Vereinbarung

nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG)

über die Einführung, Anpassung und den laufenden Betrieb

des IT-Verfahrensteils INEZ.Core als Teil der DRiVe-IT (früher: HERAKLES-IT)

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

Die Bürgerschaft der Freien und Hansestadt Hamburg hat mit Drucksache 19/5094 vom 19.01.2010 die Finanzbehörde beauftragt, die Buchhaltungsorganisation der Hamburgischen Verwaltung zu optimieren und die Bewirtschaftungsprozesse in den Fachbehörden und Bezirksämtern der Freien und Hansestadt Hamburg elektronisch zu unterstützen.

Die Partner dieser Vereinbarung sind sich einig, dass die Bewirtschaftungsprozesse in den Fachbehörden und Ämtern der Freien und Hansestadt Hamburg durch das neu einzuführende IT-Verfahren INEZ.Core elektronisch unterstützt und dabei teilweise automatisiert werden sollen.

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 INEZ.Core als Modul der DRiVe-IT (früher: HERAKLES-IT)[1] soll die Anwender bei der Bearbeitung von Zuwendungsvorgängen unterstützen. Durch den Einsatz von INEZ.Core wird den Benutzern eine einfache und effiziente Lösung zur Bearbeitung der Zuwendungsvorgänge angeboten und gleichzeitig die Transparenz sämtlicher relevanten Bearbeitungsschritte sichergestellt. Es soll ergonomisch ausgestaltet und sinnvoll in den Gesamtprozess der Mittelbewirtschaftung integriert sein. Um dies zu gewährleisten, erfolgte bereits die Entwicklung von INEZ.Core unter enger Einbeziehung eines Anwenderarbeitskreises. Mit der Reduktion auf den Kernprozess des Zuwendungsrechts und einer Anbindung von INEZ.Core an die bestehenden Prozesse der DRiVe-IT (früher: HERAKLES-IT) soll eine höhere Akzeptanz geschaffen werden.

---

[1] Das Verfahren HERAKLES-IT wurde aufgrund des Ausbaus mit weiteren Verfahrensteilen umbenannt in „Digitales Rechnungswesen in der Verwaltung – DRiVe".

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

** Abweichung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

1.

Gegenstand dieser Vereinbarung

Gegenstand dieser Vereinbarung sind die verbindliche Einführung, Nutzung und Weiterentwicklung sowie der laufende Betrieb des IT-Verfahrensteils INEZ.Core.

Im Hintergrund stützt sich diese Anwendung auf eine Reihe von Webservices (Geschäftspartner, Kontierungen, Benutzer- und Berechtigungsverwaltung) sowie ein ELDORADO-Archiv zur elektronischen und revisionssicheren Ablage zahlungsbegründender Unterlagen. Das ELDORADO-Archiv für INEZ.Core ist technisch getrennt von den ELDORADO-Instanzen der elektronischen Registraturen. Die für die elektronische Registratur benötigte Client-Anwendung (teraDoc-Client) wird nicht benötigt. Das ELDORADO-Archiv dient dem Dokumentenmanagement für buchungsbegründende Unterlagen im Hintergrund. Der Endanwender hat darauf keinen direkten Zugriff.*

Zweck und Ziel des Verfahrensteils INEZ.Core sind in der Anlage „Beschreibung der Verarbeitungstätigkeit" (Anlage 1) näher beschrieben. Die Anlage ist Bestandteil der vorliegenden Vereinbarung.

2.

Geltungsbereich

Diese Vereinbarung gilt für alle Behörden und Ämter. Für Hochschulen, Landesbetriebe und Sondervermögen sowie sonstige Einrichtungen der Freien und Hansestadt Hamburg gilt diese Vereinbarung nur, soweit diese INEZ.Core zur Wahrnehmung ihrer Aufgaben einsetzen.**

3.

Ergonomie und Arbeitsplatzgestaltung

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).

Es wird unter Hinzuziehung des Arbeitsmedizinischen Dienstes, nach dessen Votum erforderlichenfalls weiterer sachkundiger Experten, geprüft, welche der durch den Verfahrensteil INEZ.Core auszuführenden Tätigkeiten auch von Menschen mit Behinderung vorgenommen werden könnten und wie das IT-Verfahren hierfür barrierefrei ausgestaltet werden kann.*

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.

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

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung
** Abweichung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

jeweils zuständige Behörde bzw. Dienststelle, wird dabei die sich aus den §§ 3-14 Arbeitsschutzgesetz und Anlage 6 der Verordnung über Arbeitsstätten ergebenden Pflichten erfüllen.

4.

Arbeitsplatz- und Einkommenssicherung

Die Einführung und der laufende Betrieb des Verfahrensteils INEZ.Core 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 des bzw. der 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. In diesen Fällen wird die Verwaltung eventuelle notwendig werdende personelle Maßnahmen ohne betriebsbedingte Kündigung und ohne Änderungskündigung mit dem Ziel der tariflichen Herabgruppierung umsetzen.

Die Arbeitsplatz- und Einkommenssicherung für Tarifbeschäftigte 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.

5.

Datenschutz, Schutz vor Leistungs- und Verhaltenskontrollen

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 revisionssichere Identifikation und dauerhafte Speicherung erfassender und den Genehmigungsworkflow durchführender Personen sowie der das Verfahren administrierenden Personen.

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung
** Abweichung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

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

- Name, Vorname
- Benutzer-Kennung
- dienstliche E-Mail-Adresse
- dienstliches Telefon sowie Fax
- Organisationseinheit
- Universelle Benutzergruppe

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 2 näher beschrieben.

6.

Qualifizierung

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.

---

[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

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung
** Abweichung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

Sofern Defizite im Nachgang zu Schulungsmaßnahmen bestehen, werden hierzu in Abstimmung mit der zuständigen Behörde bzw. Amt Lösungsmaßnahmen vereinbart.*

Alle Beschäftigten, die mit dem Verfahrensteil INEZ.Core arbeiten, werden gemäß dem beigefügtem Qualifizierungskonzept (Anlage 3) qualifiziert. Alle von der Einführung des IT-Verfahren betroffenen Beschäftigten haben Anspruch auf Präsenzschulungen, die Teilnahme hieran ist verpflichtend. **

Es wird gewährleistet, dass auch Menschen mit Behinderungen geschult werden können. Hier muss von Fall zu Fall nach einer behindertengerechten Lösung gesucht und ggf. individuell geschult werden.

Den Anwenderinnen und Anwendern werden Hilfen zum Umgang mit dem IT-Verfahren bereitgestellt, die sich an zentraler Stelle im Sharepoint-Bereich der Fachlichen Leitstelle DRiVe aufrufen lassen. Es wird außerdem gewährleistet, dass für alle Anwenderinnen und Anwender im Falle auftretender Probleme eine versierte Ansprechstelle zur Verfügung steht.

Die Spitzenorganisationen und die Personalräte erhalten Gelegenheit an diesen Qualifizierungen teilzunehmen.

7.

