Vereinbarung

nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG)

über den laufenden Betrieb, die Nutzung und die Weiterentwicklung der IT-Systeme

Hunderegister und OKTAGON

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

Im Rahmen des Programms Cupola wurden zur Ablösung von BACom (Behördliche Aufgaben mit Computer-Unterstützung) die neuen IT-Fachverfahren Hunderegister und Oktagon BAU und SWAN[1] eingeführt, um die Digitalisierung der Dienststellen zu unterstützen (vgl. Anhang 1).
Ziel ist es, die Qualität der Arbeitsprozesse für alle Beteiligten zu verbessern und die Beschäftigten bei der effektiven und effizienten Aufgabenerledigung durch durchgängig digitalisierte, nutzerfreundliche sowie zukunftssichere IT-Verfahren zu unterstützen.
Mit dieser Produktivvereinbarung wird die Einführungsvereinbarung vom 03. August 2021 abgelöst.

§ 1

Gegenstand der Vereinbarung

Gegenstand der Vereinbarung sind die in den Anlagen 1, 2 und 3 beschriebenen IT-Fachverfahren Hunderegister und Oktagon BAU und SWAN[1]. Die Anlagen sind Teil der Vereinbarung.

§ 2

Geltungsbereich

Die Vereinbarung gilt für alle Verwaltungseinheiten der FHH, für die der Senat oberste Dienstbehörde ist und die mit den in den Anlagen beschriebenen IT-Fachverfahren arbeiten.

§ 3

Ergonomie und Arbeitsplatzgestaltung

Die Gestaltung der ergonomischen Eigenschaften der IT-Verfahren 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). Der Prozess zur Weiterentwicklung der Gebrauchstauglichkeit wird fortgesetzt und transparent gemacht.

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 Maßnahmen zur Erreichung der digitalen Barrierefreiheit sind in dem als Anlage 3 beigefügten Maßnahmenplan dargestellt. Der Prozess zur weiteren Herstellung der Barrierefreiheit wird fortgesetzt und transparent gemacht.

---

[1] Ohne die Verfahren „Wasserrecht" und „Naturschutz".

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].

§ 4

Arbeitsplatz- und Einkommenssicherung

Der laufende Betrieb der IT-Fachverfahren 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.

§ 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.

---

[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

Dabei sollen im Produktivbetrieb keine nutzerbezogenen Auswertungen verwendet werden, die sich auf Gruppen mit weniger als drei Personen beziehen, soweit keine gesetzlichen Verpflichtungen diesem Grundsatz widersprechen (ergänzend zu Oktagon siehe Anlage 4).

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[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 der in den Anlagen 5 und 6 beigefügten Rechte- und Rollenkonzepten, in denen die für die verschiedenen Funktionen/Mitarbeitergruppen erforderlichen Berechtigungen festgelegt werden.

§ 6
Qualifizierung der Anwenderinnen und Anwender

Mit der Einführung der Verfahren 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 Qualifizierungsmaßnahmen sollen zeitnah vor Einführung der IT-Verfahren erfolgen. Für die Qualifizierungsmaßnahmen trägt die zuständige Behörde oder Dienststelle in Verbindung mit der fachlich zuständigen Stelle die Verantwortung.

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.

[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.

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

Die als Anlagen 7 bis 9 beigefügten Qualifizierungskonzepte bilden die Grundlage für die Ermittlung des Qualifizierungs- und Nachqualifizierungsbedarfs der Beschäftigten sowie den Rahmen für die entsprechende Umsetzung im Kontext der Fachverfahren.

§ 7

Evaluation des Betriebs unter Beteiligung der Spitzenorganisationen

Spätestens 3 Jahre nach Inkrafttreten der Vereinbarung 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),
- Anwendungstauglichkeit (Gebrauchstauglichkeit).

Die Evaluation umfasst auch die Überprüfung der Umsetzung des Maßnahmenplanes. Soweit möglich werden bei der Evaluation alle Entwicklungsziele zu fachlichen Belangen, Datenschutz 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.

§ 8

Verfahren bei Änderungen

Die in den Anlagen beschriebenen IT-Fachverfahren werden bei Bedarf weiterentwickelt.

Vor wesentlichen Änderungen der Verfahren sowie erforderlichen Anpassungen der Anlagen, z. B. des jeweiligen Berechtigungs- oder 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.

§ 9

Weitere Verfahren

Im Falle der Einführung weiterer Verwaltungsverfahren bzw. Verfahrenstypen über die Software Oktagon werden die Spitzenorganisationen rechtzeitig vorab schriftlich informiert. Es werden eine Beschreibung von Zielen und Zwecken des Verfahrens sowie die gemäß der IT-Rahmenvereinbarung üblichen Anlagen übersandt.

Die Spitzenorganisationen der Gewerkschaften haben die Möglichkeit binnen 6 Wochen nach Zugang der Information die Notwendigkeit zur Aufnahme von Verhandlungen zu erklären. Geht keine Erklärung der Spitzenorganisationen der Gewerkschafften ein, so gelten die Anlagen als genehmigt und werden Bestandteil dieser Vereinbarung.

§ 10

Schlussbestimmungen

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

Die Vereinbarung tritt am 01. Januar 2025 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.

Bei Beendigung eines einzelnen IT-Fachverfahrens ist eine Kündigung von einzelnen Anlagen zulässig. In diesem Fall ist eine Kündigung dieser Anlage mindestens 6 Monate im Vorwege möglich. Die Anlage wird nach Ablauf der Kündigungsfrist unter Angabe des Beendigungsdatums als gekündigt gekennzeichnet.

Gleichzeitig tritt die Vereinbarung nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG) über die im Rahmen des Programms Cupola einzuführenden IT-Verfahren (Einführungsvereinbarung) vom 03.08.2021 außer Kraft*.

Hamburg, den 31. Jan. 2025

Freie und Hansestadt Hamburg

für den Senat

Volker Wiedemann

dbb hamburg

beamtenbund und tarifunion

Thomas Treff

Deutscher Gewerkschaftsbund

-Bezirk Nord-

Olaf Schwede

Anlagen:

1. Beschreibung der Verarbeitungstätigkeit Hunderegister
2. Beschreibung der Verarbeitungstätigkeit OKTAGON
   2.a Beschreibung von Zweck und Ziel des Fachverfahrens Oktagon SWAN
3. Maßnahmenplan Barrierefreiheit
4. Regelung zur Datenauswertung in Oktagon
5. Rechte- und Rollenkonzept Hunderegister
6. Rechte- und Rollenkonzept OKTAGON
7. Qualifizierungskonzept Oktagon BAU
8. Schulungskonzept Oktagon SWAN
9. Qualifizierungskonzept Hunderegister

.

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:	23.05.2022	
	Ausfüllende Person:	Projektteam Hunderegister	
	Mail:	hunderegisterhamburg@sk.hamburg.de	
	Bezeichnung des Verfahrens:	Hunderegister	
	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 Verknüpfen ☒ Einschränken ☒ Löschen ☐ Vernichten	
	Beginn der Verarbeitung[3]:	Test (u.a. Datenmigration) ab November 2021, Live-Betrieb ab Ende April 2022 geplant	
	Änderung bestehende Verarbeitung: **Überführung bestehende Verarbeitung in geltende Rechtslage nach DS-GVO:**	☒ ja, Ablöse des alten Hunderegisters (bisher: BACom) ☒ ja	
	Neue Verarbeitung:	☐ ja	
	Abmeldung bestehende Verarbeitung[4]:	☐ ja	
1. Grundsätzliche Angaben zur Verantwortlichkeit			
1.1	Verantwortliche Organisationseinheit[5] (optional):	Zeitlich befristet vor Überführung in den Betrieb: Amt für IT und Digitalisierung (ITD) – Senatskanzlei (SK) – Programm Cupola	

[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

		Parallel dazu (beratend) die fachlich zuständigen Stellen in ihrem nach DSGVO und mitgeltenden Vorschriften geregelten Zuständigkeitsbereichen: **Bezirksamtsleitungen der Bezirksämter** Hamburg-Mitte Altona Eimsbüttel Hamburg-Nord Wandsbek Bergedorf Harburg **vertreten durch die Fachämter Verbraucherschutz, Gewerbe und Umwelt der folgenden Bezirksämter und jeweiligen Abteilungen:** **Bezirksamt Hamburg-Mitte** Abt. Veterinärwesen und Lebensmittelüberwachung Caffamacherreihe 1-3, 20355 Hamburg **Bezirksamt Altona** Abt. Gewerberecht, Marktwesen und Lebensmittelüberwachung Jessenstraße 1-3, 22767 Hamburg **Bezirksamt Eimsbüttel** Abt. Veterinärwesen und Lebensmittelüberwachung Grindelberg 66, 20144 Hamburg **Bezirksamt Nord** Abt. Veterinärwesen und Lebensmittelüberwachung Kümmellstraße 6, 20249 Hamburg **Bezirksamt Wandsbek** Abt. Gewerberecht, Marktwesen und Lebensmittelüberwachung Schloßgarten 9, 22041 Hamburg **Bezirksamt Bergedorf** Abt. Gewerberecht, Marktwesen und Lebensmittelüberwachung Alte Holstenstraße 65-67, 21029 Hamburg **Bezirksamt Harburg** Abt. Lebensmittelüberwachung und Ordnungsangelegenheiten Harburger Rathausplatz 4, 21073 Hamburg	

		und **vertreten durch die Fachämter Einwohnerwesen der Bezirksämter:** **Bezirksamt Hamburg-Mitte** Fachamt Einwohnerwesen Caffamacherreihe 1-3, 20355 Hamburg **Bezirksamt Altona** Fachamt Einwohnerwesen Ottenser Marktplatz 10, 22765 Hamburg **Bezirksamt Eimsbüttel** Fachamt Einwohnerwesen Grindelberg 66, 20144 Hamburg **Bezirksamt Nord** Fachamt Einwohnerwesen Kümmellstraße 7, 20249 Hamburg **Bezirksamt Wandsbek** Fachamt Einwohnerwesen Robert-Schumann-Brücke 8, 22041 Hamburg **Bezirksamt Bergedorf** Fachamt Einwohnerwesen Alte Holstenstraße 65-67, 21029 Hamburg **Bezirksamt Harburg** Fachamt Einwohnerwesen Harburger Rathausforum 3, 21073 Hamburg **<u>Zugriff mit lesenden Rechten:</u>** **Behörde für Inneres und Sport** Johanniswall 4, 20095 Hamburg - Innerhalb der Polizei betrifft dies den Hundekontrolldienst bei der Wasserschutzpolizei und die Polizeivollzugsdienststellen	
1.2	Vertreter der verantwortlichen Organisationseinheit (optional):		
1.3	Fachliche Leitstelle (bei IT-Verfahren) bzw. zuständige Stelle (bei nicht automatisierten Verfahren): Verantwortliche Führungskraft: Leitzeichen:	BA Hamburg-Nord: Fachamt IT-Angelegenheiten der Bezirksverwaltung (N/ITB) Wodke, Christian, ITB3 - IT-Koordination D2 und D4	
1.4	Ansprechpartner, sofern nicht verantwortliche Führungskraft: Telefonnummer:	Zeitlich befristet vor Überführung in den Regelbetrieb: Amt für IT und Digitalisierung (ITD), Senatskanzlei – Programm Cupola, Kleine Rosenstraße 10, 20095 Hamburg, E-Mail: programmcupola@sk.hamburg.de	

1.5	Name des Datenschutzbeauftragten (optional):	Frau Yasmin Heinemann, Datenschutzbeauftragte der Bezirke	
1.6	Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt[6]: Auftragsnummer:	Dataport, Anstalt öffentlichen Rechts, Altenholzer Straße 10-14, 24616 Altenholz	

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung[7]			
2.1	Beschreibung und Zweckbestimmung der Verarbeitung von Daten[8]	Beschreibung der Verarbeitung: Das Hunderegister bietet gemäß § 24 HundeG und § 9 HundeGDVO ein zentrales Register bestehend aus einem automatisiert geführt einheitlichen Bestand von Daten. Die zu erfassenden Daten sind in § 24 HundeG definiert. Das Hunderegister unterstützt die mit dem Vollzug des Hundegesetzes betrauten Personen bei Ihren Tätigkeiten: - Antragsbearbeitung (An- und Änderungsmeldungen) - Erfassung der gemäß HundeG erforderlichen Daten (inkl. Erfassung von Verstößen, Vorfällen und Anordnungen) - Ermittlung von Halterschaften (gem. § 24 HundeG) - Erteilung von Auskünften gem. § 10 HundeGDVO - Automatisierter Abruf personenbezogener Daten gem. § 11 HundeGDVO - Berichterstattung / Statistik gem. § 26 HundeG - Datenübermittlungspflichten (siehe § 24 HundeG) Beschreibung der Zweckbestimmung: Sonstiges: Das Hunderegister dient zur Bearbeitung aller Anliegen rund um die Hundehaltung (u.a. An- und Abmeldung von Hunden, Anträge z.B. auf Leinenbefreiung) gem. des Hamburgischen Gesetzes über das Halten und Führen von Hunden (Hundegesetz vom 26. Januar 2006).	
2.2	Rechtsgrundlage (Zutreffendes bitte ankreuzen und ggf. erläutern):	Hamburgisches Gesetz über das Halten und Führen von Hunden (Hundegesetz - HundeG) und Durchführungsverordnung zum Hundegesetz (HundeGDVO)	
☒	Spezialgesetzliche Regelung außerhalb der DS-GVO	§ 24 Hamburgisches Gesetz über das Halten und Führen von Hunden (Hundegesetz - HundeG)	

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

☐	Einwilligung des Betroffenen (Art. 6 Abs. 1 a DS-GVO):	*Bitte fügen Sie die Einwilligungsklausel und den Einwilligungsmechanismus hier ein*	
☒	Kollektivvereinbarung (z.B. Vereinbarung gem. HmbPersVG, Tarifvertrag)	§ 7 der Vereinbarung nach § 93 HmbPersVG über die im Rahmen des Programms Cupola einzuführenden IT-Verfahren vom 3. August 2021	
☒	Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 4 HmbDSG n.F.)	§ 24 Hamburgisches Gesetz über das Halten und Führen von Hunden (Hundegesetz - HundeG)	
☐	Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§ 10 HmbDSG n.F. und national geregelt im BDSG):		
☐	Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b DS-GVO)		
☐	Interessenabwägung (Art. 6 Abs. 1 f DS-GVO)	*Bitte benennen Sie die vorrangigen Interessen:*	
☐	Weitere:	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz*	
3. Beschreibung betroffener Personen- und Datenkategorien			
3.1	Beschreibung der betroffenen Personengruppen[9]:	Bürger und Beschäftigte Beschreibung: - Hundehalterinnen und -halter (§ 24 HundeG) - Hundeführerinnen und –führer (gem.§ 11 HundeGDVO) - Beschäftigte der Bezirksämter - Bedienstete der Polizei gem. § 11 Hunde GDVO - Sachverständige Personen gem. § 25 HundeG	
3.2	Beschreibung der Art der Daten[10] bzw. Datenkategorien	Identifikations- und Adressdaten und Mitarbeiterdaten Sonstige: - Identifikations-, Adress- und Kontaktdaten von Hundehalterinnen und -haltern - Identifikations-, Adress- und Kontaktdaten von Hundeführerinnen und -führern - Daten der zugehörigen Hunde	

