Vereinbarung

nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG)

über die Einführung, den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens

FIETE – Wiki der hamburgischen Ausländerverwaltung

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

Das Ausländerrecht ist eines der komplexesten Rechtsgebiete. Es ist durch Bundesrecht, Europarecht und Völkerrecht geprägt und beeinflusst. Um den rechtlichen Anforderungen, insbesondere einer einheitlichen Rechts- und Ermessensauslegung Rechnung zu tragen, erfordert es ein zentrales Wissensmanagement. In FIETE sollen alle aktuell gültigen Informationen sowie eine Historie an einer Stelle, verständlich aufbereitet und einfach zu finden sein. Langfristig sollen alle am unmittelbaren Ausländerwesen beteiligten Stellen (bezirkliche Ausländerdienststellen, Rechtsämter der Bezirke, das Einwohner-Zentralamt sowie das Referat A25) an FIETE beteiligt sein. Alle Kolleginnen und Kollegen sollen durch FIETE in ihrer täglichen Arbeit, insbesondere in ihren täglichen Recherchen unterstützt werden. In Form eines Wiki wird FIETE das zentrale Wissensmanagementsystem für das Ausländerwesen in Hamburg. FIETE ermöglicht durch seine Informationen allen Anwenderinnen und Anwendern eine einheitliche Rechtsanwendung und der für die fachliche Steuerung zuständigen Fachbehörde letztlich eine zentrale Steuerungsmöglichkeit.

Zur Erfüllung dieses globalen Ziels, sind im Sinne des Wissensmanagements alle Kolleginnen und Kollegen dazu aufgerufen, sich freiwillig an FIETE zu beteiligen. Konkret ist gemeint, dass neue Seiten erstellt oder bestehende Seiten bearbeitet werden können. Damit diese Inhalte/Änderungen mit der fachlichen Steuerung bzw. den fachlichen Entscheidungsträgern abgestimmt sind, bevor sie für fachlich gültig in FIETE veröffentlicht werden, bedarf es eines Freigabeverfahrens. Das Freigabeverfahren wird über einen Workflow (nicht HIM-Workflow) innerhalb der FIETE-Webanwendung abgebildet.

Nr. 1

Gegenstand der Vereinbarung

Gegenstand der Vereinbarung sind die Einführung, der Betrieb, die Nutzung und die Weiterentwicklung des neuen IT-Verfahrens.

Zweck und Ziel des IT-Verfahrens sind in der Anlage 1 – Beschreibung der Verarbeitungstätigkeit[1] - näher beschrieben. Die Anlage ist Bestandteil der vorliegenden Vereinbarung.

Nr. 2

Geltungsbereich

Die Vereinbarung gilt für alle Verwaltungseinheiten der FHH, für die der Senat oberste Dienstbehörde ist, und die das Verfahren FIETE im Ausländerwesen der FHH anwenden bzw. nutzen.

Nr. 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).

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 jeweils zuständige Behörde bzw. Dienststelle, wird dabei die sich aus den §§ 3-14 Arbeitsschutzgesetz und Anlage 6 der Verordnung über Arbeitsstätten ergebenden Pflichten erfüllen[2].

---

[1] Eine Verfahrensbeschreibung soll nach den Vorgaben des Art 30 Abs. 1 Satz 2 lit. b DS-GVO als eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung oder als inhaltliche „Beschreibung des Verfahrens" erfolgen. Zumindest sollten der Zweck und das Ziel aus der Verfahrensbeschreibung hervorgehen.

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

Nr. 4

Arbeitsplatz- und Einkommenssicherung

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

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

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

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

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

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

Nr. 5

Datenschutz, Schutz vor Leistungs- und Verhaltenskontrolle

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

Die 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) zuläs-

sig. Der auslösende Sachverhalt ist zu dokumentieren. Der zuständige Personalrat ist möglichst[3] vorher zu unterrichten. Die bzw. der betroffene Beschäftigte ist zu unterrichten, sobald dies ohne Gefährdung des Aufklärungsziels möglich ist. Daten, die ausschließlich zum Zwecke der Aufklärung erhoben wurden, sind zu löschen, sobald der Verdacht ausgeräumt ist oder sie für Zwecke der Rechtsverfolgung nicht mehr benötigt werden.

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

Nr. 6

Qualifizierung der Anwenderinnen und Anwender

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

Bei der Entwicklung des Qualifizierungskonzepts wird geprüft, ob bei mittelbar von dem IT-Verfahren betroffenen Beschäftigten ein Qualifizierungsbedarf besteht. Die Einzelheiten werden in einem Qualifizierungskonzept dargestellt, das als Anlage 2 beigefügt ist.