Organisation und Ablauf

Einführung und Inbetriebnahme des Verfahrensteils INEZ.Core werden durch Mitarbeiterinnen und Mitarbeiter der Fachlichen Leitstelle begleitet.*

Die Einführung des neuen IT-Verfahrens bedeutet für die Anwenderinnen und Anwender, dass die bisherigen Arbeitsweisen sich verändern. Sie setzt daher sorgfältig organisierte und durchgeführte Einführungsprozesse voraus. Die Einführung des IT-Verfahrens in den Behörden und/oder Dienststellen wird in zeitlicher und organisatorischer Hinsicht als Meilenstein- oder Roll-Out-Planung beschrieben. Sie erfolgt grundsätzlich im Rahmen der bestehenden Organisation der Dienststelle. Bei Bedarf können auch andere Umsetzungsstrukturen gewählt werden.

Den örtlichen Personalräten wird Gelegenheit gegeben, an der Umsetzung teilzunehmen.

Der Verfahrensteil INEZ.Core wird durch den IT-Dienstleister der FHH (Dataport) zentral betrieben. Es handelt sich um eine Web-Anwendung, die am lokalen Arbeitsplatz lediglich eine aktuelle Browser-Umgebung voraussetzt. Dataport übernimmt im Produktivbetrieb auch den Support und die Störungsbeseitigung.*

Die § 93-Verhandlungspartner sind sich darüber einig, dass die Spitzenorganisationen der Gewerkschaften und Berufsverbände Sachverständige im Rahmen der eigenen Organisation in Anspruch nehmen oder zu ihrer allgemeinen Beratung hinzuziehen können. Die Verwaltung wird die erforderlichen Kosten für eine sachverständige Beratung der Spitzenorganisationen der Gewerkschaften und Berufsverbände nach entsprechender Konsultation in Anlehnung an § 47 HmbPersVG übernehmen.*

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung
** Abweichung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

Sollte es bei der Einführung des Verfahrens zu nicht auflösbaren Konflikten in einer Behörde oder Dienststelle kommen, werden sich die Verhandlungspartner dieser Vereinbarung um eine einvernehmliche Lösung bemühen.

8.

Evaluation des Betriebs unter Beteiligung der Spitzenorganisationen

Spätestens im 3. Quartal 2021 wird durch die fachlich zuständige Stelle eine Evaluation durchgeführt.*

Die Evaluation umfasst insbesondere die Gestaltung

- der Arbeitsprozesse (z.B. Unterstützung der Aufgabenerledigung durch das Verfahren),
- der Dialogoberfläche (logischer Bildschirmaufbau),
- die Hardware-Ausstattung (z.B. Angemessenheit der Monitorgröße).

Soweit möglich werden bei der Evaluation alle Entwicklungsziele zu fachlichen Belangen, Datenschutz, Anwendungstauglichkeit (Gebrauchstauglichkeit) und Qualifizierungsmaßnahmen berücksichtigt. Die Einzelheiten des Evaluationsverfahrens werden mit den Spitzenorganisationen der Gewerkschaften beraten. Die Anmerkungen werden bei der Durchführung berücksichtigt.

Die Erhebung erfolgt anonymisiert auf elektronischem Wege. Zur Konkretisierung der Ergebnisse können in begrenzter Zahl Gespräche mit Mitarbeiterinnen und Mitarbeitern bzw. Anwender-Workshops stattfinden.

Das Ergebnis wird den Spitzenorganisationen der Gewerkschaften vorgestellt und mit Ihnen erörtert.

9.

Verfahren bei Änderungen

Das unter lfd. Nummer 1. beschriebene Verfahren wird bei Bedarf weiterentwickelt.

Vor wesentlichen Änderungen des Verfahrens sowie erforderlicher Anpassungen der Anlagen, z. B. des Berechtigungs- oder des Qualifizierungskonzeptes, welche einen eigenständigen inhaltlichen Gehalt haben, informiert die für das Fachverfahren verantwortliche Behörde bzw. Dienststelle in Abstimmung mit der für die Verhandlungsführung zuständigen Stelle die Spitzenorganisationen der Gewerkschaften so rechtzeitig, dass sie noch Einfluss auf die Änderungen nehmen können.

Die Spitzenorganisationen der Gewerkschaften erhalten die Gelegenheit, sich binnen 4 Wochen nach Zugang der Information zu der wesentlichen Änderung zu äußern. Wenn sich keine der Spitzenorganisationen der Gewerkschaften der Änderung innerhalb dieser Frist äußert, gilt die Zustimmung als erteilt. Andernfalls nehmen die Beteiligten Verhandlungen auf.

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung
** Abweichung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

10.

Schlussbestimmungen

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

Diese Vereinbarung tritt mit sofortiger Wirkung in Kraft. Sie kann mit einer Frist von sechs Monaten zum Ende eines Jahres gekündigt werden.

Bei Kündigung wirkt diese Vereinbarung bis zum Abschluss einer neuen Vereinbarung nach. In diesem Fall werden die Partner der Vereinbarung unverzüglich Verhandlungen über den Abschluss einer neuen Vereinbarung aufnehmen.

Bei Beendigung des Verfahrens DRiVe-IT und der Vereinbarung nach §94 HmbPersVG (a.F.) über die Einführung, Anpassung und den laufenden Betrieb des IT-Verfahrens Herakles in der Fassung der Änderungsvereinbarung vom 15. Juni 2018 werden der IT-Verfahrensteil INEZ.Core und diese Vereinbarung aufgehoben.*

Hamburg, den 02. Jan. 2020

Freie und Hansestadt Hamburg
für den Senat

Volker Wiedemann

Rudolf Klüver
dbb hamburg
- beamtenbund und tarifunion -

Olaf Schwede
Deutscher Gewerkschaftsbund
- Bezirk Nord -

Anlagen:

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

* Ergänzung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung
** Abweichung gegenüber den Standardformulierungen des Teil 2 der IT-Rahmenvereinbarung

Anlage 1

Hamburg

Beschreibung der Verarbeitungstätigkeit

(Bitte an die Verzeichnisführende Stelle absenden!)

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

Blatt-Nr.:
Von der Verzeichnisführenden Stelle auszufüllen!

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

Allgemeines			
	Datum:	01.10.2019	
	Ausfüllende Person:	Sinje Smeenge (i.V. für Manfred Janz)	
	Telefonnummer:	42823-2626 (Manfred Janz -2411)	
	Bezeichnung des Verfahrens:	DRiVe – INEZ.Core	
	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]:	10/2018 Pilotbetrieb	
	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):	Kasse.Hamburg	
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):	Fachliche Leitstelle DRiVe	

[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

Bearbeitungsstand: 08.10.2019

	Verantwortliche Führungskraft: Leitzeichen:	Eva Jadamus-Ulitzka K25	
1.4	Ansprechpartner, sofern nicht verantwortliche Führungskraft: Telefonnummer:	Dirk Brummund 42823-2760	
1.5	Name des Datenschutzbeauftragten (optional):	Yvonne Jagla, FB 14/1	
1.6	Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt[6]: Auftragsnummer:	Dataport, Billstraße 82, 20539 Hamburg Klicken Sie hier, um Text einzugeben.	