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

		- Erfassung von zuzuordnenden Anträgen (z.B. Erlaubnis, Freistellung), Verstößen, Vorfällen, Anordnungen, Vollstreckungsaufträgen gem. § 24 HundeG - Beschäftigtendaten aus dem Active Directory der FHH: Benutzername, Abteilung, Leitzeichen, Position, Email, Dienststelle, Straße, Ort, Raum, Telefon, Mobil, Fax, eFax - Vor- und Nachnamen der Sachverständigen Personen - Protokollierungsdaten gemäß Protokollierungskonzept (u.a. Vorgaben HundeGDVO § 11 Abs. 4 und § 63 PolDVG Abs. 3). Diese Daten werden nicht zur Verhaltens- und Leistungskontrolle genutzt. Zugriff auf diese Daten ist eingeschränkt und wird nur über das Technische Verfahrensmanagement ermöglicht, sodass nur anlassbezogen und mit Beauftragung durch die fachliche Leitstelle auf die Daten zugegriffen werden kann.	Protokollierungskonzept (siehe Anlage)
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)		
	Art der Daten		
	Zweck der Daten-Mitteilung		
4.3	Externe Empfänger und Dritte	☒ ja ☐ nein	
	Externe Stelle	Behörden, Polizei, Steuerverwaltung, Dataport	
	Art der Daten	Auskünfte und Abrufe gem. § 9, 10 und 11 Hunde GDVO sowie gem. Hundesteuergesetz	
	Zweck der Daten-Mitteilung	- Erfüllung der Aufgaben nach den jeweils geltenden Rechtsvorschriften über das Halten und Führen von Hunden oder nach dem Tierschutzgesetz in der jeweils geltenden Fassung - Erfüllung der Aufgaben im Rahmen der Verfolgung von Straftaten und Ordnungswidrigkeiten	

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

		- Datenübermittlung an Dataport nur im Rahmen der Erstellung von beauftragten Statistiken - Datenübermittlung gem. Hundesteuergesetz	
4.4	Geplante Datenübermittlung in Drittstaaten (außerhalb der EU) bzw. internationale Organisation	☐ ja ☒ nein	
	Drittstaat bzw. internationale Organisation		
	Art der Daten		
	Zweck der Daten Mitteilung		
	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?		
5. Regelfristen für die Löschung der Daten[13]			
	Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Löschungsfristen?	☒ ja, falls ausgewählt bitte benennen: § 12 HundeGDVO ☐ nein	
	Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:	Nach Abmeldung aus dem Hunderegister werden je nach Konstellation die Daten von Hundehalterinnen und -haltern, Hundeführerinnen und -führern, Hunden sowie den dazugehörigen Einträgen automatisiert gelöscht. Bei der seltenen Konstellation eines Hundes mit gemeldeten Verstößen ohne Halter-/Führerschaft, verbleibt dieser im Hunderegister, solange bis dieser verjährt ist und wird dann seitens der Sachbearbeitung manuell gelöscht. Details siehe Entscheidungstabelle Löschung Hund-Person. Die darüber hinaus gesetzlich definierten Lösch- und Tilgungsfristen sind von den verantwortlichen Behörden umzusetzen. Dies geschieht durch die jeweiligen Sachbearbeitungen in den jeweiligen Bezirken. Dazu ist ein „Lösch-Button“ vorhanden.	Entscheidungstabelle (siehe Anlage)

[13] Hinweis Nr. 13 der Anlage 1

		In Bezug auf die Beschäftigtendaten in den Anmeldeprotokollen: Die Protokollierungen der letzten Anmeldungen von Benutzerinnen und Benutzern am System werden in einer Frist von 24 Stunden vorgehalten und anschließend gelöscht. In Bezug auf die im System hinterlegten Daten von Benutzerinnen und Benutzern nach dem Ausscheiden aus ihrer Funktion: Die Zugänge für Anwenderinnen und Anwender wird über die Admin-Funktion gesteuert. Ausgeschiedene Nutzerinnen und Nutzer müssen ausgetragen werden. Im Fall der Austragung erfolgt eine sofortige Löschung der Daten von Benutzerinnen und Benutzern.	
6. Mittel der Verarbeitung (optional) **Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?[14]**			
	Bezeichnung: Hersteller: Funktionsbeschreibung: Bereitstellung:	Hunderegister Dataport Registerführung ☒ Eigenentwickelte/ individuelle Software ☐ Standard-Software ☐ Cloud-Services ☐ Sonstige:	
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 Rechte- und Rollenkonzept	Rechte- und Rollenkonzept (siehe Anlage)
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 Standardverfahren → RaSiKo wird eingehalten ☐ nein	
8.2	Die allgemeine Zielsetzung aus dem Rahmensicherheitskonzept wurde sichergestellt.	☒ ja ☐ nein, Abweichungen erläutern:	
8.3	Werden bei der Verarbeitung die Grundsätze des Datenschutzes durch Technikgestaltung (privacy by design) gem. Art 25 Abs. 1 DS-GVO und der datenschutzfreundlichen Voreinstellungen (privacy by	☒ ja (Dokument mit Vertraulichkeitsstufe liegt vor, kann bei Bedarf über den Produktverantwortlichen bei Dataport angefordert und eingesehen werden.)	

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

	default) gem. Art 25 Abs. 2 DS-GVO eingehalten?[17]	☐ nein, Begründung:	
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. Schutzbedarfsfeststellung mit Vertraulichkeitsstufe liegt vor, kann bei Bedarf über den Produktverantwortlichen bei Dataport angefordert und eingesehen werden.)	
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 Dokument wird zur Abstimmung separat per Mail eingereicht	Schwellwertanalyse (siehe Anlage)
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 <u>nicht</u> bei Dataport gehostet werden: Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMs laut Anlage 2 sichergestellt.	☐ Es liegt kein Verfahren vor, das bei Dataport gehostet wird. ☐ Die Anlage 2 wurde ausgefüllt und liegt vor.	
8.8	Es liegen schriftlich vor	☐ interne Verhaltensregeln ☐ DSFA ☒ Risikoprüfung/ Schutzbedarfsfeststellung ☐ allg. Datensicherheitsbeschreibung ☐ umfassendes Datensicherheitskonzept ☐ Wiederanlauf- bzw. Notfallkonzept ☒ Sonstiges: Siehe allgemeine RZ²Standards von Dataport/ Betriebskonzept	
9. Datenübertragbarkeit[18] (Datenportabilität)			
	Nur bei - auf Grundlage einer Einwilligung- zur Verfügung gestellten Daten:	☐ ja, Format: ☒ nein, Begründung:	

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

	Ist der Export der verarbeiteten Daten an den Betroffenen oder andere Dienste in einem gängigen, standardisierten Format möglich?		
10. Informationen der Betroffenen[19]			
	Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?	Datenschutzerklärung und allgemeines Informationsblatt Art 12 bis 14 DS-GVO im Online Dienst Hunderegister eingebunden	
11. Sonstiges			
	Anmerkungen:		

[19] Hinweis Nr. 19 der Anlage 1

.

Anlage 1**:**

Hinweise zum Formular

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

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

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

.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

.

.

Anlage 2

Übersicht und Erläuterungen zu den technischen und organisatorischen Maßnahmen

Fehler! Keine gültige Verknüpfung.

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.

<u>Hinweis:</u> 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).

<u>Maßnahmen zur Pseudonymisierung personenbezogener Daten</u>

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

Hamburg

.

Beschreibung der Verarbeitungstätigkeit

Blatt-Nr.:

Von der Verzeichnisführenden Stelle auszufüllen!

(Bitte an die Verzeichnisführende Stelle absenden!)

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

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

Allgemeines			
	Datum:	07.11.2022	
	Ausfüllende Person:	Max Stange/ Jan Aita-Schmitz	
	Telefonnummer:	+49 176 42857054	
	Bezeichnung des Verfahrens:	Oktagon	
	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 Verknüpfen ☒ Einschränken ☒ Löschen ☒ Vernichten	
	Beginn der Verarbeitung[3]:	Pilotbetrieb ab April 2022. Beginn des Regelbetriebs ab Januar 2023.	
	Änderung bestehende Verarbeitung: **Überführung bestehende Verarbeitung in geltende Rechtslage nach DS-GVO:**	☐ ja ☐ ja	
	Neue Verarbeitung:	☒ ja	
	Abmeldung bestehende Verarbeitung[4]:	☐ ja	
1. Grundsätzliche Angaben zur Verantwortlichkeit			
1.1	Verantwortliche Organisationseinheit[5] (optional):	**Zeitlich befristet im Rahmen der Pilotierung oder bis zur Einrichtung einer Koordinierungsstelle:** • Amt für IT und Digitalisierung (ITD) – Senatskanzlei (SK) – Programm Cupola	

[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

		Parallel dazu (beratend) die fachlich zuständigen Stellen in ihrem nach DS-GVO und mitgeltenden Vorschiften geregelten Zuständigkeitsbereichen: • Behörde für Stadtentwicklung und Wohnen (BSW) • Bezirksämter Hamburg-Mitte, Altona, Eimsbüttel, Hamburg-Nord, Wandsbek, Bergedorf, Harburg • Hamburg Port Authority (HPA) **Nach Überführung in den Betrieb:** • Koordinierungsstelle, Behörde für Stadtentwicklung und Wohnen (BSW) • Bezirksämter Hamburg-Mitte, Altona, Eimsbüttel, Hamburg-Nord, Wandsbek, Bergedorf, Harburg • Hamburg Port Authority (HPA) Im Einzelnen sind dies: **Amt für IT und Digitalisierung (ITD)** **Senatskanzlei (SK) – Programm Cupola** Kleine Rosenstraße 10 20095 Hamburg **Bezirksamt Hamburg-Mitte** Dezernat Wirtschaft, Bauen und Umwelt Fachamt Bauprüfung Caffamacherreihe 1-3, 20355 Hamburg **Bezirksamt Altona** Zentrum für Wirtschaftsförderung, Bauen und Umwelt Fachamt Bauprüfung Platz der Republik 1, 22765 Hamburg **Bezirksamt Eimsbüttel** Zentrum für Wirtschaftsförderung, Bauen und Umwelt Fachamt Bauprüfung Grindelberg 66, 20144 Hamburg **Bezirksamt Hamburg-Nord** Zentrum für Wirtschaftsförderung, Bauen und Umwelt Fachamt Bauprüfung Kümmellstraße 6, 20249 Hamburg **Bezirksamt Wandsbek** Zentrum für Wirtschaftsförderung, Bauen und Umwelt Fachamt Bauprüfung Wandsbeker Allee 62, 22041 Hamburg **Bezirksamt Bergedorf** Zentrum für Wirtschaftsförderung, Bauen und Umwelt	

		Fachamt Bauprüfung Wentorfer Str. 38, 21029 Hamburg **Bezirksamt Harburg** Zentrum für Wirtschaftsförderung, Bauen und Umwelt Fachamt Bauprüfung Harburger Rathausforum 1, 21073 Hamburg **Hamburg Port Authority AöR (HPA)** Bauprüfabteilung Hafen Neuer Wandrahm 4 20457 Hamburg Zuständig im Hafennutzungsgebiet. **Behörde für Stadtentwicklung und Wohnen (BSW)** Amt für Bauordnung und Hochbau - ABH 23 Referat Baugenehmigungen Neuenfelder Straße 19 21109 Hamburg	
1.2	Vertreter der verantwortlichen Organisationseinheit (optional):		
1.3	Fachliche Leitstelle (bei IT-Verfahren) bzw. zuständige Stelle (bei nicht automatisierten Verfahren): Verantwortliche Führungskraft: Leitzeichen:	Koordinierungsstelle Oktagon bei der Behörde für Stadtentwicklung und Wohnen (BSW) Neuenfelder Straße 19, 21109 Hamburg	
1.4	Ansprechpartner, sofern nicht verantwortliche Führungskraft: Telefonnummer:		
1.5	Name des Datenschutzbeauftragten (optional):	Die verantwortlichen Datenschutzbeauftragten der Bezirksämter, BSW und HPA	
1.6	Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt[6]: Auftragsnummer:	• Dataport, Anstalt öffentlichen Rechts, Altenholzer Straße 10-14, 24616 Altenholz • Rhenus Docs to Data GmbH, Röntgenstraße 10, 21493 Schwarzenbek	

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung[7]			
2.1	Beschreibung und Zweckbestimmung der Verarbeitung von Daten[8]	Beschreibung der Verarbeitung: Oktagon unterstützt zurzeit die Aufgaben der beteiligten Nutzungspartner in den Fachthemen Bau und Baunebenrecht, Sondernutzungsverfahren, Verfahren nach § 127 I und IV TKG sowie Aufgrabungen nach HWG. Beschreibung der Zweckbestimmung: Antragsbearbeitung (Antrags-, Genehmigungs- und Überwachungsverfahren sowie Beteiligungen) Beschreibung:	

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

		• Bearbeitung gestellter Anträge entsprechend den o.g. Fachthemen • Berechnung anfallender Aufwände wie Gebühren • Kommunikation mit Antragsteller:innen und anderen Verfahrensbeteiligten • Einholung von Stellungnahmen, Gutachten • Übermittlung von Daten an beteiligte Stellen, siehe § 29 BauVorlVO, (Bau), § 13 (2) HmbVwVfG (SWAN) z.B. an die Feuerwehr für ein Brandschutzgutachten. • Recherche von Altfällen anhand des Vornamens und Nachnamens der im Verfahren beteiligten Personen • Steuerung der Verfahren in Form eines Berichtswesens bzw. Bereitstellung . • Revisionssichere Dokumentation aller Bearbeitungsschritte • • Gewährleistung eines rechtskonformen und sicheren Betriebes des IT-Verfahrens	
2.2	Rechtsgrundlage (Zutreffendes bitte ankreuzen und ggf. erläutern):		
☒	Spezialgesetzliche Regelung außerhalb der DS-GVO	§ 28 und §29 BauVorlVO, §13 HmbVwVfG	
☐	Einwilligung des Betroffenen (Art. 6 Abs. 1 a DS-GVO):		
☒	Kollektivvereinbarung nach Vorgaben des HmbBG, § 85 und des HmbDSG, § 10 (z.B. Vereinbarung gem. HmbPersVG, Tarifvertrag)	Vereinbarung nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG) über die im Rahmen des Programms Cupola einzuführenden IT-Verfahren vom 3. August 2021	
☒	Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 4 HmbDSG n.F.)	*Ist gegeben*	
☐	Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§ 10 HmbDSG n.F. und national geregelt im BDSG):		
☐	Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b DS-GVO)		
☐	Interessenabwägung (Art. 6 Abs. 1 f DS-GVO)	*Bitte benennen Sie die vorrangigen Interessen:*	
☐	Weitere:	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz*	
3. Beschreibung betroffener Personen- und Datenkategorien			

3.1	Beschreibung der betroffenen Personengruppen[9]:	Beschäftigte (Verwaltungsangehörige), die die Verfahren bearbeiten bzw. an der Bearbeitung beteiligt sind. Dazu zählen neben den Antragsbearbeitenden ebenfalls: • Brandschau-Dienststelle nach FeuerwG § 6 • Planfeststellungsbehörde nach HWaG, SchfHwG § 8 (B) • VertreterIn von Amts wegen nach HmbVwVfG § 16 • Vollstreckungsbehörde nach § 4 HmbVwVG Externe Verfahrensbeteiligte: • AnliegerIn nach § 3 HWG • Antragsteller*in nach HmbVwVfG • Antragsteller*in nach WEG • Baufirma (bit.) nach HWG § 22 • Baufirma (Leitung) nach HWG § 22 • Bauherr*in nach § 54 HBauO • Baulastgeber*in nach § 79 HBauO • Betreiber*in nach § 15 PVO • Beistand nach HmbVwVfG § 14 • BeteiligteR nach HmbVwVfG § 13 • Betreiber einer Anlage nach AwSV, PolderO • BetreiberIn Störfallbetriebe § 5 BImSchG • BetroffeneR nach § 3 ÖffbetVO • BetroffeneR nach GewO • BetroffeneR nach OWiG • Bevollmächtigte/r BezirksschornsteinfegerIn, nach GewO • BevollmächtigteR nach HmbVwVfG § 14 • Dritte nach § 10 SOG • Eigentümer nach HWaG, SchfHwG § 1 • Eigentümer von Feuerungsanlagen § 1 SchfHwG, OWiG • EmpfangsbevollmächtigteR nach HmbVwVfG § 15 • Entwurfsverfasser*in nach §55 HBauO • Fachbetrieb nach § 62 AwSV, HmbVwVfG § 13 • Fachplaner*in nach §55 HBauO • Firma i.V.m. Ersatzvornahme nach HmbVwVG • Gebührenschuldner*in nach der Baugebührenordnung • GebührenpflichtigeR nach § 9 GebG • Genehmigungsbehörde nach BImSchG • Genehmigungsinhaber nach § 19 HWaG • GrundeigentümerIn/ErbbauberechtigteR nach BGB • HochwasserschutzbeauftragteR nach § 23 PolderO • InsolvenzverwalterIn nach § 27 InsO • MieterIn nach BGB • Nachbar*in nach § 71 HBauO • Pflichtige*r nach §9 HmbVwVfG	

