an die Fachliche Leitstelle.
Im Workshop sollen u.a. die erweiterten Themen wie Benutzergruppen und Rechte, Geschäftspartner behandelt werden. Die Teilnehmerinnen und Teilnehmer sollen vertiefte Kenntnisse über die Anwendungsarchitektur und die Systemschnittstellen erlangen. Wesentliche Arbeitsschritte werden an den Systemen geübt.

3.1.6 Train-the-Trainer

Die Schulungen werden durch ein Team von haupt- und nebenamtlichen Dozenten durchgeführt. In einem Workshop erhält das Team die Gelegenheit, sich mit den Schulungsinhalten vertraut zu machen. Darüber hinaus werden technische und organisatorische Rahmenbedingungen für die Schulungsdurchführung geklärt.

3.2 Veranstaltungsorganisation und -ort

Die Schulungen werden durch das ZAF organisiert. Hierdurch wird gewährleistet, dass der Standardprozess für die Veranstaltungsdurchführung genutzt werden kann.

4. Schulungsunterlagen

Im Rahmen der Erstellung der Schulungsunterlage wird der benötigte Arbeitsvorrat genauer analysiert und mit den Beteiligten abgestimmt.

Es ist ein Handout in Form einer Powerpoint-Präsentation geplant. Form und Umfang sollen der Anforderung genügen, im praktischen Einsatz als Anwendungsleitfaden dienen zu können.

Für die übrigen Veranstaltungen wird ebenfalls ein Powerpoint-Handout benötigt, für die Train-the-Trainer-Workshops sind weitere Arbeitshilfen vorgesehen.

5. System

Die Schulung wird als IT-Veranstaltung konzipiert. Es steht eine Schulungsumgebung zur Verfügung, die sich vom Entwicklungsstand an der Produktion orientiert und regelmäßig angepasst wird. Ein Koordinierungsprozess hierfür wird gesondert definiert.

5.1. Installation

Die Anwendung INEZ.Core ist webbasiert. Eine Installation auf den Dataport-Schulungsrechnern ist nicht erforderlich.

5.2 Kennungen und Passwörter

Die Berechtigung von Schulungsteilnehmern erfolgt durch die Zuordnung der Schulungskennungen zu Benutzergruppen. Eine Einrichtung von Schulungsusern mit entsprechender Gruppenzuordnung wird durch Kasse.Hamburg vorgenommen.

Die Passwortverwaltung erfolgt analog zu den DRiVe-Schulungen durch den Dataport-Veranstaltungsservice. Entsprechende AD-Berechtigungen werden durch Kasse.Hamburg beantragt.

5.3 Übungsvorgänge

Es werden pro Veranstaltung jeweils ausreichend Übungsvorgänge benötigt. Im Nach heutigem Stand müssen diese Dokumente vor jedem Termin bereitgestellt und durch den ZRE eingescannt werden. Ein entsprechender Prozess wird noch definiert und zwischen den Beteiligten abgestimmt werden.