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

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

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

---

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

Nr. 7

Organisation und Ablauf

Die Einführung des neuen IT-Verfahrens bedeutet für die Anwenderinnen und Anwender, dass sich die bisherigen Arbeitsweisen 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.

Auf dieser Basis sollen repräsentative Anwenderinnen und Anwender sowie die örtlichen Personalräte und die Spitzenorganisationen der Gewerkschaften und Berufsverbände die Möglichkeit erhalten, das zukünftige IT-Verfahren frühzeitig kennen zu lernen und in Bezug auf zentrale funktionelle Anforderungen qualitätssichernde Hinweise zu geben.

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

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.

Nr. 8

Evaluation des Betriebs unter Beteiligung der Spitzenorganisationen

Spätestens ein Jahr* nach Inkrafttreten der Vereinbarung wird durch die fachlich zuständige Stelle eine Evaluation durchgeführt.

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 und ggf. 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.

Nr. 9

Verfahren bei Änderungen

Das unter der Präambel 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 zu der Änderung innerhalb dieser Frist äußert, gilt die Zustimmung als erteilt. Andernfalls nehmen die Beteiligten Verhandlungen auf.

Nr. 10

Schlussbestimmungen

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

Die Vereinbarung tritt mit sofortiger Wirkung in Kraft.

Sie kann mit einer Frist von sechs Monaten zum Ende eines Jahres gekündigt werden. Bei Kündigung wirkt die 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.

Hamburg, den 22. Sep. 2021

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 nach Art 30 Abs. 1 Satz 2 lit. b DS-GVO
2. Berechtigungs- und Rollenkonzept
3. Qualifizierungskonzept

Hamburg

Beschreibung der Verarbeitungstätigkeit

(Bitte an die Verzeichnisführende Stelle absenden!)

Blatt-Nr.:
Von der Verzeichnisführenden Stelle auszufüllen!

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

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

Allgemeines			
	Datum:	10.05.2021	
	Ausfüllende Person:	Ole Themlitz	
	Telefonnummer:	040/42839-2223	
	Bezeichnung des Verfahrens:	FIETE – Wiki der hamburgischen Ausländerverwaltung	
	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]:	Mit Rollout der Software, voraussichtlich Ende drittes Quartal 2021	
	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):	Behörde für Inneres und Sport	
1.2	Vertreter der verantwortlichen Organisationseinheit (optional):	-	

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

1.3	Fachliche Leitstelle (bei IT-Verfahren) bzw. zuständige Stelle (bei nicht automatisierten Verfahren): Verantwortliche Führungskraft: Leitzeichen:	BIS – Amt für Migration – Abteilung M3 – Fachliche Leitstelle FIETE Ole Themlitz M310.LF	
1.4	Ansprechpartner, sofern nicht verantwortliche Führungskraft: Telefonnummer:	- -	
1.5	Name des Datenschutzbeauftragten (optional):	Manuel Manhart	
1.6	Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt[6]: Auftragsnummer:	- -	

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung[7]			
2.1	Beschreibung und Zweckbestimmung der Verarbeitung von Daten[8]	Beschreibung der Verarbeitung: FIETE ist ein Wiki, welches die zentrale Wissensdatenbank für die hamburgische Ausländerverwaltung werden soll. In FIETE können von allen an die Anwendung angeschlossenen User neue Wiki-Seiten erstellen oder bestehende Wiki-Seiten bearbeiten. Im Wiki werden jegliche Änderungen revisionssicher über eine Seitenversionierung dokumentiert. Dabei wird der Name der bearbeitenden Person in Verbindung mit (teilweise) Datum, Uhrzeit und Inhalt der Bearbeitung gespeichert. Zudem besitzen alle User eine eigene Profilseite, auf der neben individuellen Eintragungen (freier Text zur Person und Profilbild) Daten aus dem Active Directory der FHH übertragen werden und alle eigenen Bearbeitungen im Wiki aufgelistet sind. Darüberhinaus gibt es zu fast allen Inhaltsseiten eine Diskussionsmöglichkeit, bei der alle Anwenderinnen und Anwender Gedanken und Fragen platzieren können, um sich untereinander auszutauschen. Dabei ist wie bei Seitenänderungen der Name sichtbar. Weiterhin gibt es spezielle Wiki-Seiten, auf denen Änderungen von bestimmten Personen oder Änderungen auf bestimmten Seiten gezielt gesucht und aufgelistet werden können. Dazu gibt es spezielle Wiki-Seiten, auf denen letzte Änderungen aufgelistet werden – dort sind ebenfalls die Namen der Bearbeiterinnen und Bearbeiter zu finden. Diese Seiten sollen verfügbar bleiben, um grundsätzlich inhaltliche Änderungen nachvollziehen zu können.	