[9] Hinweis Nr. 9 der Anlage 1

		• Polder-EinsatzleiterIn nach § 28 PolderO • Poldergemeinschaft nach PolderO • Poldergesellschaft nach PolderO • PrüfingenieurIn nach PVO • PrüfsachverständigeR für Erd-u.Grundbau nach PVO • PrüfsachverständigeR für techn. Anlagen u. Einrichtungen • Rechtsvertreter d. Widersprechenden nach VwGO nach PVO • SachverständigeR nach § 26 HmbVwVfG • SachverständigeR nach § 5 UVPG • SachverständigeR nach § 53 AwSV • SchuldnerIn nach nach § 17 InsO • Schuldner*in nach §17 ZVG • Schornsteinfeger*in nach SchfHwG • Verantwortliche Person nach §9 SOG • Verfasser*in bautechnischer Nachweise nach §55 HBauO • VeranlasserIn nach HWG § 22 • Verantwortliche Person nach § 9 SOG • Verhaltensstörer nach § 8 SOG • VerteidigerIn nach StPO § 137 • VertreterIn nach HmbVwVfG § 17 • Widersprechende*r nach VwGO • WidersprechendeR nach VwGO • Zeugin/Zeuge nach HmbVwVfG § 26 • Zuständiges Amtsgericht nach § 4 HmbAGGVG (B) • Zwangsverwalter nach § 1 ZwVwV	
3.2	Beschreibung der Art der Daten[10] bzw. Datenkategorien	Identifikations- und Adressdaten Sonstige: Beschreibung: **Daten von Verfahrensbeteiligten** (Externe): • Vor- und Nachname • Anschrift • Telefon • Mailadresse Im Verfahren Kehrgebühren/Beitreibung“: • Kontodaten des Schornsteinfegers/der Schornsteinfegerin **<u>Beschäftigtendaten</u>** (Verwaltungsangehörige): • Benutzername, User-Kennung aus dem AD der FHH • Vor- und Nachname • Dienstliche Anschrift • Dienstliche Telefonnummer • Dienstliche Mailadresse Letztere werden verwendet und ergänzt	

[10] Hinweis Nr. 10 der Anlage 1

		• zur Gewährleistung der IT-Sicherheit zur Anmeldung am System: Benutzer*innenname aus dem AD in Verbindung mit Datum sowie Uhrzeit der letzten Anmeldung am System • zur Steuerung der Vorgänge: Datensatz zum Vorgang; dabei Namen des Bearbeitenden und Status der Aufgabe • für die revisionssichere Dokumentation der Bearbeitung: ○ Datensatz zum Vorgang; dabei Namen des Bearbeitenden, Status der Aufgabe und Datum (bei Status erledigt) ○ Dokumente bzw. eAkte eines Vorgangs mit Namen des Bearbeitenden bzw. Benutzer*innenname aus dem AD, Datum, Uhrzeit (bei Check-In, Check-Out, Anlage, Änderung, Ungültigkeitserklärung, Löschung) • für die Kommunikation mit Verfahrensbeteiligten: ○ Name, dienstliche Anschrift, dienstliche Telefonnummer, dienstliche Mailadresse	
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)	Siehe die in § 29 BauVorlVO benannten Stellen bzw. Beteiligte in HmbVwVfG.	
	Art der Daten	Siehe 3.2: Die Daten der Verfahrensbeteiligten sowie die Daten der Beschäftigten zur Kommunikation mit den Verfahrensbeteiligten	
	Zweck der Daten-Mitteilung	Siehe § 28 Abs. 1 + 2,§29 BauVorlVO bzw. Beteiligte in HmbVwVfG	
4.3	Externe Empfänger und Dritte	☒ ja ☐ nein	
	Externe Stelle	Siehe die in § 29 BauVorlVO benannten Stellen. + Daten an die Baustatistik gem. § 81 Abs. 9 HBauO + Daten für die Steuerungsfunktionen + Berichtswesen (Datawarehouse) an das Statistikamt Nord +Daten an die Kasse. Hamburg zur Zahlungsanweisung	
	Art der Daten	Siehe 3.2: Die Daten der Verfahrensbeteiligten sowie die Daten der Beschäftigten zur Kommunikation mit den Verfahrensbeteiligten	
	Zweck der Daten-Mitteilung	Siehe § 28 Abs. 1 + 2, § 29,BauVorlVO Baugenehmigungsstatistik des Bundes bzw. Beteiligte in HmbVwVfG.	

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

4.4	Geplante Datenübermittlung in Drittstaaten (außerhalb der EU) bzw. internationale Organisation	☐ ja ☒ nein	
	Drittstaat bzw. internationale Organisation		
	Art der Daten		
	Zweck der Daten Mitteilung		
	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?		
5. Regelfristen für die Löschung der Daten[13]			
	Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Löschungsfristen?	☒ ja, falls ausgewählt bitte benennen: § 30 BauVorlVO sowie die generellen Aufbewahrungsvorschriften nach Archivgesetz / die allgemeinen Aktenordnungen der Dienststellen ☐ nein	
	Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:	○ In Bezug auf die mit der Vorgangs- und Aktenverwaltung genutzten Daten: Die Verwahrungsfrist bestimmt, wie lange Unterlagen von den Stellen, die die Bauaufsichtsakten führen, selbst zu verwahren sind und wann die Verpflichtung zur Ablieferung an das Staatsarchiv entsteht. Die Aufbewahrungsfrist bestimmt, wie lange die Unterlagen zur Wahrnehmung berechtigter Belange von Bürgerinnen und Bürgern oder zur Bereitstellung von Informationen für Gesetzgebung, Verwaltung und Rechtspflege aufbewahrt werden müssen. Die Aufbewahrungsfrist für die nicht archivwürdigen Unterlagen wird in den Stellen, die die Bauaufsichtsakten führen, erfüllt. Die Aufbewahrungsfrist für die archivwürdigen Unterlagen wird im Staatsarchiv erfüllt. Ein Vorgang wird mit der Verfügung „z.d.A." abgeschlossen, wenn die Genehmigung erteilt oder versagt wurde, ein Gebührenbescheid erteilt und ein Abschlussdatum gesetzt wurde. Die Aufbewahrungsfrist und die Verwahrungsfrist beginnen an dem Tag, welcher dem Abschlussdatum folgt, da beide Fristen von dem jüngsten Dokument des Vorgangs abhängig sind. Die Verwahrungsfrist beträgt 50 Jahre, die Aufbewahrungsfrist beträgt 100 Jahre. Die Bauaufsichtsakten führende Stelle kann die Aufbewahrungsfrist verlängern werden, wenn ein Gebäude nach Ablauf der 100 Jahre noch steht.	

[13] Hinweis Nr. 13 der Anlage 1

		Eine Ausnahme bilden Daten aus Widerspruchsvorgängen. Diese werden 5 Jahre gespeichert. Mit der Z.d.A- Setzung erfolgt eine Kopie der Vorgangsdokumente in Eldorado. Vereinbarungen mit dem Staatsarchiv bezgl. Aufbewahrungsfrist ist über Eldorado geregelt. ○ In Bezug auf die Beschäftigtendaten in den Anmeldeprotokollen für das Incident- und Problemmanagement: Die Protokollierungen der letzten Anmeldungen von Benutzer*innen am System werden in einer Frist von drei Monaten vorgehalten und anschließend gelöscht. ○ In Bezug auf die im System hinterlegten Benutzer*innendaten nach dem Ausscheiden aus ihrer Funktion: Es gelten die für die revisionssichere Vorgangs- und Aktenverwaltung geltenden Verwahrungs- und Aufbewahrungsfristen (s.o.).	
6. Mittel der Verarbeitung (optional) **Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?[14]**			
	Bezeichnung: Hersteller: Funktionsbeschreibung: Bereitstellung:	• G2vb²Plus, ots, Vorgangsbearbeitung (customized)/ eAktePlus (eAkte), ots, digitale Akte (customized)/ Posteingangsscannen, Kofax Express/ PDF Exchange Pro, Tracker Software, Dokumentenverarbeitung/ Office, Microsoft, Dokumentenbearbeitung • ots informationstechnologie ag, Kofax Limited, Tracker Software, Microsoft ☐ Eigenentwickelte/ individuelle Software ☒ Standard-Software mit für die Freie und Hansestadt Hamburg programmierten Modulen (Beteiligung) ☐ Cloud-Services ☐ Sonstige:	
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 Prozess ist ausführlich im Berechtigungskonzept dargestellt.	
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:	

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

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:	
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.	
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	
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 <u>nicht</u> bei Dataport gehostet werden: Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMs laut Anlage 2 sichergestellt.	☐ Es liegt kein Verfahren vor, das bei Dataport gehostet wird. Im Rahmen des Posteingangsscannens werden für vertraglich vereinbarte Fälle und Dokumentenformate die Digitalisate im Rechenzentrum von Rhenus gespeichert und über einen verschlüsselten Kanal in das Fachverfahren übertragen. Eine Datenschutzkonforme Verarbeitung nach EU Standards wird gemäß Betriebsvertrag gewährleistet. ☐ Die Anlage 2 wurde ausgefüllt und liegt vor.	
8.8	Es liegen schriftlich vor	☒ interne Verhaltensregeln ☐ DSFA ☒ Risikoprüfung/ Schutzbedarfsfeststellung ☒ allg. Datensicherheitsbeschreibung ☒ umfassendes Datensicherheitskonzept	

[17] Hinweis Nr. 17 der Anlage 1

		☒ Wiederanlauf- bzw. Notfallkonzept ☐ Sonstiges: Siehe allgemeine RZ²Standards von Dataport/ Betriebskonzept	
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: Csv-Dateien ☐ nein, Begründung:	
10. Informationen der Betroffenen[19]			
	Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?	Datenschutzerklärung und allgemeines Informationsblatt Art 12 bis 14 DS-GVO	
11. Sonstiges			
	Anmerkungen:		

30.05.2023

……..	……..	……
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. Die Verarbeitung der personenbezogenen Daten muss im IT-Verfahren der Hauptzweck sein.

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

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

.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Anlage 2:

Übersicht und Erläuterungen zu den technischen und organisatorischen Maßnahmen

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.

<u>Hinweis:</u> 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).

<u>Maßnahmen zur Pseudonymisierung personenbezogener Daten</u>

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

<u>Maßnahmen zur Verschlüsselung personenbezogener Daten</u>
(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

<u>Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste</u>

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.

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

- 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

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

- 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

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

- 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 2a
zur Vereinbarung nach §93 HmbPersVG über die im Rahmen des Programms Cupola einzuführenden IT-Verfahren

Beschreibung von Zweck und Ziel des Fachverfahrens Oktagon SWAN

Im Zuge der Ablösung des Altverfahrens BACom wurde in einem ersten Schritt das Fachverfahren Oktagon in den bauprüfenden Dienststellen eingeführt. Aufbauend auf die bestehende Struktur, z.B. die integrierten Schnittstellen zu verschiedenen IT-Anwendungen (u.a. zu SAP, Eldorado) sowie zu Online-Diensten im Service-Portal der FHH wird im Projekt Oktagon SWAN die digitalisierte Vorgangsbearbeitung (g2vb+) sowie anhand der eAkte die elektronische Aktenverwaltung (DMS3) in den Arbeitsbereichen Sondernutzung, Aufgrabeschein und Trasse eingeführt. Darüber hinaus werden in diesem Zuge, die Beteiligungen am baurechtlichen Verfahren, die bis Dato im Altverfahren BACom bearbeitet wurden, ebenfalls in Oktagon integriert. Die Umsetzung umfasste zunächst gemäß Einsetzungsbeschluss der Lenkungsgruppe vom 19.09.2022 folgende Verfahren der Aufgabengebiete Sondernutzung, Aufgrabungen und Trassenanweisungen sowie Naturschutz und Wasserrecht:

Fachbereich	Verfahren	Ausprägung
TAGS	Aufgrabescheine gem. §22 HWG + Trassenanweisungen gem. HWG	Detail
Sondernutzungen	Sondernutzungsverfahren nach HWG	Detail
Naturschutz	Ausnahmegenehmigunng nach §6 der BaumschutzVO	Detail
Beteiligungen	Beteiligung der zuständigen Stelle am bauaufsichtlichen Verfahren	Basis
Beteiligungen	Beteiligung der sachverständigen Stelle am bauaufsichtlichen Verfahren	Basis
Sondernutzungen	Unerlaubte Sondernutzung nach HWG	Basis
Sondernutzungen	Benutzungserlaubnis nach §4 GrünAnlG	Basis
Naturschutz	Ausnahmegenehmigung nach LSG-Verordnung	Basis
Wasserrecht	Genehmigungsverfahren nach §15 HWaG	Basis
Wasserrecht	Wasserbehördliche Überwachung nach §100 WHG	Basis
Beteiligungen	Beteiligung der Naturschutzbehörde	Basis
Beteiligungen	Beteiligung der Wegeaufsichtsbehörde	Basis

Mit der Entscheidung der Staatsräte von BUKEA, SK und BWFGB vom 28. Februar 2024 sowie der 36. Lenkungsgruppe vom 15. April 2024 wurden die Verfahren zum Naturschutz und Wasserrecht aus dem Projektumfang gestrichen.

Damit werden nur noch die folgenden Verfahren im Aufgabenbereich Sondernutzung, Aufgrabungen und Trassenanweisungen umgesetzt:

Fachbereich	Verfahren	Ausprägung
TAGS	Antragsverfahren nach §127 Abs. 1 TKG	Detail
TAGS	Geringfügige Maßnahmen nach § 127 Abs. 4 TKG	Detail
TAGS	Aufgrabung mit Leitungs-verlegung nach HWG	Detail
TAGS	Aufgrabung ohne Lei-tungsverlegung nach HWG	Detail
TAGS	Aufgrabung geringeren Umfangs nach HWG	Detail
Sondernutzungen	Sondernutzungsverfahren nach HWG	Detail
Sondernutzungen	Unerlaubte Sondernutzung nach HWG	Basis
Sondernutzungen	Benutzungserlaubnis nach §4 GrünAnlG	Basis
Beteiligungen	Beteiligung der zuständigen Stelle am bauaufsichtlichen Verfahren	Basis
Beteiligungen	Beteiligung der sachverständigen Stelle am bauaufsichtlichen Verfahren	Basis
Beteiligungen	Beteiligung der Wegeaufsichtsbehörde	Basis

Ziel ist es, die Qualität der Arbeitsprozesse für alle Beteiligten nach der Abschaltung des Altverfahrens zu gewährleisten und perspektivisch zu verbessern, indem die Beschäftigten bei der effektiven und effizienten Aufgabenerledigung durch digitalisierte, nutzerfreundliche sowie zukunftssichere IT-Verfahren unterstützt werden. Oktagon SWAN bietet die Grundlage, um einen digitalisierten Arbeitsprozess in den Arbeitsbereichen zu ermöglichen, Medienbrüche in den baunahen Arbeitsfeldern tendenziell zu reduzieren und die Arbeitsbereiche in Hinblick auf zukünftige Anforderungen an die digitale Bearbeitung weiterzuentwickeln.