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung[7]			
2.1	Beschreibung und Zweckbestimmung der Verarbeitung von Daten[8]	Beschreibung der Verarbeitung: Erfassung und Bearbeitung von Zuwendungsanträgen, deren Bewilligung sowie Auszahlung der Zuwendung und Prüfung der Verwendung Beschreibung der Zweckbestimmung: Antragsbearbeitung (Bauanträge, Wohngeldanträge, etc.) Sonstiges: Klicken Sie hier, um Text einzugeben.	
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* Klicken Sie hier, um Text einzugeben.	
☒	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:*	

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

		Klicken Sie hier, um Text einzugeben.	
☒	Weitere:	§ 46 LHO und zugehörige VV.	
3. Beschreibung betroffener Personen- und Datenkategorien			
3.1	Beschreibung der betroffenen Personengruppen[9]:	Beschäftigte **Sonstige:** Antragstellende Ansprechpersonen von Antragstellenden Stelleninhabende (sofern diese im Antrag genannt werden) Geförderte Personen Teilnehmende Personen (TN-Daten) **Beschreibung:** Die Daten der genannten Personengruppen werden in unterschiedlicher Form im Verfahren gespeichert. Dokumente werden in Eldorado und Datenbankfelder in der Datenbank gespeichert.	
3.2	Beschreibung der Art der Daten[10] bzw. Datenkategorien	Identifikations- und Adressdaten Sonstige: Stammdaten Daten zu Bankkonten IT-Nutzungsdaten	
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)	Finanzbehörde (FB212), Schnittstelle zum Vorgangsbuch, Power-BI (Standardwarenkorb)	
	Art der Daten	Zuwendungsbericht und andere Auswertungen, zahlungsrelevante Daten	
	Zweck der Daten-Mitteilung	Berichterstattung ggü. Behördenleitung und Politik, Fachcontrolling, Auszahlung von Zuwendungen oder deren Rückforderung	
4.3	Externe Empfänger und Dritte	☒ ja ☐ nein	
	Externe Stelle	Bürgerschaft und politische Ausschüsse, Transparenzportal und Europäische Union	

[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

	Art der Daten	Zuwendungsbericht und andere Auswertungen, Datenübermittlung gemäß Transparenzgesetz, Teilnehmer- und Abrechnungsdaten	
	Zweck der Daten-Mitteilung	Berichtserstattung ggü. Politik, Information und Transparenz ggü. dem Bürger, Berichtserstattung ggü. der EU im Rahmen der Förderung (EFRE/ESF)	
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, ☐ 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: Es gibt unterschiedliche Aufbewahrungsfristen je nach Fachbereich und Aufgaben (Förderung) ☐ nein	
	Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:	Die gespeicherten Daten werden nach Beendigung des Zuwendungsfalls und der für sie geltenden Aufbewahrungsfrist gelöscht.	
6. Mittel der Verarbeitung (optional) **Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?[14]**			
	Bezeichnung: Hersteller: Funktionsbeschreibung: Bereitstellung:	INEZ.Core Dataport Erfassung und Bearbeitung von Zuwendungsfällen (Antrag, Bescheid, Zuwendungsmanagement, Auszahlungen, Verwendungsnachweis, Erfolgskontrollen) ☒ Eigenentwickelte/ individuelle Software ☐ Standard-Software ☐ Cloud-Services	

[13] Hinweis Nr. 13 der Anlage 1
[14] Hinweis Nr. 14 der Anlage 1

		☐ 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:	Der Zugriff wird über im Programm berechtigte AD-Gruppen ausgesteuert. Die Pflege der AD-Gruppen obliegt den Behörden und Bezirksämtern. (Das Berechtigungs- und Rollenkonzept INEZ.Core liegt anbei.)	
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 default) gem. Art 25 Abs. 2 DS-GVO eingehalten?[17]	☒ ja (ggf. Betriebs-/Herstellerkonzept beifügen) ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
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 Grundsätzlich ist davon auszugehen, dass die in der IT-Infrastruktur der FHH implementierten Maßnahmen zusammen mit den organisatorischen Vorgaben ein Schutzniveau „normal" garantieren. Punkt 7.4 Datenschutzkonforme Datenverarbeitung nach der EU-Datenschutz-Grundverordnung - EU 2016/679 (Konzept Datenverarbeitung – Konzept DV) Version 1.5	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 siehe 8.4	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:	☐ Es liegt kein Verfahren vor, das bei Dataport gehostet wird.	

[15] Hinweis Nr. 15 der Anlage 1
[16] Hinweis Nr. 16 der Anlage 1
[17] Hinweis Nr. 17 der Anlage 1

	Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMs laut Anlage 2 sichergestellt.	☐ 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: Auf Grundlage des Transparenzgesetzes ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
10. Informationen der Betroffenen[19]			
	Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?	Über die zuständige Behörde	Link zu den Formularen
11. Sonstiges			
	Anmerkungen:	Klicken Sie hier, um Text einzugeben.	

G. Madamus-Ulrike
Verantwortlicher

8/10/19
Datum

Unterschrift

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

Hinweis Nr. 2
Gemeint ist, welche Verarbeitungstätigkeiten durch das Verfahren berührt werden.

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

Grundsätze	ergriffene Maßnahmen
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 Vereinbarung nach § 93 HmBPersVG über die Einführung, Anpassung und den laufenden Betrieb des IT-Verfahrensteils INEZ.Core als Teil der Herakles-IT (neu: DRiVe-IT)

Berechtigungs- und Rollenkonzept

im Verfahrensteil INEZ.Core

Version 1.0

Stand 05.04.2019

Inhalt

1 Ausgangslage

INEZ.Core stellt einen Verfahrensteil der Herakles-IT-Verfahren dar (neu: DRiVe-IT). Für die notwendigen Systemzugriffe in INEZ.Core 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 Mitarbeiterinnen und Mitarbeiter zu eingerichteten Benutzergruppen. Durch diese Struktur wird sichergestellt, dass nur berechtigte Personen Zugriff auf die jeweiligen Module und 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 INEZ.Core

3.1 Zugriff mittels Single Sign On

Der Zugang der Benutzerinnen und Benutzer für alle DRiVe-IT-Verfahren einschließlich dem Verfahrensteil INEZ.Core 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.

Für die Authentifizierung der Benutzerinnen und 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 universellen Gruppen 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 Benutzerinnen und Benutzer in einer Benutzergruppe im Active Directory gepflegt sind, liegt die Verantwortlichkeit außerhalb von INEZ.Core, und es wird sichergestellt, dass die Passwort-RL erfüllt ist.

4 Verwendung der Benutzergruppen

Die Anwenderinnen und Anwender der Behörden und Bezirksämter bearbeiten im Rahmen ihrer Aufgabenwahrnehmung die der Dienststelle obliegenden Zuwendungsfälle in INEZ.Core. Hierfür werden die zu verwendenden Berechtigungen durch die Fachliche Leitstelle INEZ in INEZ.Core 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 für die Anlage von Zuwendungsfällen und/oder das Sichtrecht auf Zuwendungsfälle vorgenommen werden. Beispielsweise bei der Ersterfassung eines Antrages in der Erfassung, bei der die Anwenderin bzw. der Anwender nur eine Mindestanzahl an Eingaben für eine Ersterfassung und Speicherung vornehmen muss.