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

		Letztlich werden auch auf allen Inhaltsseiten direkt die Autorinnen und Autoren sowie die letzten Bearbeiterinnen und Bearbeiter genannt. Diese sind ebenfalls für alle anderen User sichtbar. Alle übrigen personenbezogenen, systemseitig verfügbaren Auswertungen werden zugriffsbeschränkt und dürfen nicht ausgewertet werden. Zur besseren Anschaulichkeit wird als Anlage zu dieser Verfahrensbeschreibung eine Übersicht zu Wiki-Seiten gegeben, auf denen die Nennung der Namen im Wiki dargestellt wird. Beschreibung der Zweckbestimmung: Sonstiges: Die Sichtbarkeit der Namen an den zuvor genannten Stellen beruht im Wesentlichen auf zwei Gründen: Da in einem Wiki grundsätzlich alle User Bearbeitungen vornehmen können, muss revisionssicher festgehalten werden, wann welche Veränderungen durch wen vorgenommen worden sind. Dies erhöht die Transparenz und Nachvollziehbarkeit der dargestellten Wissensinhalte enorm. Letztlich wird damit auch Vandalismus im Wiki unwahrscheinlicher. Zudem ist es ein zentraler Ansatz im Wissensmanagement, dass Personen, die freiwillig eigene Wissensinhalte im Wiki teilen, eine „Belohnung" bzw. „Motivation" erhalten. Es ist evident, dass die Bereitschaft Inhalte und Wissen zu teilen maßgeblich steigt, wenn sie unter dem eigenen Namen veröffentlicht werden. Die Verfasserinnen und Verfasser erhalten „Ruhm" und „Anerkennung".	
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* Die User haben die Möglichkeit, einer systemseiteigen Datenschutzerklärung zuzustimmen. Es ist vorgesehen, dass beim Ablehnen der Einwilligung der Zugriff auf FIETE verweigert wird. Zudem wird durch die aktive Arbeit im Wiki (alles, was über den rein lesenden Zugriff hinausgeht) in Form des Bearbeitens oder Ergänzens von Wissensinhalten, eine Hinweis zur	

		Einwilligung beim Speichern gezeigt. Sollen Seiten bearbeitet oder neu hinzugefügt werden, ohne den eigenen Namen sichtbar zu machen, kann sich vertrauensvoll an die FIETE-Redaktion gewandt werden. Sie kümmert sich um die Bearbeitung oder Einstellung.	
☐	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:* Klicken Sie hier, um Text einzugeben.	
☐	Weitere:	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Klicken Sie hier, um Text einzugeben.	
3. Beschreibung betroffener Personen- und Datenkategorien			
3.1	Beschreibung der betroffenen Personengruppen[9]:	Beschäftigte Sonstige: - Beschreibung: Alle unmittelbar an der hamburgischen Ausländerverwaltung beteiligten Kolleginnen und Kollegen, insbesondere aus dem Referat A25 der BIS, den Abteilungen M2, M3 und M4 des Amtes für Migration der BIS sowie den bezirklichen Ausländerdienststellen und Rechtsämtern.	
3.2	Beschreibung der Art der Daten[10] bzw. Datenkategorien	Mitarbeiterdaten Sonstige: - Beschreibung: Vor- und Nachname, Anmeldedaten, Kontaktdaten aus Active Directory	
3.3	Werden besondere Kategorien[11] von Daten verarbeitet (Art. 9 Abs. 1 DS-GVO)?	☐ ja, welche? Wählen Sie ein Element aus.	