Maßnahmenplan zur Erreichung der digitalen Barrierefreiheit

im Hinblick auf die monierten Punkte aus den Prüfberichten zur Barrierefreiheit

Erklärung und Hintergrund

Oktagon besteht unter anderem aus den Bestandteilen g2vb+ und DMS3. G2vb+ wird für die Vorgangserfassung und -bearbeitung benötigt, DMS3 ist die sogenannte „eAkte“. OTS hat diese beiden Bestandteile durch das Pfenningparade Gutachten praxisnah untersuchen lassen und die Umsetzbarkeit bewertet. Mit einer neuen technischen Basis („Flowversion“) können viele der Mängel einfach und schnell beseitigt werden.

Status

- Ein Großteil der „**einfach**“ zu lösenden Mängel wurden in den **Flowversionen** bereits beseitigt (bzw. werden dies noch für g2vb+)
    - Die DMS3 Flowversion ist bereits geliefert, erste Mängel behoben
    - Die g2vb+ Flowversion ist ebenfalls bereits geliefert. Weitere Mängel wurden beseitigt.
    - Aufstellung
- Die verbleibenden Mängel werden in dem **Hilfesystem Barrierefreiheit** behandelt, damit zumindest eine Hilfe vorhanden ist, wenn es keine passende technische Lösung gibt.
- Einige Mängel werden durch Konfigurationsmöglichkeiten gelöst, die sowohl die individuellen Einstellungen wie auch eine Lösung für unterschiedliche Belange bringen (z.B. Kontrastanpassungen, Hervorhebung Pflichtfelder, etc.).
- Damit zukünftig die Mängel nicht wieder auftreten, wurden **Entwickler Guidelines** erstellt, die von der OTS QM **auf Einhaltung überprüft** werden. Als Basis für die Anwendungensentwicklung bei den Flowversionen von OTS wird der Vaadin-Standard[1] verwendet.

[1] Vaadin ist eine Plattform für die Entwicklung von Webanwendungen, die besonders auf die Benutzerfreundlichkeit und Zugänglichkeit Wert legt. Die Barrierefreiheit bei Vaadin umfasst verschiedene Aspekte wie Tastaturnavigation, Screen-Reader-Unterstützung und visuelle Anpassungen, die das Lesen erleichtern. Vaadin unterstützt die Einhaltung international anerkannter Richtlinien für Barrierefreiheit, wie die Web Content Accessibility Guidelines (WCAG 2.1 Level AA), die sicherstellen, dass Webinhalte für Menschen mit verschiedensten Behinderungen zugänglich sind. Vaadin fördert die Entwicklung von UI-Komponenten, die von Grund auf zugänglich sind. Das bedeutet, dass Entwickler, die Vaadin verwenden, darauf vertrauen können, dass die Standardkomponenten der Plattform bereits so gestaltet sind, dass sie den Barrierefreiheitsrichtlinien entsprechen.

Mängel und Bewertung Status Barrierefreiheit nach Prüfpunkten

#	Prüfpunkt	Umsetzungsschritt/Lösung	Bis wann	Wer
	g2vb / g2vb+ = Vorgangserfassung und -bearbeitung			
1	g2vb: Überschriften sind nur teilweise verfügbar und werden nicht hierarchisch verwendet	Handbuch	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
2	g2vb: Kontrastanpassungen erforderlich (Mindestkontrast nicht eingehalten)	erledigt	g2vb+ 2024.2 Flow	OTS
3	g2vb: Skalierungsprobleme	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
4	g2vb: Inhalte brechen nicht um	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
5	g2vb: Englische als Hauptsprache angegeben	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
6	g2vb: Fehlende Erläuterung der visuellen Hervorhebung von Pflichtfeldern	erledigt	g2vb+ 2024.2 Flow	OTS
7	g2vb: Hinweis Name, Rolle, Wert	Handbuch	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
8	g2vb: Fehlermeldung nicht zugeordnet	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
9	g2vb: Menüs als Tabelle umgesetzt	Handbuch	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
10	g2vb: Tooltips sind nur bei Mausbedienung verfügbar	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
11	g2vb: Fokusverlust zwischen dem ersten und zweiten Return	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
12	g2vb: Eingabeformate sind nicht ersichtlich	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
13	g2vb: Fehlende Labels	Handbuch	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
14	g2vb: Fehlerhaft ausgefüllte Eingabefelder nicht benannt	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS

15	g2vb: Textalternativen für Bedienfeld	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
16	g2vb: Nach Eingabe wird die Bedienung erschwert	Handbuch	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
17	g2vb: Nach Eingabe ist der Fokus nicht sichtbar Z.B. Dokumentbeschreibung wird vorgelesen	Handbuch	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
18	g2vb: Sichtbare Beschriftung unterscheidet sich von zugänglichem Namen	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
19	g2vb: Fehlermeldungen in Textform nicht identifizierbar	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
20	g2vb: Zustand wird nicht ausgegeben (Spaltenauswahl, Menüeinträge)	Handbuch	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
21	g2vb: Beim Setzen der Favoriten kommt es beim waagrechten Scrollen zu abgeschnittenen Texten	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
22	g2vb: Schreibgeschützte Eingabefelder sind beschriftet aber kaum sichtbar	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
23	g2vb: Beschriftung des Kalenders auf Englisch	erledigt	g2vb+ 2024.1 Flow (1. HJ 2024)	OTS
	DMS3 / eAkte			
24	DMS3: Überschriften sind nur teilweise verfügbar und werden nicht hierarchisch verwendet	Handbuch	DMS3 2024.1	OTS
25	DMS3: Kontrastanpassungen erforderlich (Mindestkontrast nicht eingehalten)	in Bearbeitung (Konfig)	DMS3 2025.1	OTS
26	DMS3: Skalierungsprobleme	erledigt	DMS3 2024.1	OTS
27	DMS3: Inhalte brechen nicht um	erledigt	DMS3 2024.2	OTS
28	DMS3: Englische als Hauptsprache angegeben	erledigt	DMS3 2024.2	OTS
29	DMS3: Fehlende Erläuterung der visuellen Hervorhebung von Pflichtfeldern	in Bearbeitung (Konfig)	DMS3 2025.1	OTS
30	DMS3: Hinweis Name, Rolle, Wert	Handbuch	DMS3 2024.2	OTS

31	DMS3: Fehlermeldung nicht zugeordnet Zurodnun erfolgt	erledigt	DMS3 2024.2	OTS
32	DMS3: Menüs als Tabelle umgesetzt	Handbuch	DMS3 2024.2	OTS
33	DMS3: Tooltips sind nur bei Mausbedienung verfügbar	erledigt	DMS3 2024.2	OTS
34	DMS3: Fokusverlust zwischen dem ersten und zweiten Return	erledigt	DMS3 2024.2	OTS
35	DMS3: Eingabeformate sind nicht ersichtlich	erledigt	DMS3 2024.2	OTS
36	DMS3: Fehlende Labels	Handbuch	DMS3 2024.2	OTS
37	DMS3: Fehlerhaft ausgefüllte Eingabefelder nicht benannt	erledigt	DMS3 2024.2	OTS
38	DMS3: Textalternativen für Bedienfeld	erledigt	DMS3 2024.2	OTS
39	DMS3: Nach Eingabe wird die Bedienung erschwert	Handbuch	DMS3 2024.2	OTS
40	DMS3: Nach Eingabe ist der Fokus nicht sichtbar	Handbuch	DMS3 2024.2	OTS
41	DMS3: Sichtbare Beschriftung unterscheidet sich von zugänglichem Namen	erledigt	DMS3 2024.2	OTS
42	DMS3: Fehlermeldungen in Textform nicht identifizierbar	erledigt	DMS3 2024.2	OTS
43	DMS3: Zustand wird nicht ausgegeben (Spaltenauswahl, Menüeinträge)	Handbuch	DMS3 2024.2	OTS

Anmerkung: Die Angabe „Handbuch“ bezieht sich auf das Dokument „Erklärung zur Barrierefreiheit der Software“. Das Handbuch beschreibt in screenreadertauglicher Form die Lücken der Barrierefreiheit, so dass Anwenderinnen und Anwender mit Beeinträchtigungen der Sehfähigkeit Probleme erkennen und etwaige individuelle Unterstützungsbedarfe einschätzen können.

Die Einspielung im Testsystem ist bereits erfolgt. Die ordnungsgemäße Umsetzung der Punkte wird unter Beteiligung von ITD (Projekt digit. Barrierefreiheit) geprüft. Die Einspielung in die Produktivsysteme ist für Release 4.1 geplant, bei erheblichen Mängeln für das Folgerelease.

I. Ziel der Anlage

Durch die digitale Verarbeitung der bau- und wegerechtlichen Verwaltungsvorgänge in Oktagon wird eine Datenbasis bereitgestellt. Von Seiten der Dienststelle besteht das Interesse, dass diese Datenbasis genutzt wird, um Vorhaben im Sinne der FHH zu unterstützen und den Informationsbedarf insbesondere politischer Gremien zu decken. Gleichzeitig besteht der Auftrag den rechtlichen Vereinbarungen im Sinne der Mitbestimmung gerecht zu werden. Diese Anlage bietet die Regelungen hierzu bezogen auf das Fachverfahren Oktagon.

II. Ausgangslage

Die KST (BSW) ist als Koordinierungsstelle für den Betrieb von Oktagon zuständig und somit ebenfalls zuständig für Abstimmungen und Austausch mit den Vertreter:innen der Spitzenorganisationen (im folgenden SpO) im laufenden Betrieb. Die Standardsoftware Oktagon beinhaltet ein Auswertungsmodul, das jedoch in der FHH nicht eingesetzt wird und vom Hersteller OTS abgekündigt wurde. Die Auswertungen sind somit begrenzt auf Standardreports, die nur von der KST aus der separaten Struktur des Datawarehouse (DW) abgerufen werden (Vgl. Standardreport). Datenauswertungen werden somit nicht aus dem operativen System vorgenommen, sondern aus einem gesonderten Datawarehouse. Die Übertragung der Echtdaten aus dem operativen System in das DW erfolgt unter Anwendung einer Filterung, bei der personenbezogene Daten nicht in das DW übertragen werden. Datenauswertungen werden nicht für Zwecke der Verhaltens- und Leistungskontrolle von Beschäftigten durchgeführt (vgl. § 5 der Vereinbarung).

III. Regelungen

1) Sollten Veränderungen der Ausgangslage, beispielsweise die Aktivierung des Auswertungsmoduls, auftreten, ist von Seiten der KST die Abstimmung mit den Vertreter:innen der SpO im Rahmen des kontinuierlichen Austauschs zu suchen.
2) Sollte sich die Zuständigkeit im Betrieb verändern, sind die Vertreter der SpO von Seiten der KST entsprechend zu informieren, ggf. ist hierüber Einvernehmen herzustellen, wenn die Änderungen relevante Auswirkungen auf den Vereinbarungsinhalt erzeugen. Gemäß der Vereinbarung nach § 94 HmbPersVG über den Prozess zur Einführung und Nutzung allgemeiner automatisierter Bürofunktionen und multimedialer Technik (Bürokommunikation) und zur Entwicklung von E-Government ist eine Datenerhebung zum Zwecke der Leistungserfassung von Mitarbeitenden durch Führungskräfte auf einer digital unterstützten Grundlage nicht zulässig. Die Bereitstellung von Daten, die in Oktagon erfasst wurden, zu diesem Zwecke ist somit ebenfalls nicht zulässig.
3) Der Arbeitnehmerdatenschutz gemäß DSGVO bzw. BDSG wird sachgemäß im Rahmen der Auswertungen gewährleistet.
4) Daten, die eine Organisationseinheit unter drei Personen betreffen, werden regelhaft nicht ausgewertet. Sollte ein berechtigtes Interesse einer solchen Auswertung bestehen, sucht die

KST in den Regelaustauschen eine Klärung des begleitenden Sachverhalts mit den Vertreter:innen der SpO[1].

[1] Die Belange der Rechts- und Fachaufsicht und hierauf bezogene Auswertungen werden nicht berührt. Für hierbei etwa anfallende personenscharfe Daten gilt das Verbot der Verhaltens- und Leistungskontrolle nach § 5 der Vereinbarung.

CUPOLA

Rechte- und Rollenkonzept Hunderegister

Rechte- und Rollenkonzept für das Hunderegister
Projekt Ablöse Hunderegister
Programm Cupola

verantwortlich:	Markus Block; DP21/04	
Version:	1.0.9	vom: 22.03.2022
Status:	Gültig	
Aktenzeichen:	ggf. eingeben	
Schutzstufe:	Vertraulich	
Zielgruppe:		

Inhaltsverzeichnis

1 Einleitung

Worum geht es?

Das bestehende Hamburger Hunderegister (BACom) wird durch eine Neuentwicklung abgelöst.

In diesem Zuge muss ein neues Rechte- und Rollenkonzept für alle Nutzungsgruppen/ Zielgruppen erstellt und etabliert werden.

In diesem Dokument wird beschrieben, wie das Rechte- und Rollenkonzept umgesetzt wurde, welche Nutzer- bzw. Nutzerinnengruppen es gibt und wie das Zusammenspiel der Rechte und Rollen im neuen Hunderegister funktioniert.

2 Zielgruppen

2.1 Allgemein

Hier werden die einzelnen Zielgruppen aufgelistet und beschrieben.

Die Zielgruppen wurden mit den Kotaktpersonen besprochen und abgestimmt.

Die Berechtigungen der Zielgruppen sind die gewünschten „Default Einstellungen“. Die Berechtigungen und Zugriffe können durch die Administration beliebig verändert und erweitert werden.

2.2 Sachbearbeitung in den Bezirken (Verbraucherschutz)

- Hauptanwendungsgruppe des neuen Registers.
- Können alle Einträge (bezirksübergreifend) im Hunderegister lesen und bearbeiten.
- Haben Zugriff auf den Posteingang zum Online-Dienst. Eingeschränkt können sie Aufträge vom Online-Dienst nur einsehen und bearbeiten, wenn sie regional über die ihnen zugeordnete Dienststelle berechtigt sind.
- Die Sachbearbeitung benötigt „Lesen“ und „Bearbeiten“ -Rechte, damit sie ihre Aufgaben gemäß HundeG und HundeGDVO erfüllen können.

2.3 Führungskräfte

- Nutzen die Fachanwendung eher auf dem Supervisionslevel und steuern die Arbeit der Sachbearbeiter und Sachbearbeiterinnen.
- Haben einen rein lesenden Zugriff auf vorhandene Daten.
- Die Führungskräfte, sofern Sie nicht aktiv im Register arbeiten, benötigen „Lesen“-Rechte, damit sie ihrer Steuerungsfunktion und Führungsaufgabe nachkommen können.

2.4 Mitarbeiter und Mitarbeiterinnen der Kundenzentren (KUZ / EA)

- Bearbeiten die analogen An- und Abmeldebegehren, sowie Datenänderungen der Hamburger- und Hamburgerinnen vor Ort und pflegen diese live in das Hunderegister ein.
- Können nur definierte Einträge (Personen-/ Hundedaten, Halter-/ Führerschaften) im Hunderegister lesen und bearbeiten.
- Die Mitarbeiter und Mitarbeiterinnen der Kundenzentren (KUZ/ EA) benötigen „Bearbeiten"-Rechte für Anmeldungen, Abmeldungen und Datenänderungen, damit sie den behördlichen Aufgaben gemäß HundeG und HundeGDVO nachkommen können.
- Im Sinne einer bürgernahen Verwaltung "One Face to the Customer" (direkt ohne zusätzlichen Aufwand für den Bürger/ die Bürgerinnen), gehört neben den originären Aufgaben im Meldewesen auch die Verarbeitung von Meldedaten der Hunde im Hunderegister.
- Für Anordnungen, Erlaubnisse, Vorfälle und Verstöße werden keine Berechtigungen erteilt.