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

In INEZ.Core werden weder Anordnungen erzeugt oder vorgenommen, noch Zahlungen generiert. Anordnungen und Zahlungen werden weiterhin über das kassenführende Verfahren RVP vorgenommen bzw. angestoßen, für die die jeweils notwendigen speziellen Berechtigungen außerhalb von INEZ.Core erteilt werden. Demgegenüber beinhalten die INEZ.Core-Berechtigungen voraussetzend keine kassenrechtlichen Befugnisse. Insofern ist die Erteilung oder das Vorhandensein von haushaltsrechtlichen Befugnissen für die im INEZ.Core vorgesehenen Rollen nicht relevant.

5 Notwendige Berechtigungen für INEZ.Core

5.1 Übersicht über die Berechtigungen

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

Name	Einsicht
Technischer Name	Einsicht (INEZ. Recherche)
Prozesskette	INEZ.Recherche
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 von INEZ.Core genommen werden.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die Sichtrechte in die zu bearbeitenden Zuwendungsfälle erhalten sollen.
Berechtigungsprofil	Lesen
Benutzergruppe	U-Behördenkürzel-INEZCORE-Sicht Beispiel: U-FB-124-INEZCORE-Sicht

Name	Erfassung
Technischer Name	Erfassung (INEZ.Antragsverarbeitung)
Prozesskette	INEZ.Antragsverarbeitung
Art der Aufgabe	Erfassung
Verwendung	Erfassung der Antragsdokumente
Aufgabenbeschreibung:	Innerhalb der Aufgabe sollen Zuwendungsdokumente, deren Daten sowie weitere (optional zu erfassende) Daten erfasst werden können.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die Neuantragsdokumente erfassen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Antrag-Erfassung Beispiel: U-FB-124-INEZCORE-Antrag-Erfassung

Name	**Doppelförderungsprüfung nach Erfassung**
Technischer Name	**Doppelförderungsprüfung (INEZ.Antragsverarbeitung)**
Prozesskette	INEZ.Antragsverarbeitung
Art der Aufgabe	Doppelförderungsprüfung
Verwendung	Durchführung der Doppelförderungsprüfung
Aufgabenbeschreibung:	Innerhalb der Aufgabe soll die Doppelförderungsprüfung des Zuwendungsfalls durchgeführt werden.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die die Doppelförderungsprüfung durchführen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Antrag-Doppelfoerderung Beispiel: U-FB-124-INEZCORE-Antrag-Doppelfoerderung

Name	**Formelle Prüfung**
Technischer Name	**Formelle Prüfung (INEZ.Antragsverarbeitung)**
Prozesskette	INEZ.Antragsverarbeitung
Art der Aufgabe	Durchführung Formelle Prüfung
Verwendung	Formelle Prüfung von Antragsdokumenten
Aufgabenbeschreibung:	Erfasste Zuwendungsdokumente werden auf formelle Richtigkeit geprüft.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die die formelle Antragsprüfung durchführen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Antrag-FormellePruefung Beispiel: U-FB-124-INEZCORE-Antrag-FormellePruefung

Name	**Fachliche Prüfung**
Technischer Name	**Fachliche Prüfung (INEZ.Antragsverarbeitung)**
Prozesskette	INEZ.Antragsverarbeitung
Art der Aufgabe	Durchführung Fachliche Prüfung
Verwendung	Fachliche Prüfung (Zuwendungsrecht) von Antragsdokumenten / Zuwendungsfällen.

Aufgabenbeschreibung:	Erfasste Zuwendungsdokumente / Zuwendungsfälle werden auf fachliche Richtigkeit geprüft. Es wird entschieden, ob eine Zuwendung bewilligt oder eine Ablehnung erteilt wird.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die die fachliche Prüfung (Zuwendungsrecht) durchführen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Antrag-FachlichePruefung Beispiel: U-FB-124-INEZCORE-Antrag-FachlichePruefung

Name	**Doppelförderungsprüfung nach Fachlicher Prüfung**
Technischer Name	**Doppelförderungsprüfung (INEZ.Antragsverarbeitung)**
Prozesskette	INEZ.Antragsverarbeitung
Art der Aufgabe	Doppelförderungsprüfung
Verwendung	Durchführung der Doppelförderungsprüfung
Aufgabenbeschreibung:	Innerhalb der Aufgabe soll die Doppelförderungsprüfung des Zuwendungsfalls durchgeführt werden.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die die Doppelförderungsprüfung durchführen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Antrag-Doppelfoerderung Beispiel: U-FB-124-INEZCORE-Antrag-Doppelfoerderung

Name	**Mittelbindung**
Technischer Name	**Mittelbindung (INEZ.Antragsverarbeitung)**
Prozesskette	INEZ.Antragsverarbeitung
Art der Aufgabe	Erfassen Mittelbindung
Verwendung	Erfassen einer Mittelbindung
Aufgabenbeschreibung:	Es wird eine Mittelbindung im Vorgangsbuch (VoBu) angelegt und die Daten anschließend in INEZ.Core hinterlegt.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die eine Mittelbindung im VoBu anlegen und die Daten in INEZ.Core hinterlegen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Antrag-Mittelbindung Beispiel: U-FB-124-INEZCORE-Antrag-Mittelbindung

Name	**Bescheiderstellung**
Technischer Name	**Bescheiderstellung (INEZ.Antragsverarbeitung)**
Prozesskette	INEZ.Antragsverarbeitung
Art der Aufgabe	Dokumenterstellung
Verwendung	Erstellung von Bescheiden
Aufgabenbeschreibung:	Der Zuwendungs- bzw. Ablehnungsbescheid wird erstellt.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die einen Bescheid erstellen werden.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Antrag-Bescheiderstellung Beispiel: U-FB-124-INEZCORE-Antrag-Bescheiderstellung

Name	**Bescheidfinalisierung**
Technischer Name	**Bescheidfinalisierung (INEZ.Antragsverarbeitung)**
Prozesskette	INEZ.Antragsverarbeitung
Art der Aufgabe	Dokument ablegen
Verwendung	Finalisierung (Abschließen) von Bescheiden
Aufgabenbeschreibung:	Der Zuwendungs- bzw. Ablehnungsbescheid wird finalisiert / abgeschlossen.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die einen Bescheid finalisieren / abschließen werden.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Antrag-Bescheidfinalisierung Beispiel: U-FB-124-INEZCORE-Antrag-Bescheidfinalisierung

Name	**Bescheidversand**
Technischer Name	**Bescheidversand (INEZ.Antragsverarbeitung)**
Prozesskette	INEZ.Antragsverarbeitung
Art der Aufgabe	Erfassung Versanddatum
Verwendung	Versendung von Bescheiden
Aufgabenbeschreibung:	Das Versanddatum des Bescheids wird hinterlegt.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die einen Bescheid versenden.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Antrag-Versand Beispiel: U-FB-124-INEZCORE-Antrag-Versand