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

		☒ 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)	Fachverfahren FIETE	
	Art der Daten	Anmeldenamen, Vor- und Nachname, Kontaktdaten aus Active Directory	
	Zweck der Daten-Mitteilung	Siehe Verfahrensbeschreibung	
4.3	Externe Empfänger und Dritte	☐ ja ☒ nein	
	Externe Stelle	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.	
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: Klicken Sie hier, um Text einzugeben. ☒ nein	
	Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:	Seiten (auf denen ggf. Namen der Autorin bzw. des Autors stehen) werden nicht gelöscht – sie werden in einer Historie archiviert, um auch ältere Informationsstände abbilden zu können.	
6. Mittel der Verarbeitung (optional) **Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?[14]**			

[12] Hinweis Nr. 12 der Anlage 1
[13] Hinweis Nr. 13 der Anlage 1
[14] Hinweis Nr. 14 der Anlage 1

	Bezeichnung: Hersteller: Funktionsbeschreibung: Bereitstellung:	Wiki-Webanwendung Bluespice / WikiMedia Standardsoftware zum Aufbau von Wikis ☐ Eigenentwickelte/ individuelle Software ☒ Standard-Software ☐ Cloud-Services ☐ Sonstige: Klicken Sie hier, um Text einzugeben.	
7. Zugriffsberechtigte Personengruppen (vereinfachtes Berechtigungskonzept)[15]			
	Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte Berechtigungskonzept:	Siehe Anlage 3	
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 Bitte Ergebnis der Risikoprüfung als Anlage beifügen.	Link zur Datenbank bzw. pdf-Format BSI-Standard
8.5	Es wurden die Erforderlichkeitsprüfung („Schwellwertanalyse") und ggf. die Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO durchgeführt.	☒ ja, Ergebnis der Erforderlichkeitsprüfung („Schwellwertanalyse") und ggf. die durchgeführte DSFA als Anlage beifügen ☐ nein	Schwellwertanalyse; DSFA
8.6	Bei Verfahren, die bei Dataport gehostet werden: Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMS der FHH sichergestellt (vgl. Anlage 3).	☐ Es liegt ein Verfahren vor, das bei Dataport gehostet wird.	
8.7	Bei Verfahren, die nicht bei Dataport gehostet werden:	☒ 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: Über die Datenschutzzentrale innerhalb der Anwendung kann eine Liste mit den gesammelten Daten abgerufen werden. ☐ 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?	Direkt in FIETE, im Bereich „Alles über FIETE:Datenschutz“	Link zu den Formularen
11. Sonstiges			
	Anmerkungen:	Klicken Sie hier, um Text einzugeben.	

..... Verantwortlicher

..... 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. Folgende Definitionen beschreiben die einzelnen Verarbeitungsschritte:

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

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

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

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

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

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

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

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

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

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

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

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

Hinweis Nr. 12

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Anlage 2

Übersicht und Erläuterungen zu den technischen und organisatorischen Maßnahmen

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

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

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

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

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

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

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

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

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

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

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

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

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

Maßnahmen zur Pseudonymisierung personenbezogener Daten

Hierzu zählen u. a.:

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

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

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

für den Schutz personenbezogener Daten eingesetzt werden.

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

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

Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste

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

Hierzu zählen u. a.:

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

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

Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste

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

Hierzu zählen u. a.:

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

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

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

Hierzu sind u. a. folgende Maßnahmen erforderlich:

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

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

Hierzu zählen u. a.:

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

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

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

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

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten

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

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

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

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

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

Anlage 3

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

Grundwerte nach DS-GVO	Definierte Technische und Organisatorische Maßnahmen (TOMs) nach § 64 BDSG	Ergriffene Technische und Organisatorische Maßnahmen (TOMs) der FHH
Datenminimierung Art. 5 Abs. 1 lit.c DS-GVO	-	Verwaltungsvorschrift IT-Projekte (bei kleineren IT-Projekten wird diese VV sinngemäß angewendet) Richtlinie über Mindestanforderungen an die Sicherheit der Datenverarbeitung auf UNIX-Rechnern (UNIX-Richtlinie)
Gewährleistung der **Integrität** Art. 32 Abs. 1 lit. b DS-GVO	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)
	Datenintegrität (§ 64 Abs. 3 Nr. 11 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Geschäftsbestimmungen der Behörden (Revisionfähige Prozessbeschreibungen, Überprüfbarkeit des Verwaltungshandelns)
	Datenträgerkontrolle (§ 64 Abs. 3 Nr. 2 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich Entsorgungs-Richtlinie
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz

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

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

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

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

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

Definitionen der Grundwerte nach DS-GVO:

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

Definitionen der TOMs gem. § 64 BDSG:

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

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

Anlage 2 – Qualifizierungskonzept

Für die allgemeine Nutzung von FIETE sind im Prinzip keine besonderen Kenntnisse und Fähigkeiten erforderlich. FIETE wird durch seine übersichtliche und anwenderorientierte Gestaltung intuitiv und einfach als Webanwendung zu benutzen sein.