2.5 Amtstierärztinnen und Amtstierärzte der Bezirke

- Prüfen Daten und im Hunderegister hinterlegte Informationen im Rahmen ihrer Arbeit.
- Können grundsätzlich alle Einträge im Hunderegister lesen, haben aber keinen Zugriff auf den Statistikbereich oder den Online-Dienst-Posteingang.
- Die Amtstierärztinnen und Amtstierärzte der Bezirke benötigen die „Lesen"-Rechte, damit sie ihre Kontrollfunktion erfüllen können.
- In einigen Bezirken obliegt ihnen auch die Aktualisierung der Daten. Hierfür wird die Rolle „Bearbeiten (BASIC)" benötigt.

2.6 Hundekontrolldienst

- Im gesamten Stadtgebiet Hamburg als Kontroll- und Vollzugsorgan zuständig und nutzt das Hunderegister mit lesendem Zugriff als Information. Es werden u. a. der Leinenzwang sowie die rechtmäßige Haltung von Hunden überprüft.
- Rein lesender Zugriff auf vorhandene Registereinträge und damit auf die erstellten Dokumente sowie die zu Personen und Hunden erfassten Daten.
- Der Hundekontrolldienst benötigt lesenden Zugriff, damit sie ihrer Funktion als Kontroll- und Vollzugsorgan nachkommen können.

2.7 Polizeivollzugsdienststellen

- Können im Rahmen der Verfolgung von Straftaten und Ordnungswidrigkeiten konkrete Abfragen zu hunderelevanten Sachverhalten über das Hunderegister durchführen.
- Können hierfür einzelne Datensätze aus dem Register entsprechend der gesetzlichen Vorgaben abfragen und diese ausschließlich lesen.
- Die Polizeivollzugsdienststellen erhalten diesen Zugang, damit sie Abfragen gemäß HundeG und HundeGDVO (§11) durchführen können.

2.8 Sachbearbeiter und Sachbearbeiterinnen Hundesteuerstelle im Finanzamt für Verkehrssteuern und Grundbesitz

- Wünschen zu steuerrechtlichen Recherchezwecken lesenden Zugriff auf das Hunderegister. Dies kann durch den Auftraggeber im Rahmen der Zielgruppenverwaltung festgelegt werden.
- Der Zugriff wird gewünscht, damit die Sachbearbeitende der Hundesteuerstelle im Finanzamt für Verkehrssteuern und Grundbesitz, bei Klärungen nicht auf die Sachbearbeitung in den Bezirken (Verbraucherschutz) zugehen müssen, sondern die Klärung selbst herbeiführen können.
- Da der Zugriff derzeit noch nicht genehmigt ist, wird diese Zielgruppe als „Wunschzielgruppe“ aufgeführt. Über den zukünftigen Zugriff auf das Register entscheidet das federführende Fachamt bzw. der Auftraggeber/ die Auftraggeberin.

2.9 ADMIN Behörde

- Kann alle Einträge (bezirksübergreifend) im Hunderegister lesen, verändern und löschen sowie auf den Statistikbereich zugreifen.
- Hat Zugriff auf den Posteingang zum Online-Dienst.
- Zugriff auf den Adminbereich, um die Nutzerdaten zu pflegen, Stammdaten zu ändern, etc.

2.10 Verschiedene Gastzugänge (Audit, Revision, etc.)

- Können alle Einträge (bezirksübergreifend) im Hunderegister lesen.
- Der Zugriff ist immer zeitlich begrenzt und muss durch einen Admin eingetragen werden.
- Die Gastzugänge benötigen lesenden Zugriff, damit sie ihrer Kontrollfunktion nachkommen können.

3 Zielgruppenverwaltung

3.1 Allgemein

Die Zielgruppenverwaltung erfolgt zur Einführung des Registers durch den Auftraggeber.

Der Auftraggeber kann zwischen den folgenden Optionen wählen.

Die Optionen sind nicht voneinander abhängig und können je Zielgruppe oder Untergruppe der Zielgruppe festgelegt werden.

3.2 Zentrale Zielgruppenverwaltung

Bei der zentralen Zielgruppenverwaltung erhält eine zentrale Stelle einen Adminzugang (siehe Kapitel Rechte und Rollen). Bevorzugt erhält der Auftraggeber diese Rolle.

Die zentrale Stelle legt alle Daten von Nutzern und Nutzerinnen und deren Zugriffsoptionen an und verwaltet diese.

3.3 Dezentrale Zielgruppenverwaltung

Bei der dezentralen Zielgruppenverwaltung erhalten ausgewählte Personen einer Zielgruppe einen Adminzugang (siehe Kapitel Rechte und Rollen).

Somit ist die einzelne Zielgruppe für die Verwaltung der Nutzer und Nutzerinnen und deren Zugriffe zuständig.

4 Rollen

4.1 Allgemein

Die Nutzer und Nutzerinnen des Hunderegisters erhalten keine einzelnen Rechte, sondern werden jeweils einer Rolle zugeordnet. Über diese Rolle werden die einzelnen Berechtigungen sowie Zugriffsbeschränkungen gesteuert.

Die Rollen werden nach Funktionen gebildet. Dies hat zur Folge, dass man mit weniger Rollen auskommt und somit den administrativen Aufwand verringert.

Die Rollen sind in zwei Kategorien aufgeteilt: BASIC und ADVANCED.

Alle Nutzer und Nutzerinnen müssen zwingend einer BASIC-Rolle zugewiesen werden. Alle weiteren Rollenzuweisungen (ADVANCED-Rollen) sind optional.

Durch Kombination dieser beiden Rollen (pro nutzender Person), ergeben sich eine Vielzahl an Berechtigungsmöglichkeiten für das Hunderegister.

Dennoch gibt es Bereiche, wie z. B. die Protokolldaten, die für keine nutzende Person des Hunderegisters einsehbar sind. Diese Bereiche sind nur für Dataport-Administratoren zugänglich.

Eine detaillierte Beschreibung folgt in den nächsten Abschnitten.

4.2 BASIC-Rollen:

BASIC-Rollen bilden die Grundrechte der Nutzer und Nutzerinnen ab, z. B. lesen oder schreiben.

Alle Nutzer und Nutzerinnen müssen einer BASIC-Rolle zugewiesen werden. Ohne diese Rolle ist eine Nutzungsfreischaltung im Register und somit die Bearbeitung oder Ansicht nicht möglich.

Es kann jeweils nur eine BASIC-Rolle pro Nutzer und Nutzerinnen gewählt werden.

4.2.1 Lesen (BASIC)

Einträge im Hunderegister können gelesen werden.

Nutzer und Nutzerinnen mit dieser Berechtigung können alle Eintragungen (bezirksübergreifend), die im Register getätigt wurden, lesen aber nicht ändern.

4.2.2 Bearbeiten (BASIC)

Alle Einträge (bezirksübergreifend) im Hunderegister können gelesen, verändert und gelöscht werden.

4.2.3 Externe Mitarbeiter und Mitarbeiterinnen der Polizei (BASIC)

Diese Rolle ist explizit für Mitarbeiter und Mitarbeiterinnen der Polizeivollzugsdienststellen vorgesehen, da diese besondere gesetzlich geregelte Zugriffe erhalten.

Nutzer und Nutzerinnen mit dieser Berechtigung können nur die lt. Gesetz definierten Abfragen tätigen und erhalten die vorgegebenen Ergebnisse.

Bei dieser Rolle kann man keine weiteren ADVANCED-Rollen zuordnen.

4.2.4 Externe Mitarbeiter und Mitarbeiterinnen der EA (BASIC)

Diese Rolle ist expliziert für Mitarbeiter und Mitarbeiterinnen der Kundenzentren (KUZ) vorgesehen, da diese nur besondere Aufgaben (Anmeldung, Abmeldung u. Datenänderung zur Person und/ oder Hund) im Register wahrnehmen dürfen.

Alle weiteren Funktionen des Registers sind für diese Rolle deaktiviert.

Bei dieser Rolle kann man keine weiteren ADVANCED-Rollen zuordnen.

Jede durchgeführte Aktion (Anmeldung, Abmeldung u. Datenänderung zur Person und/ oder Hund) dieser Rolle löst eine Weiterleitung der Informationen an das Postfach der zuständigen Sachbearbeitung aus. (Die zuständige Sachbearbeitung wird anhand der Adressdaten der hundehaltenden Person ermittelt).

In der Antragsweiterleitung an den Posteingang sind nur Daten zur getätigten Aktion enthalten. Eine Nachverfolgung, welcher Mitarbeiter oder welche Mitarbeiterin die Eingabe getätigt hat, ist nicht möglich.

4.3 ADVANCED-Rollen:

ADVANCED-Rollen sind Zusatzrechte, die Nutzer und Nutzerinnen erhalten können, z. B. Zugriff auf Statistiken oder den Posteingang.

Über die ADVANCED-Rollen werden die Zugriffsrechte auf bestimmte Funktionen im Register geregelt.

ADVANCED-Rollen sind optionale Rollen und nicht verpflichtend.

Nutzern und Nutzerinnen können beliebig viele ADVANCED-Rollen zugeordnet werden. Es gibt aber bestimmte BASIC- und ADVANCED-Kombinationen die sich gegenseitig ausschließen. Dies wird in den folgenden Abschnitten genauer erläutert.

4.3.1 Admin (ADVANCED)

Mit dieser Rolle erhält man Zugriff auf den Adminbereich.

Voraussetzung: Rolle Ändern (BASIC).

Kein Zugriff auf die Protokolldaten. Keine Möglichkeiten zur Auswertung/ Leistung und Verhaltenskontrolle.

(Ein Zugriff auf die Protokolldaten kann anlassbezogen durch die fachlich verantwortliche Stelle begründet und beauftragt werden.)

4.3.2 Posteingang (ADVANCED)

Mit dieser Rolle erhält man Zugriff auf den Posteingang und kann somit Aufträge, die über den Online-Dienst oder die Rolle Externe Mitarbeiter und Mitarbeiterinnen (EA) übermittelt wurden, einsehen und/ oder bearbeiten.

4.3.3 Posteingang-Klärung (ADVANCED)

Mit dieser Rolle werden berechtigten Personen die Klärungsaufträge im Posteingang angezeigt, die über den Online-Dienst übermittelt wurden.

Klärungsaufträge sind Aufträge, wenn die zuständige Dienststelle, aufgrund einer fehlerhaften Adresse, nicht ermittelt werden konnte.

4.3.4 Statistik (ADVANCED)

Mit dieser Rolle erhält man Zugriff auf den Bereich der gesetzlichen Statistiken (bezirksübergreifend) und kann diese erstellen.

4.3.5 Online-Dienst (Systemrolle)

Eine Systemrolle, die für die Verarbeitung der Online-Dienst-Aufträge benötigt wird.

Diese Rolle darf keinen weiteren Nutzern und Nutzerinnen zugeordnet werden.

5 Rollenverwaltung

5.1 Allgemein

Es gibt keine Rollenverwaltung. Es ist somit nicht möglich, weitere Rollen anzulegen.

Durch die Kombination der BASIC- und ADVANCED-Rollen sind alle Funktionalitäten, die für das Register benötigt werden, abgedeckt.

6 Zugriffseinrichtung

6.1 Allgemein

Die Einrichtung für die Nutzer und Nutzerinnen erfolgt zweistufig. Erst über das Active Directory und anschließend über den Admin-Bereich im Hunderegister.

6.2 Zugriffseinrichtung (Active Directory/ AD)

Die Verwaltung mittels AD erfolgt zweistufig. Über RES-Gruppen in der Verfahrens-OU (Domäne dpaorde) berechtigt das TVM auf das Verfahren. Diese RES-Gruppen enthalten ROL-Gruppen der jeweiligen Organisationseinheiten/ Zielgruppen (Domäne z. B. fhhnet). Die ROL-Gruppen werden durch die IT-Stellen der Zielgruppen gepflegt.

6.3 Zugriffseinrichtung (Register)

Alle Nutzer und Nutzerinnen- können durch einen Admin dem Register hinzugefügt werden. (Hierzu ist zwingend erforderlich, dass sich die jeweiligen Personen in der o .g. AD-Gruppe befinden.)

Über die Suche im Adminbereich wählt man die nutzenden Personen aus. Anschließend müssen die Rolle, die Dienststelle und der Gültigkeitszeitraum festgelegt werden. Erst jetzt ist ein Speichern möglich und die nutzende Person wird dem Register hinzugefügt.

Bei der Suche nach nutzenden Personen werden nur solche angezeigt, die lt. AD-Gruppe berechtigt und noch nicht dem Register hinzugefügt sind.

6.4 Datenabruf und Aktualisierung

Bei der Ersteinrichtung der Nutzer und Nutzerinnenwerden die folgenden Daten aus dem AD ausgelesen und in das Register übertragen: Abteilung, Leitzeichen, Position, E-Mail, Dienstelle, Straße, Ort, Raum, Telefon, Mobil, Fax, eFax.

Eine Aktualisierung dieser Daten erfolgt bei jeder Anmeldung am Register.

Diese Daten werden z. B. für die automatisierte Befüllung der Dokumente benötigt.

7 Zugriffsverwaltung (Register)

Die Zugriffsverwaltung kann nur durch Personen mit der entsprechenden Rolle (BASIC-Admin) geöffnet und verwendet werden.

7.1 Hinzufügen

Neue Nutzerinnen und Nutzer müssen durch einen Admin dem Register hinzugefügt werden. (Hierzu ist zwingend erforderlich, dass sich die jeweilige Person in der jeweiligen AD-Gruppe befindet.)

Siehe Kapitel Zugriffseinrichtung.

7.2 Bearbeiten

Die folgenden Eintragungen können pro nutzender Person eingestellt und beliebig angepasst werden.

- Rollen (BASIC und ADVANCED),
- Dienststelle/Verantwortlichkeit,
- Gültigkeit der Zugriffsberechtigung (von/ bis Datum).

7.3 Deaktivieren/Gültigkeit beenden

Zugriffsrechte werden nicht gelöscht sondern, dessen Gültigkeit beendet. Sobald die Gültigkeit beendet wurde, wird automatisch der Zugriff ab der nächsten Anmeldung gesperrt.

Zu empfehlen ist, dass die Nutzer und Nutzerinnen Person auch aus der AD-Gruppe entfernt wird. Dies ist aber nicht zwingend erforderlich.

8 Authentifizierung / Anmeldung

8.1 Anmeldung

Durch die LDAP-Anbindung zum AD können sich die Nutzer und Nutzerinnen mit ihrer FHH-Kennung und Passwort anmelden.

8.2 Authentifizierung (LDAP/AD)

Es wird bei jeder Anmeldung überprüft, ob die Nutzer und Nutzerinnen eine gültige Kennung sowie ein gültiges Passwort eingegeben haben.

Im zweiten Schritt wird überprüft, ob die jeweilige Person der entsprechenden AD-Gruppe zugeordnet ist.

Trifft beides zu, war die erste Authentifizierung erfolgreich und die Authentifizierung im Register wird eingeleitet.

8.3 Authentifizierung (Register)

Es wird überprüft, ob die Nutzer und Nutzerinnen im Register eingetragen sind (nach vorangegangener AD-Prüfung).