Name	**Laufender Vorgang (Stammvorgang)**
Technischer Name	**Laufender Vorgang (INEZ.Zuwendungsmanagement)**
Prozesskette	INEZ.Zuwendungsmanagement
Art der Aufgabe	Verwalten laufender Zuwendungsfälle
Verwendung	Verwalten von laufenden Zuwendungsfällen
Aufgabenbeschreibung:	Laufende Zuwendungsfälle werden hier verwaltet. Im Rahmen der Aufgabe können weitere Sternprozesse gestartet werden.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die mit der Betreuung von laufenden Zuwendungsfällen beschäftigt sind.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Zuwendungsmanagement Beispiel: U-FB-124-INEZCORE-Zuwendungsmanagement

Name	**Mittelabforderung**
Technischer Name	**Mittelabforderung (INEZ.Zuwendungsmanagement)**
Prozesskette	INEZ.Zuwendungsmanagement
Art der Aufgabe	Bearbeitung von Mittelabforderungen
Verwendung	Bearbeitung von Mittelabforderungen
Aufgabenbeschreibung:	Mittelabforderungen werden hier zuwendungsrechtlich geprüft und anschließend an das Vorgangsbuch übergeben / übertragen.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die Mittelabforderungen zuwendungsrechtlich prüfen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Zuwendung-Mittelabforderung Beispiel: U-FB-124-INEZCORE-Zuwendung-Mittelabforderung

Name	**Rechtsmittelverzichtserklärung**
Technischer Name	**Rechtsmittelverzichtserklärung (INEZ.Zuwendungsmanagement)**
Prozesskette	INEZ.Zuwendungsmanagement
Art der Aufgabe	Bearbeitung von Rechtsmittelverzichtserklärungen
Verwendung	Bearbeitung von Rechtsmittelverzichtserklärungen
Aufgabenbeschreibung:	Eingehende Rechtsmittelverzichtserklärungen werden formell geprüft.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die Rechtsmittelverzichtserklärungen formell prüfen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Zuwendung-Rechtsmittelverzichtserklaerung Beispiel: U-FB-124-INEZCORE-Zuwendung-Rechtsmittelverzichtserklaerung

Name	**Erfolgskontrolle**
Technischer Name	**Erfolgskontrolle (INEZ.Zuwendungsmanagement)**
Prozesskette	INEZ.Zuwendungsmanagement

Art der Aufgabe	Durchführung von Erfolgskontrollen
Verwendung	Durchführung von Erfolgskontrollen
Aufgabenbeschreibung:	Durchführung und Dokumentation von Erfolgskontrollen.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die Erfolgskontrollen des Zuwendungsfalls / beim Zuwendungsempfangenden durchführen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Zuwendung-Erfolgskontrollen Beispiel: U-FB-124-INEZCORE-Zuwendung-Erfolgskontrollen

Name	**Begleitung**
Technischer Name	**Begleitung (INEZ.Zuwendungsmanagement)**
Prozesskette	INEZ.Zuwendungsmanagement
Art der Aufgabe	Begleitung von Zuwendungsfällen
Verwendung	Begleitung des Zuwendungsfalls
Aufgabenbeschreibung:	Dokumentation von Begleitungen des Zuwendungsfalls z.B. Besuch beim Zuwendungsempfänger.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die Begleitungen des Zuwendungsfalls / des Zuwendungsempfangenden durchführen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Zuwendung-Begleitung Beispiel: U-FB-124-INEZCORE-Zuwendung-Begleitung

Name	**Doppelförderungsprüfung**
Technischer Name	**Doppelförderungsprüfung (INEZ.Zuwendungsmanagement)**
Prozesskette	INEZ.Zuwendungsmanagement
Art der Aufgabe	Doppelförderungsprüfung
Verwendung	Durchführung der Doppelförderungsprüfung
Aufgabenbeschreibung:	Innerhalb der Aufgabe soll die Doppelförderungsprüfung des Zuwendungsfalls durchgeführt werden.
Mögliche Mitarbeitergruppen:	Mitarbeiterinnen und Mitarbeiter, die die Doppelförderungsprüfung durchführen.
Berechtigungsprofil	Lesen und Schreiben
Benutzergruppe	U-Behördenkürzel-Abteilung/Referat-INEZCORE-Zuwendung-Doppelfoerderung Beispiel: U-FB-124-INEZCORE-Zuwendung-Doppelfoerderung

5.2 Verwaltung von Berechtigungen

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

Folgende Berechtigungen werden zentral in der Fachlichen Leitstelle INEZ verwaltet:

- Berechtigungen für die Administration
- Berechtigung für die Geschäftspartnersuche

Die Berechtigung einer Anwenderin bzw. eines Anwenders, die Geschäftspartnersuche durchführen zu können, erfolgt über eine zusätzlich bestehende Zugehörigkeit zu einer DRiVe-IT-Nutzergruppe oder durch Hinterlegung der INEZ.Core-Nutzergruppe in der Rollenverwaltung, über welche die Steuerung der Geschäftspartnersuche vorgenommen wird.

Folgende Berechtigungen werden dezentral durch die Behörden und Bezirksämter gesteuert:

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

5.2.1 Bildungsregel in INEZ.Core

Die eigentliche Benutzerverwaltung erfolgt in den Behörden / Bezirken selbst. Die Benutzerinnen und Benutzer werden in den Behörden / Bezirken den eingerichteten Benutzergruppen zugeordnet.

Ebenso wie die Benutzergruppen der DRiVe-IT-Verfahren werden die Nutzergruppen von INEZ.Core dezentral über das Active Directory abgebildet und nach Meldung der Behörden / Bezirke an die Fachliche Leitstelle INEZ automatisch über eine Schnittstelle zu INEZ.Core mittels eines automatischen Joblaufes (LDAP-Job) in INEZ.Core hinterlegt und täglich aktualisiert. Die Pflege der Gruppen erfolgt dezentral über die jeweilige IT-Abteilung einer Behörde oder eines Bezirksamtes. Die Fachliche Leitstelle INEZ erteilt dann im Rahmen ihrer Administratorenzuständigkeit die gemäß der Rollenzuteilung zustehenden Lese- und/oder Schreibrechte für INEZ.Core.

Das Ziel der ordnungsgemäßen Berechtigungsverwaltung ist, dass auf das IT-Verfahren INEZ.Core 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 INEZ. Änderungen erfolgen nur, wenn eine ordnungsgemäße Aufgabenerledigung mit den vorhandenen Musterrollen nicht möglich ist. Des Weiteren bedürfen Änderungen hinsichtlich der Berechtigungen eines schriftlichen Antrags des INEZ-Chiefs. Änderungen der Musterrollen werden schriftlich dokumentiert und laufend fortgeschrieben sowie bei Bedarf angepasst.