Nichtsdestotrotz soll es Einstiegsschulungen (ca. zwei Stunden) geben, die **alle Anwenderinnen und Anwendern**, insbesondere neuen Kolleginnen und Kollegen, über die allgemeine Struktur und Funktionen vorbereitet. Dabei sollen die folgenden Aspekte geschult werden:

- Grundzüge des Wissensmanagements und der Ziele von FIETE
- Strukturelemente in FIETE (Seitenmodell, Kategorien, Namensräume, etc.)
- Aufbau von Seiten
- Suchfunktion und dort bestehende Einstellungsmöglichkeiten
- Individualisierungsmöglichkeiten (Benutzerseite, Favoriten, etc.)
- Vorstellung des FIETE-Café (Diskussionsforum)
- Qualitätsmanagementverfahren

Diese Schulung soll bedarfsgerecht zum Roll-Out angeboten werden. Regelmäßige Auffrischungsveranstaltungen in monatlichen Formaten sind in Planung.

Für den Kreis der Berechtigungsgruppe **fachliche Steuerung** wird es eine auf der Einstiegsschulung aufbauende Vertiefungsschulung geben. Der Schwerpunkt liegt auf der Freigabe von Inhalten. Folgende Inhalte sollen geschult werden:

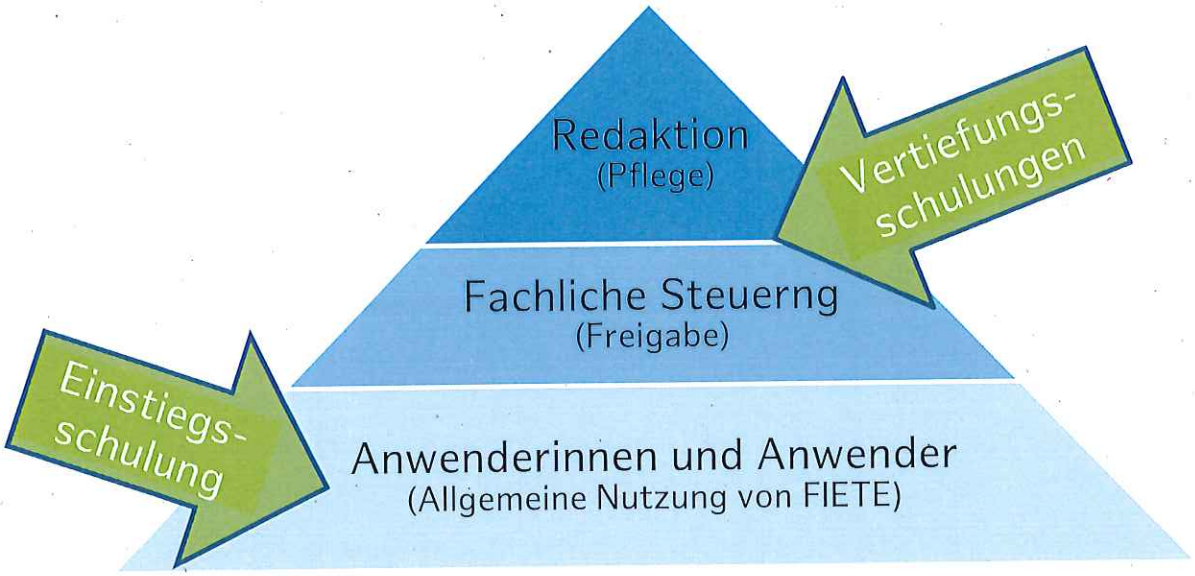
- Erweiterte Informationen zum Aufbau von Seiten, insbesondere Informationen zu Syntax sowie Anforderungen an Form und Sprache
- technische Logik der Suchfunktion
- Qualitätsmanagementverfahren aus Perspektive der fachlichen Steuerung

Hamburg

Darüber hinaus muss die **FIETE-Redaktion** auf ihre Tätigkeiten im Rahmen des Qualitätsmanagements und der Pflege von Wiki-Inhalten (insbesondere Seitenverschiebungen, Löschungen, Strukturelle Gesichtspunkte, etc.) vorbereitet werden. Folgende Inhalte sollen geschult werden:

- Erweiterte Informationen Zur Wartung von Seiten, insbesondere Löschen, strukturelle Veränderungen und Seitenverschiebung
- Vorbereitung auf First-Level-Support
- Qualitätsmanagementverfahren aus Perspektive der Redaktion

Grafisch ergibt sich folgende Schulungsübersicht, die letztlich auch mit dem in Anlage 3 beschriebenen Rollenkonzept verbunden ist:



Der Erfolg von FIETE hängt maßgeblich an den abgestimmten und verbindlichen Informationen, die hinterlegt werden. Daher steht das Freigabeverfahren an zentraler Stelle des Qualitätsmanagements. Eine besondere Stellung wird die **FIETE-AG** als regelmäßig tagendes Gremium der Nutzerinnen und Nutzer haben. Sie werden als Multiplikatoren in ihren Organisationseinheiten dienen. Im Rahmend der FIETE-AG werden Ihnen vertiefte Kenntnisse zu FIETE und den Prozessen der Redaktion vermittelt.