Ist dies der Fall, wird die Anmeldung am Register durchgeführt und die entsprechenden Rolleneigenschaften geladen.

9 LDAP/Active Directory (AD)

9.1 Allgemein

Das Register ist über LDAP (zukünftig LDAPS) mit dem Active Directory von Dataport verbunden.

Somit ist eine sichere Verwaltung der Nutzer und Nutzerinnen gewährleistet.

Die Nutzer und Nutzerinnen können sich mit ihrer FHH-Kennung und ihrem Passwort am Register anmelden.

Zusätzlich werden die hinterlegten AD-Daten an das Register übertragen und als Grundlage der Daten der Nutzer und Nutzerinnen verwendet.

10 Änderungsverzeichnis

Version	Änderungs-datum	Gliederungs-punkt	Erläuterung der Änderung	Autor/in
1.0.0	24.11.2021		Version 1.0.0 erstellt	Markus Block
1.0.1	07.12.2021		Alle Korrekturen eingepflegt	Markus Block
1.0.2	17.12.2021		Anmerkungen NITB Leonie Roestel eingearbeitet	Markus Block
1.0.3	16.01.2022		Zielgruppentext überarbeitet	Markus Block
1.0.4	26.02.2022		Zielgruppentext finalisiert	Markus Block
1.0.5	09.02.2022		Berechtigungskonzept in Rechte- und Rollenkonzept geändert	Markus Block
1.0.6	25.02.2022	4.1	Zugriff auf Protokolldaten	Markus Block
1.0.8	28.02.2022		Zugriff auf Protokolldaten	Markus Block
1.0.9	23.03.2022		Rechtschreibung/Gendern; Zielgruppe BJV entfernt	Philipp Lüke

PROGRAMM CUPOLA

PROJEKT EINFÜHRUNG OKTAGON

FACHKONZEPT RECHTE UND ROLLEN OKTAGON

Senat der Freien und Hansestadt Hamburg
Senatskanzlei Amt für IT und Digitalisierung
Postanschrift: Rathausmarkt 1
20095 Hamburg

CUPOLA

Hamburg

Information	Beschreibung
Programm	PPM-Nr.: 17.027 Cupola
Team	Projekt Einführung Oktagon
Dokumentenname	Fachkonzept Rechte und Rollen Oktagon
Status	überarbeitet
Version	2.0
Erstellungsdatum	20.01.2020
Dokumentenverantwortliche:r	Günter Erdl / Jan Aita-Schmitz
Ersteller:in	Stefan Straßner
Geprüft von / am	Jan Aita-Schmitz/ 24.07.2023
Freigegeben von / am	Jan Aita-Schmitz/ 28.07.2023

Datum	Beschreibung der Änderung	Name
20.01.2020	Initiale Erstellung	Stefan Straßer
06.04.2020	Ersetzung missverständlicher Screenshots	Werner Düll
12.07.2021	Neustrukturierung, Erweiterung und Aktualisierung	Werner Düll
15.07.2021	Erweiterung und Aktualisierung	Werner Düll
30.07.2021	Nacharbeiten und Aktualisierung	Werner Düll
15.06.2022	Nacharbeiten und Aktualisierung	Martins Rudevics
07.07.2022	Nacharbeiten und Aktualisierung	Martins Rudevics
02.08.2022	Ergänzung beteiligte Dienststellen, Aktualisierung Rechte & Rechtematrix DMS3	Martins Rudevics
23.08.2022	Beteiligte Dienststellen angepasst, Dokumentenlinks bearbeitet.	Martins Rudevics
30.09.2022	Rechte DMS3 aktualisieren	Martins Rudevics
07.11.2022	Anpassung Layout	Kirsten Stock
05.12.2022	Nacharbeiten und Aktualisierung	Jan Aita-Schmitz
30.12.2022	Nacharbeiten und Aktualisierung	Jan Aita-Schmitz
10.01.2023	Nacharbeiten und Aktualisierung	Jan Aita-Schmitz
31.01.2023	Aktualisierung DMS3 Rollen	Martins Rudevics
04.07.2023	Nacharbeiten und Aktualisierung	Martins Rudevics, Steffen Pillon

Anmerkung: Zur besseren Lesbarkeit wurde in diesem Dokument teilweise auf geschlechtsspezifische Formulierungen verzichtet. Die verwendeten Formulierungen richten sich jedoch ausdrücklich an alle Geschlechter.

Inhalt .....

1 Einführung und Grundsätze

In diesem Rechte- und Rollenkonzept wird beschrieben, wie Benutzer im System angelegt werden und auch welche Zugriffsregeln für Benutzergruppen auf die Daten und Funktionen des IT-Fachverfahrens Oktagon gelten.

Es weist jeder Rolle – und dadurch jedem potenziellen Benutzer – Zugriffsrechte zu und bestimmt dadurch, welche Ressourcen er tatsächlich nutzen darf. Dabei wird die Art der Autorisierung spezifiziert, beispielsweise lesen, verändern, löschen, etc..

1.1 Vorbemerkungen zum Rechte- und Rollenkonzept

1.1.1 Aufbau der Software Oktagon

Oktagon gliedert sich als Softwarelösung in zwei Komponenten, die als Standartsoftware vom Hersteller OTS angeboten werden und aufeinander aufbauen. Während g2vb+ (bzw. die Vorgängerversion g2vb), die Vorgangsbearbeitung darstellt, bildet die DMS3/eAkteOpen+ die Struktur für die digitale Ablage der Vorgänge. DMS3 und g2vb+ sind die Bezeichnungen, die vom Hersteller verwendet werden, während der Begriff eAkte ergänzend zur Herstellerbezeichnung DMS3 im Projektverlauf gewählt wurde, um damit einen zentralen Aspekt des Potenzials der Software eingängiger vermitteln zu können. Vormals wurde auch der Begriff eBauAkte verwendet. Da die eAkte jedoch auch für Verfahren außerhalb des Baurechts verwendet wird, stellt der Begriff eAkte nun die adäquatere Bezeichnung da. Die Vorgängerversion g2vb bietet für das Rechte- und Rollenkonzept weiterhin einen Bezugspunkt, da die Rechtematrizen fortgeführt werden bis eine komplette Ablösung durch g2vb+ stattgefunden hat.

1.1.2 Einordnung und Aufbau des Rechte- und Rollenkonzepts

Grundlegend für das Rechte und Rollenkonzept ist das Berechtigungskonzept. Dieses umfasst die Struktur der Berechtigungsverwaltung in Hinblick auf die Rollen- und Rechtearchitektur, die Vergabe und Änderung der Berechtigungen sowie die Dokumentation der entsprechenden Schritte. Den Ausgangspunkt bildet hierbei neben der grundlegenden Transparenz für die Ausgestaltung der Software, die Anforderungen der Anlage 10 zu den VV-ZBR. Damit bildet das Berechtigungskonzept den Hintergrund für die Gestaltung des Rechte- und Rollenkonzepts. Aufbauend darauf ist das Rechte- und Rollenkonzept dahingehend angelegt die konkrete Beschreibung der Nutzergruppen und der entsprechenden Rechte darzustellen. Die konkrete Zuordnung der technischen Rechte ergibt sich wiederum aufbauend darauf in den Rechtematrizen, die sowohl für g2vb+ als auch für die eAkte gepflegt werden. Somit bezieht sich das Rechte- und Rollenkonzept auf das Berechtigungskonzept und wird von den Rechtematrizen wiederum in Hinblick auf die technischen Funktionen konkretisiert.

1.1.3 Gleiches Passwort und Single Sign-on

Oktagon wurde mit dem FHH Active Directory (AD) verbunden. Somit ist es möglich sich mit dem gleichen Passwort wie für die Windows Anmeldung an Oktagon anzumelden. Außerdem wurde das Single Sign-on zwischen den Oktagon Modulen realisiert. Hierfür ist es notwendig, dass bei der Useranlage in Oktagon der Windowsanmeldename der Person verwendet wird. Das bedeutet das es nur einen Oktagon User pro Mandanten gibt.

1.2 Maßgebliche Struktur der Rollen

Im Kontext der Einführung von Oktagon hat sich die Rollenverteilung in drei maßgebliche Gruppen von Anwendern aufgeschlüsselt, die sich aufgrund der unterschiedlichen Rechtekonstellation unterscheiden:

Administratoren:

- ✓ Zugriff auf eAkte und eIndex
- ✓ Systemverwaltung
- ✓ Nutzerverwaltung

Sachbearbeiter/Führungskräfte:

- ✓ Vorgangsanlage / Vorgangsbearbeitung
- ✓ Zugriff auf eAkte und eIndex
- ✓ Abzeichnung

Fachdienststellen (Beteiligte Dienststellen):

- ✓ Zugriff auf eAkte, falls diese beteiligt wurden (über einen Beteiligungslink)
- ✓ Können die eAkte eines Vorgangs einsehen, aber nicht bearbeiten
- x Zugriff auf Vorgangsbearbeitung (g2vb+)

Fachdienststellen Schreibrechte (Rechtsämter):

- ✓ Zugriff auf eAkte, falls diese beteiligt wurden (über einen Beteiligungslink)
- ✓ Können die eAkte eines Vorgangs einsehen, bearbeiten und neue Dokumente hinzufügen
- x Zugriff auf Vorgangsbearbeitung (g2vb+)

Die Rollen von Führungskräften und Sachbearbeitern sind nahezu identisch, damit bei Ausfällen die Aufgaben übernommen werden können. Nähere Unterschiede können im Folgenden sowie in den Rechtematrizen nachvollzogen werden.

1.3 Auswertungen und Leistungserfassung

Gemäß Abschnitt 4 der Vereinbarung nach § 94 HmbPersVG über den Prozess zur Einführung und Nutzung allgemeiner automatisierter Bürofunktionen und multimedialer Technik (Bürokommunikation) und zur Entwicklung von E-Government sowie § 7 der Einführungsvereinbarung des Programm Cupola nach § 93 HmbPersVG vom 3. August 2021 werden anwenderbezogene Auswertungsfunktionen zur Leistungserfassung nicht bereitgestellt.

2 Vergabe, Änderung, Kontrolle und Löschung von Benutzerrollen und Berechtigungen

Ein wichtiger Baustein des Rechte- und Rollenkonzepts ist die Definition von Prozessen. Es muss bekannt sein, wie die Nutzereinrichtung, Vergabe von Berechtigungen, Änderung von Berechtigungen, Kontrolle, Nutzerlöschung, Löschung von Rollen (Benutzerrollen) und Rechten (Berechtigungen) erfolgt und auch wie diese dokumentiert werden.

Da diese Definition bereits integraler Bestandteil des Antrags auf Einwilligung zur Einführung des IT-Verfahrens Oktagon nach Nr. 14 Anlage 10 zu den VV-ZBR (Verwaltungsvorschriften für Zahlungen, Buchführung und Rechnungslegung (zu §§ 70 bis 72 und 74 bis 80 LHO) der Freien und Hansestadt Hamburg) ist, wird bezüglich der Ausgestaltung dieser Prozesse auf das Berechtigungskonzept verwiesen.

Die folgenden Prozesse sind Ausschnitte aus dem Berechtigungskonzept und werden im Berechtigungskonzept genauer beschrieben.

2.1 Benutzerverwaltung

Alle Benutzer des IT-Verfahrens Oktagon (anwendende Stellen, Fachliche Leitstelle etc.) werden in einer Benutzerverwaltung geführt. Oktagon kann nur von Personen genutzt werden, die als aktive Benutzer hinterlegt sind. Aktiv ist ein Benutzer, wenn sein Konto in der Oktagon-Benutzerverwaltung den Status „freigegeben“ aufweist. Die Oktagon-Benutzerverwaltung erfolgt mandantenspezifisch und kann für das Vorgangsbearbeitungssystem und die eAkte unabhängig voneinander erfolgen. Wird ein Benutzer in einem Mandanten als „System-Benutzer“ im Vorgangsbearbeitungssystem angelegt, ist dieser gleichzeitig auch Nutzer der eAkte wenn der gesetzte Haken bei „DMS3-Abgleich“ nicht entfernt wird.

2.2 Einrichtung von Rechten und Rollen

Die Einrichtung der konkreten User-Rechte und -Rollen für das IT-Verfahren „Oktagon“ erfolgt durch die Koordinierungsstelle Oktagon (fachliche Leitstelle) bzw. den jeweils dazu befugten Dienststellen in den Bezirken (siehe Kapitel 3 im Berechtigungskonzept).

Die Beauftragung der Pflege und Änderung von Musterrollen obliegt ebenfalls der Koordinierungsstelle Oktagon (fachlichen Leitstelle). Änderungen erfolgen nur, wenn eine ordnungsgemäße Aufgabenerledigung mit den vorhandenen Musterrollen nicht möglich ist. Einrichtung, Änderung und Löschung von Musterrollen werden von der Leitung der Koordinierungsstelle Oktagon in Textform an das Dataport FVM (Fachlichen Verfahrensmanagement) beauftragt. Umgesetzt und in der eAkte dokumentiert werden diese vom Dataport FVM (in der Rolle der Administration). Die geänderte Version des Rechte- und Rollenkonzepts werden ab Gültigkeit der Berechtigung im Rahmen der vorgesehenen 10-jahres Frist in der eAkte archiviert. Die Leitung der Koordinierungsstelle Oktagon wird nach der Umsetzung über die Anpassung durch Dataport informiert und überprüft die Änderung und Neueinrichtung der Musterrolle und gibt diese auch gegebenenfalls frei. Änderungen der Musterrollen werden in Textform dokumentiert, systemseitig protokolliert und als Anlage dem vorliegenden Berechtigungskonzept beigefügt.

2.3 Benutzerrollen im Vorgangsbuch

In der Oktagon-Benutzerverwaltung werden keine Berechtigungen bezüglich der Vier-Augen-Prüfung verwaltet, da der gesamte Anordnungsprozess ausgelagert wurde und über das Anordnungsmodul der DRiVe-IT abgewickelt wird. Für die Feststellung der sachlichen und rechnerischen Richtigkeit sowie die Anordnung von Buchungen wird der bereits abgestimmte Genehmigungsworkflow in Vorgangsbuch genutzt. Zur Steuerung der Berechtigungen im Vorgangsbuch werden in den Bezirken jeweils zwei Berechtigungslisten in der AD (Kontenpflegetool) geführt.

2.4 Vergabe von Berechtigungen

Maßnahmen der Berechtigungsverwaltung im IT-Fachverfahren Oktagon zur Neuanlage von Benutzerkonten, Berechtigungsänderungen für bereits eingerichtete Benutzerkonten und Löschung von Berechtigungen ausgeschiedener Mitarbeiter/innen werden von der Koordinierungsstelle aufgrund der hohen Nutzerzahlen an die Leitung der jeweilig nutzenden Dienststellen delegiert. Für die Vergabe von Berechtigungen wird ein mehrstufiges Verfahren durchlaufen. (Diese werden im Berechtigungskonzept ausführlich beschrieben)

- Antragsstellung in Textform (auch per E-Mail)
- Prüfung des Antrags und Einrichtung der Berechtigung
- Dokumentation

Die Vergabe von Berechtigungen für die Nutzung des Genehmigungsworkflows im Vorgangsbuch erfolgt durch die nutzenden Dienststellen. Die entsprechend erforderliche Feststellungs- und Anordnungsbefugnisse für die jeweiligen User werden von einer vom BfH befugten Person erteilt.