Im Unterschied zu den Nutzergruppen der Herakles-IT-Verfahren setzen sich die INEZ.Core-Nutzergruppen folgendermaßen in ihrer Bezeichnung zusammen:

- Präfix „U" für universale Gruppe[1],
- Kurzbezeichnung der Behörde / des Bezirksamtes,
- Organisationseinheit oder Aufgabengruppe in der Behörde / dem Bezirksamt,
- Bezeichnung des verwendeten Fachverfahrens: INEZ
- Rollenbezeichnung
- Maximale Zeichenlänge: 40, Trennung mit Bindestrich innerhalb des Namens

5.2.2 Übernahme der Berechtigungen / Aufgabenabgrenzung in INEZ.Core

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

Die Einrichtung der Gruppen und Festlegung auf die jeweiligen Berechtigungen in INEZ.Core erfolgt entsprechend der Verfahrensweise der DRiVe-IT-Verfahren in Absprache mit dem jeweiligen INEZ-Chief (zukünftige Verfahrensweise). Die Fachliche Leitstelle überprüft nach Mitteilung der Nutzergruppen, ob diese sich in die Organisationsstruktur der beantragenden Stelle sinnvoll einbinden und für INEZ.Core hinterlegen lassen.

---

[1] Zukünftig wird das Präfix „ROL" in der Nutzergruppenbezeichnung Anwendung finden. Die Umsetzung in den Behörden und Bezirksämtern erfolgt sukzessive seit 07.05.2019. Die Umbenennung erfolgt aus Gründen der Vereinheitlichung und Zertifizierung des Active Directory durch Dataport.

Aufgabe	Behörde	Fachliche Leitstelle INEZ
Festlegung Prozesskette	V	B
Einrichtung der universellen Gruppen im Active Directory (Benutzergruppen)	V	B
Benutzerpflge in den universellen Gruppen	V	B
Übernahme der universellen Gruppen in die Benutzerverwaltung		V

B = Beratung *V = Verantwortung*

5.3 Verwaltung der Admin-Berechtigungen

Die Administratorenrechte für INEZ.Core sollen zukünftig über eine Konsolenanbindung zu INEZ.Core gesteuert werden. 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 universelle Benutzergruppe eingerichtet, die lediglich einen lesenden Zugriff auf die Vorgänge der Behörde erlaubt. Die Mitglieder dieser Benutzergruppe können alle für den Zuständigkeitsbereich vorhandenen Vertragsdatensätze recherchieren.

Für die Prüfzwecke des Rechnungshofes wird darüber hinaus eine eigenständige Benutzergruppe eingerichtet. Über diese Benutzergruppe wird eine lesende Berechtigung je nach Zielsetzung des Prüfauftrages entweder für sämtliche Vertragsdatensätze oder mit Beschränkung

auf einen bestimmten Zuständigkeitsbereich innerhalb von INEZ.Core gesteuert. Die jeweiligen Prüferinnen und Prüfer werden für den angekündigten Prüfungszeitraum zu der Benutzergruppe zugeordnet und können somit die erforderlichen Prüfungen durchführen.

6 Betriebsorganisation/Verantwortungsabgrenzung

Der Einsatz der IT-Verfahren Herakles einschließlich INEZ.Core 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 INEZ steuert die Einsatzstrategie und betreut und berät die Verantwortlichen für eingerichtete oder zusätzliche Verfahrensteile.

Die Fachliche Leitstelle INEZ 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 INEZ obliegt auch die Führung der Testdokumentation. Die Erstellung spezieller Dokumentationsteile kann gegenüber Dritten beauftragt werden.

6.1.2 Anwendende Stellen

Die DRiVe-IT-Verfahren einschließlich INEZ.Core stehen 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 DRiVe-IT-Verfahren einschließlich INEZ.Core ist sichergestellt, dass eine Benutzerin bzw. 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 WMD für Scan- und Verifizierungssoftware
- Firma Futuresoft für das ELDORADO-Archiv
- Firma Dataport für das Modul INEZ.Core

Die Firmen sind für die gesamte Softwaredokumentation verantwortlich.

6.1.4 Rechenstelle

Die Komponenten der DRiVe-IT-Verfahren einschließlich INEZ.Core 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 Mitarbeiterinnen und 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 DRiVe-IT-Verfahren einschließlich INEZ.Core 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 DRiVe-IT-Verfahren einschließlich INEZ.Core 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 INEZ.Core eingehalten.

Anlage 3

DRiVe

Digitales Rechnungswesen in der Verwaltung

Versionsführung

Version	Datum	Inhalt	Ersteller
1.0	11.12.2018	Erstellung	M. Weichert

1. Ausgangslage

Gemäß Nr. 18.9 der VV zu §46 LHO sind alle Zuwendungsfälle im Datenbankverfahren INEZ in allen wesentlichen Teilen abzubilden. Das bisherige Verfahren SF-INEZ ist aus einer Reihe von Gründen technisch nicht mehr wartbar und weiterentwicklungsfähig. Kasse.Hamburg hat daher eine Nachfolgelösung entwickeln lassen, die einerseits in der Lage ist, den sich aus dem Zuwendungsrecht ergebenden Kernprozess rechtssicher abzubilden und andrerseits die Möglichkeit bietet, erweiterte Bedarfe mit Hilfe von Fachmodulen zu decken. Die Anwendung INEZ.Core ist in der Version 1.0 produktionsreif, das Bezirksamt Hamburg Nord und die Behörde für Kultur und Medien haben sich bereiterklärt, den Betrieb zu pilotieren. Unter der Annahme, dass die Tests erfolgreich verlaufen werden, wird 2019 mit dem Rollout in die Fläche begonnen.
Es handelt sich bei INEZ.Core um eine vollständige Neuentwicklung, so dass die Anwenderinnen und Anwender das aus SF-INEZ bekannte Anwendungswissen nicht weiter nutzen können. Im Kern wird jedoch mit der Anwendung INEZ.Core ein als fachlich hinreichend bekannt vorausgesetzter Prozess umgesetzt, so dass keine Vermittlung von Grundlagenwissen notwendig ist. Aus der Vorstellung von Prototypen im Rahmen von Anwenderarbeitskreisen liegt die Rückmeldung vor, dass die neue Oberfläche als leicht handhabbar und logisch aufgebaut wahrgenommen wird. Vor diesem Hintergrund sind für die Phase des Rollouts die im Folgenden dargestellten Schulungsbedarfe identifiziert worden.

2. Zielgruppen

Der Rollout betrifft neben den Sachbearbeiterinnen und Sachbearbeitern, die unmittelbar und mittelbar mit der Anwendung arbeiten, auch einen erweiterten Adressatenkreis.

2.1 Führungskräfte

Durch die Rückführung der Zuwendungsfallbearbeitung auf den rechtlich vorgeschriebenen Prozessablauf könnten Anpassungen an der Ablauforganisation notwendig werden. Im Zeitverlauf selbst entwickelte Prozesse rund um die Zuwendungsfallbearbeitung lassen sich zum Teil künftig nicht mehr im System darstellen. Den Führungskräften soll Gelegenheit gegeben werden, anhand der

Demonstration einer Fallbearbeitung Handlungsbedarfe für den eigenen Bereich abzuleiten und im Plenum zu diskutieren.