Hamburg

Anlage 3 – Rechte- und Rollenkonzept

Dieses Berechtigungskonzept definiert die Zugriffsregeln zum Wissensmanagementsystem FIETE für bestimmte Benutzergruppen. Grundsätzlich ist FIETE für alle Kolleginnen und Kollegen der hamburgischen Ausländerverwaltung zugänglich und nutzbar. Gewisse Tätigkeiten im Wiki sind jedoch nicht für alle Anwenderinnen und Anwender gleichermaßen vorgesehen. Neben Daten und Informationen besteht FIETE aus einer besonderen technischen Infrastruktur. Diese Ressourcen müssen vor Veränderung oder Zerstörung (**Datensicherheit**) und ihren unrechtmäßigen Gebrauch (**Datenschutz**) geschützt werden, ohne die Produktivität der Organisation zu hemmen.

a) Benutzergruppen

BlueSpice ermöglicht die Erstellung bzw. Bearbeitung eines differenzierten Berechtigungskonzeptes. Grundlage hierfür ist die Definition von Benutzern bzw. Benutzergruppen. Standardmäßig vorhanden und wegen ihrer elementaren Bedeutung für die Funktionalität für das Wiki nicht löschbar sind die Benutzergruppen *bot*, *bureaucrat* und *sysop*. Weiterhin standardmäßig vorhanden sind die Gruppen *autoreview*, *editor*, *smwadministrator*, *smwcurator*, *widgeteditor*. Alle standardmäßig vorhandenen Benutzergruppen werden nicht verwendet.

Stattdessen werden eigene Benutzergruppen erstellt, die sich zum einen aus dem individuellen Anwendungszusammenhang und zum anderen wegen der komfortablen Anknüpfung an das Active Directory ergeben. Durch die Verknüpfung der individuellen Benutzergruppen an das Active Directory entfällt die manuelle Benutzerkontenpflege.

Hamburg

Es ergeben sich folgende Benutzergruppen:

- **ROL-BIS-Wiki-Admins**
  Technische Betreuung der Wiki-Farmverwaltung auf den Datenbank- und Webservern von A/IT. Aktuell bestehend aus Susanne Mohr und Nico Rienitz.

- **ROL-BIS-FIETE-Admins**
  Administration für das Wiki FIETE durch den FIETE-Wissensmanager (M310.LS). Aktuell bestehend aus Ole Themlitz.

- **ROL-BIS-FIETE-Redaktion**
  Wahrnehmung der Redaktionstätigkeit (Steuerung von Beiträgen im Rahmen des Freigabeverfahrens) und erweiterte Bearbeitungsmöglichkeiten in FIETE. Im Testaufbau bestehend aus Birgitt Schlenga, Julia Petersen, Susanne Mohr, Karen Jäger und Ole Themlitz. Im Echtbetrieb bestehend aus den zukünftigen Beschäftigten der FIETE-Redaktion.

- **ROL-BIS-FIETE-Fachliche-Steuerung**
  Mitglieder der fachlichen Steuerung sind Entscheidungsträgerinnen und Entscheidungsträger der hamburgischen Ausländerverwaltung, die auf Grund ihrer Stelle verbindliche rechtliche Vorgaben für nachgeordnete Kolleginnen und Kollegen erlassen dürfen. Zur Gruppe zählen: A25, M20, M30, M40, alle Referatsleitungen der genannten Abteilungen sowie M312.