2.5 Änderung von Berechtigungen

Bei der Veränderung von Aufgabenzuständigkeiten oder Weggang eines Nutzers prüft dessen Vorgesetzter, ob Änderungen bei der Berechtigungsvergabe oder die Löschung von nicht mehr benötigten Berechtigungen erforderlich sind. (Die einzelnen Schritte werden im Berechtigungskonzept ausführlich beschrieben)

- Antragsstellung in Textform (auch per E-Mail)
- Prüfung des Antrags und Änderung der Berechtigung
- Dokumentation

2.6 Nachweis der Verwaltung von Berechtigungen

Aufträge von Antragsberechtigten zur Einrichtung, Erweiterung, Veränderung, Entzug oder Löschung von Berechtigungen müssen in Textform (auch per E-Mail) an das Fachliche Verfahrensmanagement erfolgen. Die Anträge sind vom Auftraggeber und von Dataport während der Gültigkeit der Berechtigung aufzubewahren.

Sämtliche Maßnahmen der Erfassung, Änderung oder Löschung von Daten eines Nutzerdatensatzes werden technisch mit altem und neuem Wert protokolliert. Systemseitig mitgeschrieben wird die Information wer, wann, welche Daten und Berechtigungen erfasst, geändert oder gelöscht hat. Die Protokolle werden dauerhaft aufbewahrt.

2.7 Beteiligte Dienststellen

Falls eine beteiligte Dienststelle in einem Vorgang keinen Zugang zu Oktagon DMS3 hat, kann dieser Zugang über das Support-Postfach beantragt werden. Die User-Anlage für beteiligte Dienststellen erfolgt nur in DMS3/eAkte+. Dabei werden dem Benutzer eingeschränkte Rechte auf der eAkte+ vergeben, damit er nur die Dokumente sehen kann, die für ihn notwendig sind.

Es wird bei dem Benutzer der „Embedded Mode“ eingestellt, um die Suche nach Dokumenten und Akten zu verweigern. Der Benutzer bekommt keinen Zugang auf g2vb/g2vb+.

Über das Beteiligungsdokument bekommt der Benutzer einen verschlüsselten Link. Über diesen Link kann der Benutzer nur die eAkte und die darin enthaltenen Dokumente dieses bestimmten Vorgangs einsehen.

Nach der User-Anlage wird der Nutzer der beteiligten Dienststelle via Email informiert und der angelegte Benutzer wird in der Benutzerliste dokumentiert.

3 Vorgangsbearbeitung (g²vb und g2vb+)

In g2vb gibt es folgende Rollen, bei Benutzeranlage wird einem Benutzer immer eine dieser Rollen vergeben:

Rolle	Zuordnung DMS³-Rolle	Beschreibung	Anmerkung
Administration	**Administratoren**	(zentrale) Systemadministratoren	
Fachadministration	**Fachadministration**	(dezentrale) fachliche Administratoren in den Bezirken mit erweiterten Rechten	
Führungskräfte	**Führungskräfte, Abzeichnung, Sachbearbeiter, eIndex Modul**	Führungskräfte der direkt vorgesetzten Ebene (ähnliche Rechte wie Sachbearbeiter)	
Sachbearbeiter	**Abzeichnung, Sachbearbeiter, eIndex Modul**	Sachbearbeiter / Bauprüfer / Geschäftszimmer	
QS_TVM	**QS_TVM**	Zugriff für TVM für Systemprüfung, keinerlei Rechte in der Vorgangsbearbeitung	
Audit	**Audit**	Rolle für Prüfer, voller Lesezugriff (z.B. Rechnungshof	zeitlich befristete Zuordnung auf Anforderung

In der Benutzeranlage ist es darüber hinaus möglich die einzelnen Benutzer durch eine Zuordnung in Teams zu gruppieren. Diese Teamzuordnung dient der organisatorischen Einteilung innerhalb einer Dienststelle und hat ggf. Auswirkungen auf Dokumenteninhalte, da z.B. unterschiedliche Funktionspostfächer im Briefkopf eines Dokuments eingebunden werden. Die Teamzuordnung hat keinen Einfluss auf erteilte oder nicht erteilte Berechtigungen und wird deshalb in diesem Konzept nicht weiter betrachtet.

3.1 Rechtezuordnung zu den Rollen in g²vb und g2vb+

Bezüglich der Rechtezuordnung zu Rollen wird auf die Rechtematrix Vorgangsbearbeitung (g²vb und g2vb+) verwiesen. Hier findet sich eine detaillierte Darstellung der entsprechenden Rechte für die bestehenden Rollen.

3.2 G2vb+ Rechte- und Layout-Zuordnung

Bei der Benutzeranlage müssen auch Rechte und Layouts dem Nutzer in g2vb+ vergeben werden. Diese Rechte und Layouts können einem Benutzer zugeordnet werden:

Rollen	Beschreibung
OTS-Standardrolle für Rechte – alle Rechte	**OTS-Standardrecht für Rechte (überall Schreibrechte)**
OTS-Standardrolle für Layout	**OTS-Standardrolle für Layout**
Sachbearbeiter Recht	**Sachbearbeiter Recht Oktagon**
Führungskräfte Recht	**Führungskräfte Recht Oktagon**
Sachbearbeiter Layout	**Sachbearbeiter Layout Oktagon**
Führungskräfte Layout	**Führungskräfte Layout Oktagon**

Die Rechte und Layouts dienen dazu, dem Benutzer den Zugang auf die g2vb+ Oberfläche zu ermöglichen. Hinter diesen Rechten hängt eine weitere Rechtestruktur. Die Rechtezuordnung ist ebenfalls in der Rechtematrix Vorgangsbearbeitung (g²vb und g2vb+) zu finden.

4 eAkte (DMS³/eAkteOpen+)

In der eAkte können einem Benutzer mehrere Rollen zugewiesen werden, die einzelnen Rechte der Rollen gelten hier additiv. Alle Rollen werden nur im Rahmen der entsprechenden fachlichen Notwendigkeit und daraus folgenden Zuschreibung vergeben. Außerdem können die Benutzereinstellungen bei der Benutzerbearbeitung unter „Optionen“ bearbeitet werden.

Rolle	Beschreibung	Anmerkung
Administratoren	DMS3-Administration	Standardrolle (administrativ)
Fachadministration	dezentrale Fachadministration	Standardrolle (administrativ)
Admin_eDesign	Berechtigung für das Modul eDesign	Standardrolle (administrativ)
Admin_eVorlageAdministration	Berechtigung für Administration der Dokumentvorlagen in DMS3	Standardrolle (administrativ)
Admin_eVorlageModul	Berechtigung für Bearbeitung von Dokumentvorlagen in DMS3	Standardrolle (administrativ)
Admin_eVorlagenGruppenBearbeiten	OTS Standardrolle für eAkte Vorlagenberechtigungen	
Admin_eVorlagenRollenfreigabe1	OTS Standardrolle für eAkte Vorlagenberechtigungen	
Admin_zentral	Adminzugang nur reine Rollen-/Benutzer-zuweisung	
Abzeichnung	Standard - Berechtigung User zum Abzeichnungsprozess	Standardrolle (operativ)
eIndex Modul	Standard - eIndex Modulaufruf	Standardrolle (operativ)
Buergerauskunft	Standard - Funktionsfreischaltung Bürgerauskunft	Standardrolle (operativ)
Akteneinsicht	Funktionsfreischaltung Akteneinsicht	
Eldorado Prüfer	Fehlerbehebung Eldorado	
Fachdienststellen	Aktenfreischaltung beteiligte Stellen	
Fachdienststellen_Schreibrechte	Aktenfreischaltung beteiligte Stellen/Rechtämter, Dokumente in die Akte ablegen	
Aktenfreigabe	Temporäre Aktenfreigabe	
Führungskräfte	Aktenfreischaltung Führungskräfte der	

Nachbar	direkt vorgesetzten Ebene Aktenfreischaltung Nachbar	
Sachbearbeiter	Aktenfreischaltung Sachbearbeiter	
QS_TVM	QS Zugriff TVM für Systemverfügbarkeit	
Audit	externe Prüfung (nur Leserechte)	zeitlich befristete Zuordnung auf Anforderung
ots_Admin_g2vb	Berechtigung für das Modul otsAdmin (g2vb)	Standardrolle (administrativ)
System_Crossmandator	Aktenfreischaltung technischer Benutzer	technische Rolle (mandantenübergreifende Zusammenarbeit)
System_Eldorado	Aktenfreischaltung technischer Benutzer	technische Rolle (Langzeitarchivierung)
System_ImportManager	Aktenfreischaltung technischer Benutzer	technische Rolle (Nachrichtenimport)
System_xExporter	Aktenfreischaltung technischer Benutzer	technische Rolle (Nachrichtenexport)
otsAdmin_otsmd	Berechtigung für das Modul otsAdmin (otsmd)	Standardrolle (administrativ)
Projektakte	Nur DEV – Aktenfreischaltung Projektakte Global	
Projektmanagement	Nur DEV – Aktenfreischaltung Projektmanagement	

4.1 Rechtezuordnung zu den Rollen in DMS³/eAkte+

Bezüglich der Rechtezuordnung zu Rollen wird auf die Rechtematrix eAkte (DMS³/eAkteOpen+) verwiesen.

4.2 Weitere Rechteprofile in DMS3

Fachprofile werden bei Benutzeranlage manuell vergeben. Man unterscheidet zwischen zwei Fachprofilarten: Fachprofil (Akten) und Fachprofil (Dokumente). Den entsprechenden g2vb-Rollen werden diese Fachprofile vergeben (Fachprofile können auch an Benutzer vergeben werden, die nur in der eAkte angelegt wurden):

Rolle (g2vb)	Zuordnung Fachprofil (Akten)	Zuordnung Fachprofil (Dokumente)
Administration	Aktenprofil_Standard	FHH-Admin
Fachadministration	FHH-Sachbearbeitung_Akten	FHH-Sachbearbeitung_Dokumente
Führungskräfte	FHH-Sachbearbeitung_Akten	FHH-Sachbearbeitung_Dokumente

Sachbearbeiter	FHH-Sachbearbeitung_Akten	FHH-Sachbearbeitung_Dokumente
Fachdienststellen	FHH-Sachbearbeitung_Akten	Oktagon-Fachdienststelle
Fachdienststellen_Schreibrechte	FHH-Sachbearbeitung_Akten	Oktagon-Fachdienststelle
Weitere Fachprofile:	Aktenprofil_Standard, FHH-Standard	, OTS-Standard

Suchprofile werden bei Benutzeranlage automatisch durch die Rollen zugeordnet und müssen nicht manuell angepasst werden. Hinter den entsprechenden DMS3-Rollen stecken diese Suchprofile:

Suchprofil	**Rolle (DMS3)**
Akten Scandienstleister	Sachbearbeiter
Dokumente QS-Defizit	Sachbearbeiter
Eldorado manuell prüfen	Sachbearbeiter
ePostfach	
fachliche Prüfung	Sachbearbeiter
Favoriten	
Genehmigungsverfahren	Sachbearbeiter
Globalakte	
GV_Objektklassen	
Meine ausgecheckten Dokumente	Sachbearbeiter
Meine Index-ausgecheckten Dokumente	Sachbearbeiter
Ordnungsaufgaben	
Projektakte	Projektakte
Rechtsakte	
Registratur	Sachbearbeiter
$STANDARD	
vollständig zur Prüfung	Sachbearbeiter
Vorlagen	Administratoren
zurück an Registratur	Sachbearbeiter

Anzeigeprofile bestimmen welche Merkmale in einer Tabelle angezeigt werden sollen und können auch manuell angepasst werden.

Anzeigeprofile sind auch den Suchprofilen zugeordnet und müssen nicht manuell angepasst werden. Dies sind die Anzeigeprofile mit den nutzenden Suchprofilen:

Anzeigeprofil	**Suchprofil**
Akten Scandienstleister	Akten Scandienstleister

AktenlinksMix	
Alle_Akte	Eldorado manuell prüfen, Genehmigungsverfahren, Globalakte, Ordnungsaufgaben, Rechtsakte
Alle_Objektklassen	GV_Objektklassen
Bauliche Anlagen	
Dokumente QS-Defizit	Dokumente QS-Defizit
Dokumenterstellung Word	
ePostfach	ePostfach
Favoriten	Favoriten
Liegenschaft_W	
Meine ausgecheckten Dokumente	Meine ausgecheckten Dokumente
Meine Index-ausgecheckten Dokumente	Meine Index-ausgecheckten Dokumente
Mustermigration_Akte	
Mustermigration_Eldorado_Objektklassen	
Mustermigration_Objektklassen	
OTS_Genehmigungsverfahren	
OTS_Genehmigungsverfahren_Bescheide	
OTS_Genehmigungsverfahren_Beteiligungen	
OTS_Genehmigungsverfahren_Objektklasse	
Posteingang Dokumente	
Projektakte_Akte	Projektakte
Projektakte_Objektklassen	
$STANDARD	fachliche Prüfung, Registratur, $STANDARD, vollständig zur Prüfung, zurück an Registratur
Ueberwachungen	
Vorlagen	Vorlagen
Wiedervorlagen	

PROGRAMM CUPOLA

PROJEKT EINFÜHRUNG OKTAGON BAU

QUALIFIZIERUNGSKONZEPT

Senat der Freien und Hansestadt Hamburg
Senatskanzlei Amt für IT und Digitalisierung
Postanschrift: Rathausmarkt 1
20095 Hamburg

CUPOLA

Hamburg

Information	Beschreibung
Programm	PPM-Nr.: 17.027 Cupola
Team	Projekt Einführung Oktagon Bau
Dokumentenname	Qualifizierungskonzept
Status	überarbeitet
Version	1
Erstellungsdatum	03.11.2022
Dokumentenverantwortliche:r	Malte Lindner
Ersteller:in	Malte Lindner
Geprüft von / am	Jan Aita-Schmitz/ 06.12.2022
Freigegeben von / am	Jan Aita-Schmitz/ 06.12.2022

Änderungshistorie:

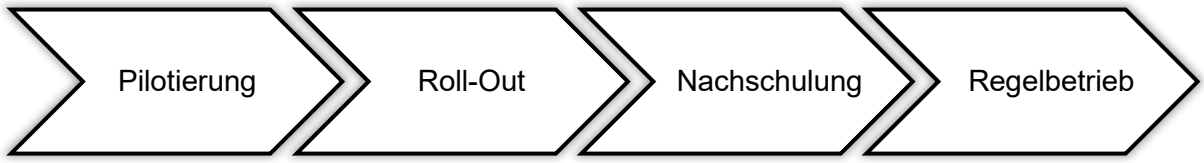
Datum	Beschreibung der Änderung	Name
03.11.2022	Erstellung	Malte Lindner
07.11.2022	Layout angepasst	Kirsten Stock
29.11.2022	Nacharbeiten und Aktualisierung	Malte Lindner
03.01.2023	Nacharbeiten und Aktualisierung	Jan Aita-Schmitz
10.01.2023	Nacharbeiten und Aktualisierung	Jan Aita-Schmitz

1 Ziel des Dokuments

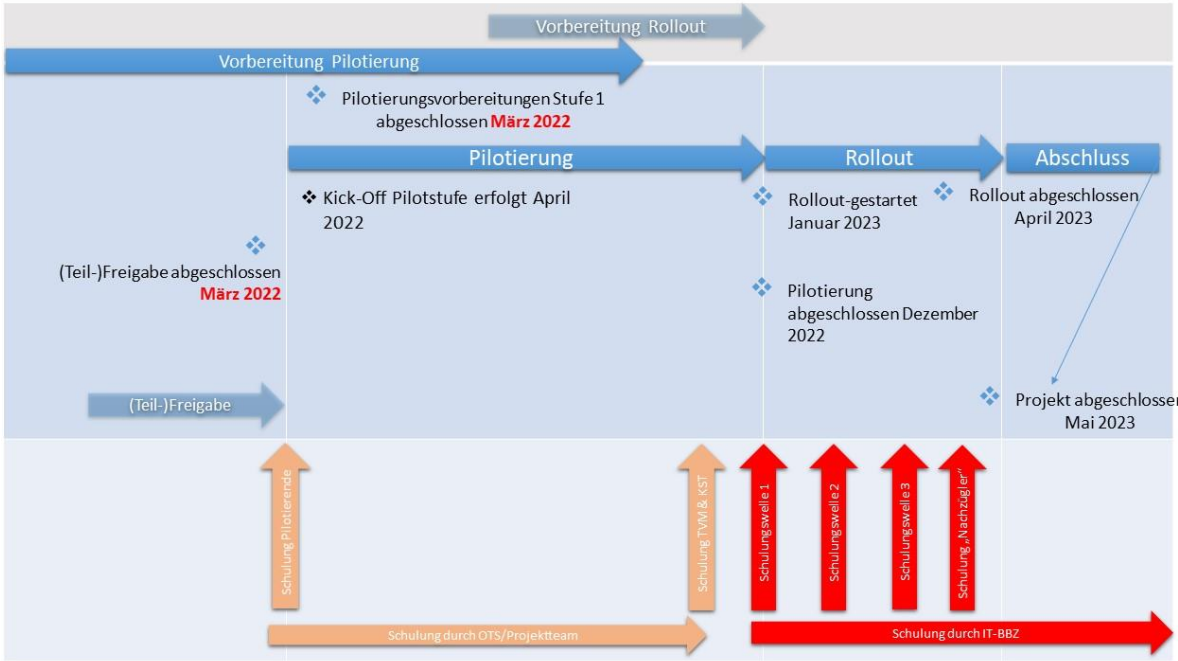
Das vorliegende Dokument hat zum Ziel einen konzeptionellen Überblick über die für die Einführung der Software Oktagon im Bauprüfbereich notwendigen Schulungen zu schaffen.