2.2 Zuwendungssachbearbeitung

Der personalstärkste Bedarfsträger ist der Bereich der Sachbearbeiterinnen und Sachbearbeiter für Zuwendungsfälle.
Für diese Zielgruppe wird zunächst eine Deltaschulung angeboten.
Nach dem Rollout wird für den Linienbetrieb darüber hinaus eine Fluktuationsschulung notwendig werden. Ebenfalls sind perspektivisch aus der Entwicklung von Fachmodulen entstehende Schulungsbedarfe abzubilden. Diese Veranstaltungen werden später konzipiert.

2.3 Multiplikatoren, DRiVe-Support

Da die Multiplikatoren und Key-User in den Behörden und Ämtern erster Ansprechpartner für fachlich-technische Fragestellungen sind, wird nach einer Bedarfsabfrage ein adressatenorientierter, zweitägiger Workshop durchgeführt. Dieser richtet sich ebenfalls an die Fachliche Leitstelle und den Dataport-Anwendungssupport.

2.4 Train-the-Trainer

Aufgrund der Entscheidung von Kasse.Hamburg und ZAF über den Personaleinsatz muss ein Team von Dozenten befähigt werden. Dies wird im Rahmen eines zweitägigen Briefing-Workshops umgesetzt.

2.5 Innenrevisionen und Rechnungshof

Für Prüfinstanzen werden im Bedarfsfall eigene Workshops konzipiert und angeboten.

3. Umfang

Laut Datenbankabfrage SF-INEZ am 30.11.2018 sind aktuell 549 Anwenderinnen und Anwender im Bereich Zuwendung tätig. Die Verteilung nach Behörden bzw. Ämtern ist wie folgt:

Behörde/Amt	Anzahl
BA Altona	23
BA Bergedorf	13
BA Eimsbüttel	24
BA Harburg	22
BA Mitte	36
BA Nord	15
BA Wandsbek	32
BASFI	101
BGV	23
BIS	13
BKM	59
BSB	20
BSW	24
BUE	20
BWFG	32
BWVI	45
FB	5
IFB	6
JB	3
RH	4
KHH	35
SK	4
	559

3.1 Anzahl

Die Anwendung ist im aktuellen Entwicklungsstand auf die Bearbeitung von „Standard"-Zuwendungsfällen (unterjährige konsumtive Projektförderungen) begrenzt. Dementsprechend kann INEZ.Core nicht in allen oben genannten Bereichen schon in 2019 ausgerollt werden, es wird von Kasse.Hamburg ein Rolloutplan erstellt.

Aus diesem lässt sich die Anzahl der benötigten Veranstaltungen konkret ableiten. Derzeit wird von folgendem Mengengerüst ausgegangen:

Zielgruppe	Anzahl	Tage ges.
Führungskräfte	2	1
Zuwendungssachbearbeitung	60	60[1]
Multiplikatoren, DRiVe-Support	2	4
Dozenten	1	2
Gesamt		**67**

3.2 Dauer und Ablauf

Die Schulungsbedarfe der unter 2.dargestellten Zielgruppen werden durch die nachfolgend aufgeführten Angebote abgedeckt.

3.2.1 Führungskräfte

Es werden Informationsveranstaltungen beim ZAF mit einem Zeitansatz von zwei Stunden mit einer Gruppengröße von maximal 30 Teilnehmenden angeboten. Hier wird die Zuwendungsfallbearbeitung an einem Beispiel demonstriert und die einzelnen Bearbeitungsschritte erläutert. Im Anschluss sollen sich hieraus ergebende Fragen diskutiert werden[2].

3.2.2 Delta-Schulung Zuwendungsfallbearbeitung

Aufgrund der getroffenen Annahme, dass im Rahmen des Rollouts ausschließlich bereits mit der vorherigen Anwendung vertraute Personen zu schulen sind, wird die Deltaschulung als eintägige Veranstaltung konzipiert. Die maximale Teilnehmerzahl pro Veranstaltung beträgt 14. Aufgrund der Raumsituation bei Dataport ist davon auszugehen, dass für den Großteil der Veranstaltungen maximal 12 Plätze zur Verfügung stehen.

Im Rahmen der Schulung werden die Unterschiede zur bisher eingesetzten Anwendung SF-INEZ dargestellt. Anhand eines Schulungsbeispiels werden die

[1] Davon voraussichtlich 40 in 2019 und 20 in 2020
[2] Näheres siehe Veranstaltungsbeschreibung im Anhang

wesentlichen Schritte der Zuwendungsfallbearbeitung mit INEZ.Core geübt. Die Teilnehmerinnen und Teilnehmer bearbeiten einen an der Praxis orientierten Zuwendungsfall mit den Prozessschritten

- Erfassung
- Doppelförderungsprüfung
- Formelle Prüfung
- Fachliche Prüfung
- Mittelbindung
- Bescheiderstellung, -finalisierung, -versand
- Mittelabforderung
- Verwendungsnachweisprüfung
- Bescheidänderung. [3]

3.2.3 Key-User und Supportpersonal

Im Workshop werden die erweiterten Themen wie Benutzergruppen und Rechte, Geschäftspartner, Kontierungen, Anbindung Vorgangsbuch, Mittelbindung und Zahlungsabwicklung behandelt. Die Teilnehmerinnen und Teilnehmer sollen vertiefte Kenntnisse über die Anwendungsarchitektur und die Systemschnittstellen erlangen. Wesentliche Arbeitsschritte werden an den Systemen geübt.[4]

3.2.4 Train-the-Trainer

Die Delta-Schulungen werden durch ein Team von haupt- und nebenamtlichen Dozenten durchgeführt. In einem zweitägigen Workshop erhält das Team die Gelegenheit, sich mit den Schulungsinhalten vertraut zu machen. Darüber hinaus werden technische und organisatorische Rahmenbedingungen für die Schulungsdurchführung geklärt.[5]

3.3 Veranstaltungsorganisation und -ort

Die Schulungen werden durch das ZAF organisiert und finden mit Ausnahme der Info-Veranstaltung für Führungskräfte bei Dataport statt. Hierdurch wird gewährleistet, dass der Standardprozess für die Veranstaltungsdurchführung genutzt werden kann.

---

[3] Näheres siehe Veranstaltungsbeschreibung im Anhang
[4] Siehe oben
[5] Siehe oben

4. Inhalte

Die detaillierten Schulungsinhalte ergeben sich aus den Veranstaltungsbeschreibungen im Anhang.
Im Rahmen der Erstellung der Schulungsunterlage wird der benötigte Arbeitsvorrat genauer analysiert und mit den Beteiligten abgestimmt.