- **ROL-BIS-FIETE-User**
  Alle Anwenderinnen und Anwender von FIETE. Zunächst bezirkliche Ausländerdienststellen, unmittelbar anschließend BIS/ Amt M.

b) Rollen und Berechtigungen

Die Rechteverwaltung ermöglicht die Vergabe von Rollen (Kombination von einzelnen Rechten) an Benutzergruppen. Rollen sind mit individuellen und systemseitig vorgegebenen Berechtigungen (Rechte, die eine bestimmte Aktion im Wiki ermöglichen) ausgestattet. BlueSpice sieht systemseitig folgende Rollen vor:

- **bot**
  Existiert zur Ausführung wiederkehrender Systemaktionen. Diese Rolle ist in BlueSpice dem BSMaintenance-Benutzer über die gleichnamige bot-Gruppe zugeordnet. Die bot-Gruppe sollte normalerweise nicht geändert werden und wird nur von der Systemadministration eingesetzt.

- **maintenanceadmin**
  Systemadministration – Ermöglicht im Wesentlichen Änderungen an Datenbank und Webservern. Stellt die Integrität des Wikis sicher.

- **admin**
  Administration – ermöglicht Zugriff auf alle administrativen Spezialseiten sowie generell alle gängigen Verwaltungsfunktionen wie die Rechteverwaltung.

- **author**
  Ermöglicht das Erstellen und Bearbeiten von Seiten. Das Verschieben oder Löschen von Seiten ist in dieser Rolle nicht enthalten.

- **structuremanager**
  Ermöglicht einige Aktionen zur strukturellen Wikipflege wie das Verschieben von Seiten, Massenlöschung von Seiten oder Text suchen und ersetzen, sowie das Umbenennen von Namensräumen.

- **accountselfcreate**
  Ermöglicht das automatische Erstellen von neuen Benutzerkonten und wird für Single-sign-on benötigt.

- **commenter**
  Ermöglicht das Erstellen von Diskussionsbeiträgen und Seitenbewertungen, aber nicht von Seiten selbst. Die Rolle editor beinhaltet alle Rechte der Rolle commenter.

- **reader**
  Ermöglicht das Lesen von Wikiseiten. Benutzer können außerdem ihre persönlichen Einstellungen bearbeiten.

- **autocreateaccount**
  Automatische Anmeldung mit einem externen Benutzerkonto.

- **editor**
  Enthält inhaltliche Bearbeitungs-, Wartungs- und Strukturierungsrechte für das Wiki.

- **reviewer**
  Fähigkeit, noch nicht freigegebene Seiten oder Änderungen freizugeben.

c) Rechteverwaltung- und Verteilung

Grundsätzlich soll es in FIETE sieben Rollen geben, die jeweils unterschiedliche systemische Rechte innehaben werden. Die Rollen definieren sich wie folgt:

Benutzergruppen	Rollen
ROL-BIS-Wiki-Admins	maintenanceadmin, reader
ROL-BIS-FIETE-Admins	admin, structuremanager, accountmanager, reader
ROL-BIS-FIETE-Redaktion	editor, reviewer, author, commenter, reader
ROL-BIS-FIETE-Fachliche-Steuerung	reviewer, author, commenter, reader
ROL-BIS-FIETE-User	author, commenter, reader

Grundsätzlich erhalten alle Anwenderinnen und Anwender (ROL-BIS-FIETE-User) eine Ausstattung mit Rechten, die die grundlegenden Kernfunktionen von FIETE nutzbar machen. Dazu zählen das Lesen von Seiten, der Export von Seiten in PDF, das Erstellen von Diskussionen, sowie das Erstellen und Bearbeiten von Wiki-Seiten.