4.1 Unterlagen

Es ist für die Delta-Schulung ein Handout in Form einer Powerpoint-Präsentation sowie ein Übungs- und Lösungsheft zu erstellen. Form und Umfang sollen der Anforderung genügen, im praktischen Einsatz als kurzer Anwendungsleitfaden dienen zu können.
Für die übrigen Veranstaltungen wird lediglich ein Powerpoint-Handout benötigt, für die Train-the-Trainer-Workshops sind weitere Arbeitshilfen (Checklisten, Moderationspläne) 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 Schulungsvoraussetzungen

5.1.1 Installation

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

5.1.2 Kennungen und Passwörter

Die Berechtigung von Schulungsteilnehmern erfolgt durch die Zuordnung der Schulungskennungen zu Benutzergruppen. Für Schulungszwecke sind die AD-Gruppen U-KHH-INEZ-DB-Schule-SchulungDozent und U-KHH-INEZ-DB-Schule-

SchulungTN eingerichtet worden. Eine Einrichtung von Schulungsusern mit entsprechender Gruppenzuordnung wird durch Kasse.Hamburg vorgenommen. Die Passwortverwaltung erfolgt analog zu den Herakles-Schulungen durch den Dataport-Veranstaltungsservice. Entsprechende AD-Berechtigungen werden durch Kasse.Hamburg beantragt.

5.1.3 Übungsvorgänge

Es werden pro Veranstaltung jeweils ausreichend Übungsvorgänge benötigt. Im Einzelnen sind das

- Zuwendungsanträge
- Mittelabforderungen
- Verwendungsnachweise.

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.

Anhang: Veranstaltungsbeschreibungen

Dezentrale Fortbildung

INEZ.Core: Informationsveranstaltung für Führungskräfte

Mit der Neuentwicklung der Anwendung INEZ.Core wird die technische Unterstützung der Bearbeitung von Zuwendungsfällen auf den zuwendungsrechtlichen Kernprozess zurückgeführt. Spezifische Anforderungen, die über die Abbildung dieses Kerns hinausgehen, können durch die Entwicklung von Fachmodulen erfüllt werden. In einigen Fällen kann die Workflow-Logik der neuen Anwendung die Notwendigkeit auslösen, organisatorische Entscheidungen zu treffen und Abläufe neu zu regeln.
In dieser Veranstaltung sollen Führungskräfte einen Überblick über Gestaltung und Architektur von INEZ.Core erhalten und im Rahmen einer offenen Diskussion zu erörtern.

Lernziele

- Den aktuellen Ist-Zustand aus behörden- und ämterübergreifender Sicht beurteilen können
- Den Entwicklungsstand der Anwendung INEZ.Core und die Erweiterungsmöglichkeit durch Fachmodule kennen
- Handlungsbedarfe im Hinblick auf die Ablauforganisation ableiten

Themen

- Darstellung des Ist-Zustands
- Zuwendungsfallbearbeitung nach §46 LHO und VV
  - Wesentliche Unterschiede SF-INEZ / INEZ.Core
  - Prozessschritte
  - Technische Abbildung
- Diskussion

Zielgruppe Führungskräfte, in deren Verantwortungsbereich die Bearbeitung von Zuwendungsfällen liegt.

Dauer 2 Stunden

Dezentrale Fortbildung

INEZ.Core: Delta-Schulung Zuwendungsfallbearbeitung

Mit der Neuentwicklung der Anwendung INEZ.Core wird die technische Unterstützung der Bearbeitung von Zuwendungsfällen auf den zuwendungsrechtlichen Kernprozess zurückgeführt. Im Rahmen des Rollouts werden zunächst Anwenderinnen und Anwender geschult, die bisher mit SF-INEZ arbeiten.
In dieser Veranstaltung wird der Umgang mit der neuen Oberfläche und Anwendungslogik geübt.
Die Teilnehmerinnen und Teilnehmer lernen, anhand eines Schulungsbeispiels einen Zuwendungsfall komplett zu bearbeiten.

Lernziele

- Die Unterschiede zur bisherigen Anwendung kennen
- Verständnis für die neue Anwendungslogik entwickeln
- Die neue Anwendung bedienen können
- Zuwendungsfälle mit INEZ.Core bearbeiten können

Themen

- Oberfläche und Funktionen
- Antragsverarbeitung
  - Abbildung des Zuwendungs-Kernprozesses
- Zuwendungsmanagement
  - Erfolgskontrolle
  - Begleitung
  - Rechtsmittelverzicht
  - Mittelabforderung
- Verwendungsnachweisprüfung
  - Prozessschritte
- Bescheidänderungen

Zielgruppe Sachbearbeiterinnen und Sachbearbeiter, die Zuwendungsfälle bearbeiten

Dauer 1 Tag

Dezentrale Fortbildung

INEZ.Core für Key-User und Supportpersonal

Die Einführung der Anwendung INEZ.Core bringt neue Anforderungen an die Multiplikatoren, Key-User und den Support mit sich. Die bisherigen Aufgaben wie z.B. die Stammdatenanlage werden durch neue Anforderungen ersetzt.
In dieser Veranstaltung werden die Teilnehmerinnen und Teilnehmer mit der Handhabung vertraut gemacht und lernen die Bedienung des Systems sowie die technischen und organisatorischen Anforderungen im jeweiligen Verantwortungsbereich.

Lernziele

- Die Einrichtung von Rollen und Rechten kennen
- Abbildung des Kernprozesses Zuwendungsbearbeitung verstehen
- Den aktuellen Entwicklungsstand der Anwendung INEZ.Core kennen
- Die Komponenten von DRiVe bedienen können
- Kommunikationswege kennen
- Support für die Anwendung leisten können

Themen

- Rollen und Rechte
  - AD-Gruppen und -Benutzer
- Anwendung INEZ.Core
  - Prozessablauf
  - Stammdaten
    - Webservice Geschäftspartner
    - Webservice Kontierungen
  - Teilprozesse
- DRiVe-IT
  - Mittelbindung
  - Genehmigungsworkflow
- Support und Kommunikation

Zielgruppe INEZ-Multiplikatoren, Key-User und Supportpersonal

Dauer 2 Tage

Dezentrale Fortbildung

INEZ.Core: Train-The-Trainer

Durch die Ablösung der Anwendung SF-INEZ und den Rollout der Nachfolgelösung INEZ.Core bei den Behörden und Ämtern entsteht neuer Schulungsbedarf.
Um den erwarteten Umfang abdecken zu können, werden mehrere qualifizierte Lehrkräfte eingesetzt.
In dieser Veranstaltung werden die Dozentinnen und Dozenten mit der Anwendung vertraut gemacht und lernen die Bedienung des Systems sowie die technischen und organisatorischen Aspekte der Veranstaltungsvorbereitung und -durchführung.

Lernziele

- Abbildung des Kernprozesses Zuwendungsbearbeitung verstehen
- Den aktuellen Entwicklungsstand der Anwendung INEZ.Core kennen
- Das Schulungssystem bedienen können
- Notwendige Schulungsvorbereitungen durchführen können
- Supportstruktur für die Schulungsdurchführung kennen

Themen

- Zuwendungsfallbearbeitung nach §46 LHO und VV
  - Prozessschritte
  - Technische Abbildung
  - Wesentliche Unterschiede SF-INEZ / INEZ.Core
- Schulungsvorbereitung
  - System
  - Teilnehmer
  - Geschäftsvorfälle
- Veranstaltungsdurchführung
  - Technik
  - Ablauf
- Supportstruktur

Zielgruppe Dozentinnen und Dozenten für die Anwendung INEZ.Core

Dauer 2 Tage