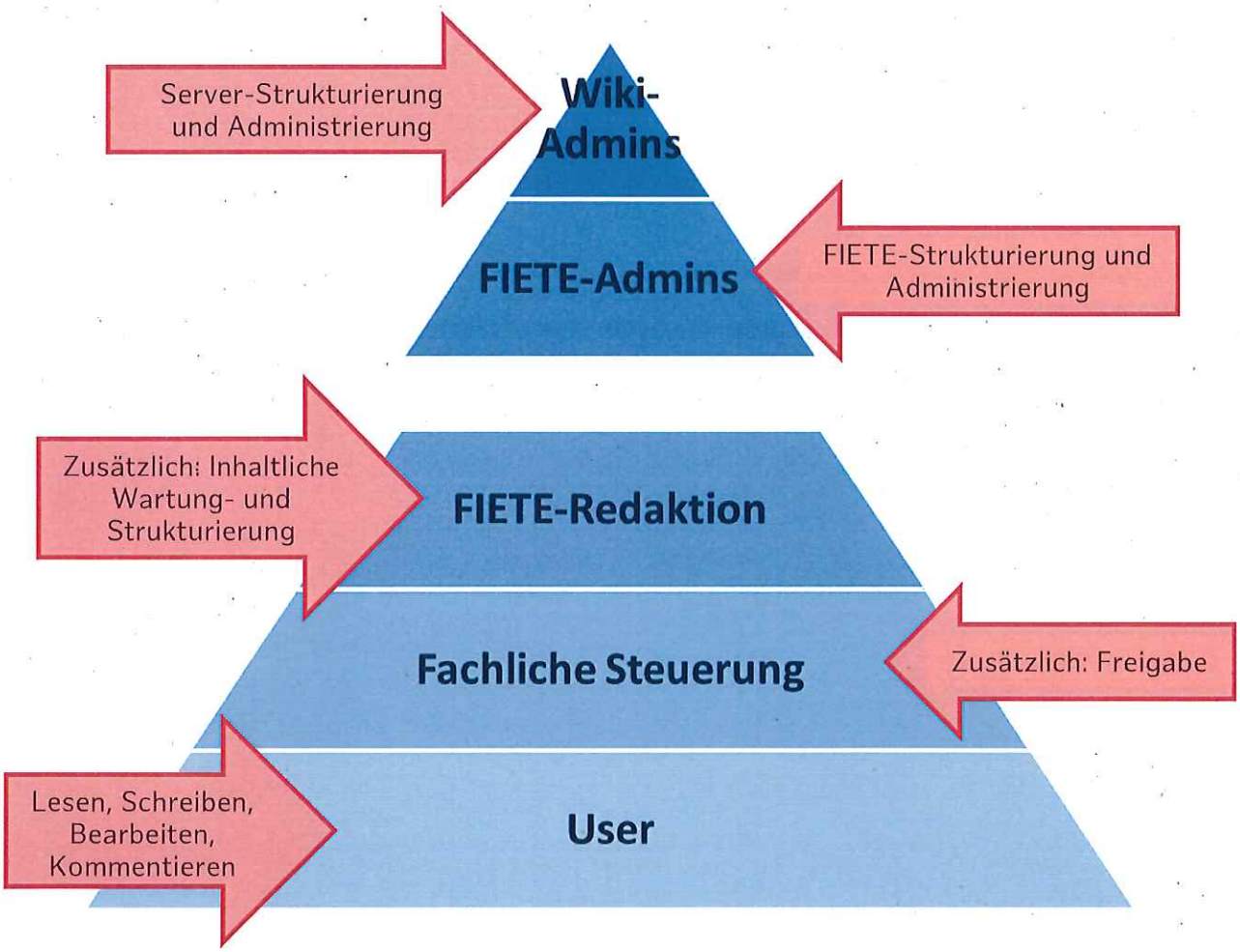
Die Mitglieder der FIETE-Redaktion (ROL-BIS-FIETE-Redaktion) erhalten umfassendere Bearbeitungs-, Wartungs- und Strukturierungsrechte im Wiki. Die Redaktion steuert fachliche Änderungswünsche und kann neue Seiten oder Änderungen auf bestehenden Seiten freigeben, damit sie im Wiki für alle sichtbar werden. Zudem achtet die Redaktion auf die Einhaltung des Stylegides sowie die allgemeine Wiki-Pflege – insbesondere auf die Aktualität.

Da die Mitglieder der fachlichen Steuerung wegen ihrer Position dazu befähigt sind, verbindliche fachliche Entscheidungen zu treffen, erhalten sie genau wie die FIETE-Redaktion Freigaberechte. Zudem erhalten Sie Zugriff auf Übersichtseiten zu noch nicht freigegeben Änderungen.

Der FIETE-Wissensmanager (ROL-BIS-FIETE-Admins) verantwortet neben dem Change- und Wissensmanagement die inhaltliche und wiki-systemische Struktur von FIETE. Er gliedert u.a. Inhaltsbereiche, berät bei der Transformation von bestehendem Wissen zu FIETE und entwickelt das Wiki kontinuierlich weiter. Dazu stehen

ihm umfangreiche Bearbeitungsrechte zur Verfügung. Zur Sicherstellung des Trennungsprinzips enthält der Wissensmanager sowohl eine Redaktions- als auch eine Admin-Kennung.
Zur Sicherstellung der technischen Integrität und Funktionalität des Wikis sind bestimmte Bearbeitungsrechte der Systemadministration bei A/IT (ROL-BIS-Wiki-Admins) vorbehalten. Sie können u.a. Änderungen auf den Web- und Datenbankservern vornehmen.

Zur vereinfachten Darstellung des Berechtigungskonzeptes dient folgende Darstellung:



Hamburg