2 Übersicht der Qualifizierungsphasen

Aus der Perspektive der Qualifizierungsplanung lassen sich folgende Phasen während der Einführung identifizieren:



3 Roadmap der Qualifizierung



4 Zielgruppen der Qualifizierung

Die Qualifizierungsangebote während der Einführung von Oktagon richten sich an folgende Zielgruppen:

- Führungskräfte und Teamleiter:innen, die Oktagon für übergeordnete Tätigkeiten nutzen.
- Bauprüfer:innen und Sachbearbeiter:innen, die in dem Fachverfahren Oktagon Bauanträge von der Prüfung bis zur Genehmigung und darüber hinaus bearbeiten.
- Mitarbeiter:innen aus Registratur und Geschäftszimmer, die in Oktagon den Eingang der Bauanträge bearbeiten

- Mitarbeiter:innen, die Sonderthemen bearbeiten (u.a. AwSV-Überwachung und Schornsteinfegerarbeiten)
- Beteiligte Dienststellen, die im Rahmen des Bauantragsverfahrens über die eAkte auf Dokumente und Akten zugreifen.
- Rechtsämter, die im Rahmen ihrer Aufgaben lesenden Zugriff haben

Zudem haben die Spitzenverbände und Personalräte die Möglichkeit an Qualifizierungsmaßnahmen teilzunehmen (siehe Vereinbarung nach §93 des HmbPersVG).

Abgesehen von den beteiligten Dienststellen und den Rechtsämtern werden alle oben genannten Zielgruppen in Präsenz geschult (sofern dies die Pandemielage erlaubt).

5 Ziele der Qualifizierung

Vor diesem Hintergrund ist das übergeordnete Ziel der Qualifizierungsmaßnahmen, die Beschäftigten bedarfsgerecht auf die Arbeit mit Oktagon vorzubereiten:

- Allen Beteiligten wird in rollenspezifischen Schulungen der Umgang mit der neuen IT-Lösung vermittelt. Die Anwender:innen werden entsprechend ihrer Rolle mit dem erforderlichen Handwerkszeug ausgerüstet, um die tägliche Arbeit mit Oktagon aufnehmen zu können – über den Eingang des Bauantrages und die Antragsprüfung bis hin zum Versenden des Bescheids.
- Die Anwender:innen haben in praxisnahen und computergestützten Schulungen die Möglichkeit, sich an die neue Software schrittweise heranzutasten und konkrete Vorgänge des Bauantragsverfahrens in Oktagon auszuprobieren.
- Als sinnvolle Ergänzung wurde während der Pilotierungsphase der Austausch und die Vernetzung untereinander gefördert. In regelmäßigen Sprechstunden und Dailys können die Teilnehmenden sich über Fragen und Herausforderungen, die sie im Zusammenhang mit der Digitalisierung ihres Arbeitsplatzes bewegen, austauschen und ihre Erfahrungen mit anderen teilen.
- Durch eine individuelle Begleitung der Anwenderinnen und Anwender an ihrem Arbeitsplatz (Betreuung durch ein Supportteam) wird sichergestellt, dass auf Fragen, die sich bei der Anwendung der neuen IT-Lösung in der Anfangszeit ergeben, direkt reagiert werden kann.
- Mit dem Ziel, auch langfristig Hilfestellungen für die Beteiligten bereitzustellen, werden ein Benutzerhandbuch, FAQs, Glossare, Übersichtsdokumente und andere Handouts konzipiert, die den Beschäftigten eine „Hilfe zur Selbsthilfe“ ermöglichen.
- Die Lernangebote werden barrierefrei angeboten.

6 Schulungsformate

Grundsätzlich sind drei Formate im Rahmen der Qualifizierung vorgesehen. Diese sind Umsteigerschulungen, Änderungsschulungen und Einsteigerschulungen.

6.1 Umsteigerschulung

Hierunter fällt die Umschulung von BACom auf die Software OKTAGON. Anwender:innen, die schon mit BACom als Bauprüfer:innen sowie Geschäftszimmer- und Registraturmitarbeiter:innen gearbeitet haben, kommen für die Umsteigerschulungen in Frage. Da zukünftig Vorgänge mit der Software OKTAGON anstatt der Software BACom bearbeitet

werden, müssen die Anwender:innen der „Alt-Software“ BACom auf die neue Software OKTAGON umgeschult werden.

6.2 Einsteigerschulung

Einsteigerschulungen richten sich an diejenigen Anwender:innen, die zuvor noch nicht mit der Software BACom gearbeitet haben. Sie richtet sich an diejenigen, die weder mit der digitalen Bearbeitung von Vorgängen noch der eAkte vertraut sind. Im Rahmen dieser Schulung muss das Wissen um die digitale Bearbeitung mit der Software OKTAGON komplett erlangt werden. Auch sollten hier Grundlagen wie die Programmphilosophie übermittelt werden, um ein gemeinsames Bild zu schaffen. Regelmäßige Einsteigerschulungen aufgrund von Personalwechseln sind bedarfsabhängig mitzudenken.

6.3 Änderungsschulung

Änderungsschulungen werden orientiert an dem Bedarf durchgeführt, d.h., dass die Auswirkungen, die Änderungen bzw. die Weiterentwicklung der Software OKTAGON mit sich bringen, in Hinblick auf die Auswirkungen auf die Nutzung betrachtet werden und dann entsprechende Formate entwickelt werden um die effektive Bedienung der Software OKTAGON zu ermöglichen. In diesem Zuge werden die Anwender:innen sachgemäß informiert und nachgeschult. Hierzu sind auch e-Learning-Format denkbar.

7 Kursangebote

Folgende Kursangebote ergeben sich für die Einführung Oktagons.

Prozessschritt	Registratur & Geschäftszimmer	MA Bereiche Schornstein-fegerrecht, PVO sowie AwSV	Bauprüfer*innen & Teamleiter*innen	Führungskräfte	Beteiligte Dienststellen
Grundverständnis Oktagon					
•Allgemeine Einleitung	x	x	x	x	x
•Oktagon/eBauAkte/Vorgangsbearbeitung	x	x	x	x	
Grundlagen Oktagon					
•Begrifflichkeiten	x	x	x	x	x
•Bewegen in der Akte	x	x	x	x	x
•Speichern/Bearbeiten	x	x	x	x	x
•Dokumentenverwaltung	x	x	x	x	x
•Arbeiten in der Vorgangsbearbeitung	x	x	x	x	
•Dokumentenerstellung/Textbausteine etc.	x	x	x	x	
Bauantrag anlegen					
•Posteingangsscannen	x				
•OSI Plattform	x	x	x		
•Georeferenzierung	x	x	x		
•Aufgabenliste	x	x	x		
Bauantrag zuweisen					
•Vorgangsstart	x	x	x		
•Sachbearbeiter zuweisen	x	x	x		
Sachliche Zuständigkeit					
•Vorgangstypänderung	x	x	x		
•Sachbearbeiterwechsel	x	x	x		
Bauantrag Vollständigkeit ermitteln					
•Aufgabenbögen			x		
•Nachforderung			x		
Fachliche Prüfung durchführen					
•Prüfthemen		x	x		
Beteiligung durchführen					
•Beteiligung von Dienststellen			x		
•Nachbarbeteiligung			x		
•Nachlieferung			x		
Entscheidung					
•Baukommission			x	x	
•Bauausschuss			x	x	
•Baubescheid erstellen		x	x		
Gebühren					
•Gebührenberechnung	x	x	x		
•Gebührenposition	x	x	x		
•Gebührenbescheid	x	x	x		
Auswertung & Statistik			x	x	

Da die Pilotierung nicht als „Big-Bang-Szenario“ geplant war und in der ersten Stufe nur die Verfahren nach §61 und §62 HBauO eingeführt wurden, war zu Beginn der Pilotierung keine Schulung zu den Themen PVO, Schornsteinfegerrecht und AwSV notwendig. In den weiteren Stufen kommen konsekutiv die anderen Verfahren hinzu. Die genaue Abfolge und der genaue

Zeitplan und damit auch die Schulungen, werden dynamisch dem Verlauf des Projektfortschrittes angepasst. Die Beteiligten Dienststellen arbeiten zunächst weiterhin in BACom, haben jedoch bereits Zugriff auf die eAkte und werden in digitalen Formaten in diese Funktionen eingewiesen.

Während des Rollouts bzw. im Regelbetrieb werden die vier Schulungsgruppen getrennt geschult. Es wird in drei Wellen geschult, so dass es in den Schulungen zu einer Durchmischung der Dienststellen kommt und ein fachlicher Austausch über die Bezirksgrenzen hinweg ermöglicht wird. Die Schulungsunterlagen werden durch den Schulungsanbieter an die Teilnehmer:innen verteilt. Die terminliche Organisation bzw. Buchung der Kurse für die drei genannten Zielgruppen läuft während des Rollouts ebenfalls über den Schulungsanbieter. Nach den flächendeckenden Schulungen werden Nachschulungen für „Nachzügler:innen“ angeboten, so dass bis zum Projektende alle Nutzer:innen geschult sind.

Im Anschluss an die jeweiligen Schulungen unterstützen die Dozent:innen die neu angelernten Mitarbeiter:innen (gegebenenfalls durch Floorwalking vor Ort in den Dienststellen) bei Fragen und Schwierigkeiten. Des Weiteren werden vom IT-Bildungs- und Beratungszentrum von Dataport regelmäßige Online-Sprechstunden angeboten in denen Fragen von den Anwender:innen gestellt werden können. Weitere Support-Angebote im Sinne einer Hypercarephase sind empfehlenswert und liegen im Ermessen der Koordinierungsstelle bei der BSW, die den Betrieb mit Beginn der Rollout-Phase übernimmt.Die Bereitstellung von Schulungen nach dem Rollout liegt in der Verantwortung der Koordinierungsstelle. Eine Übernahme der bereits während der Projektlaufzeit entwickelten Kurse ist zu empfehlen.

8 Nachbetreuung der Anwender:innen bei Fragen und Problemen

Die Nachbetreuung der Beteiligten bei Fragen und Problemen rund um die Anwendung der neuen Software gestaltet sich in den verschiedenen Phasen der Softwareeinführung unterschiedlich, bzw. wird von unterschiedlichen Stakeholdern geleistet.

Während der Pilotierung wurde die Betreuung der Pilotierungsteilnehmer:innen maßgeblich durch designierte Mitarbeiter:innen des Projekts Oktagon Bau geleistet. Ihre Aufgaben waren:

- Unterstützen der Pilotierungsteilnehmer:innen beim Umgang mit der Software OKTAGON am Arbeitsplatz
- Allgemeine Klärung und Beantwortung von Fragen der zur Software OKTAGON (inklusive der Weitergabe von Tipps und Tricks zur Anwendung),
- Fungieren als Schnittstelle zwischen Pilotierungsteilnehmer:innen und Technik (Support IT-Angelegenheiten usw.)
- Kommunizieren mit der/ dem Rolloutkoordinator:in zu pilotierungsrelevanten Themen
- Ansprechpartner:in für das Programm

Während des Rollouts und des darauffolgenden Regelbetriebs werden der 1st-Level-Support vom UHD und der 2nd-Level-Support von der Koordinierungsstelle geleistet. Nach ca. 4 – 6 Monaten Arbeit mit dem IT-Verfahren wird den Anwenderinnen und Anwendern Gelegenheit gegeben, durch eine Ergänzungsqualifizierung selbst empfundene Defizite aufzuarbeiten.

9 Evaluierung

Im Rahmen der Pilotierung wurden die Schulungen sowie Schulungsmaterialien evaluiert. Auf der Basis der Ergebnisse sind Rückschlüsse für weitere Formate möglich. Eine Evaluierung im Rahmen des Rollouts erscheint weiterhin sinnvoll, um die Schulungen an die Bedarfe der Anwender:innen anzupassen.

PROGRAMM CUPOLA

SCHULUNGSKONZEPT SWAN

Senat der Freien und Hansestadt Hamburg –
Senatskanzlei Amt für IT und Digitalisierung

Postanschrift: Rathausmarkt 1
20095 Hamburg

CUPOLA

Hamburg

Autor: Tobias Eggert
Stand: Mai 2024

Inhaltsverzeichnis

Einleitung

In Hamburg wurde Oktagon im Bauprüfbereich beginnend im Januar 2023 ausgerollt. Abschließend war es Absicht auch die Verfahren aus den Rechtsbereichen Wegerecht, Gewässeraufsicht und Naturschutz sowie die Beteiligungen am bauaufsichtlichen Verfahren in Oktagon umzusetzen, insbesondere, um die Genehmigung von Erteilungen zukünftig zu erleichtern und zu beschleunigen. Diese Arbeitsbereiche werden mit dem Akronym „SWAN“ („**S**ondernutzung“, „**W**asserrecht“, „**A**ufgrabescheine“, „**N**aturschutz“) bezeichnet.

Es arbeiteten insgesamt etwa 550 Mitarbeiter verteilt auf 23 Fachämter in den betroffenen Rechtsbereichen mit BACom. Es gab somit eine weite Bandbreite an Zielgruppen bzw. Anwendern, die an dem Projekt beteiligt waren.

Im Februar 2024 wurde entschieden die Umsetzung der Fachverfahren aus den Bereichen Naturschutz und Wasserrecht mittels Oktagon nicht weiter zu verfolgen, sondern hierfür eine Alternative zu nutzen, wodurch sich die Anzahl zu schulender Personen verringert hat (siehe Kapitel „Zielgruppen der Qualifizierung“). Das Akronym SWAN wird weiter beibehalten. Wie Beteiligungen umgesetzt werden befindet sich noch in Abstimmung. Sicher ist bereits, dass Beteiligungen zum Rollout-Zeitpunkt nicht mittels Oktagon umgesetzt werden.

Ziel des Dokuments

Das vorliegende Schulungskonzept hat folgende Ziele:

- Schaffung einer konzeptionellen Grundlage für die Planung und Umsetzung der Schulungen
- Definition der zu schulenden Zielgruppen
- Formulierung der Schulungsziele
- Identifizierung der passenden Schulungsformate
- Ausarbeitung eines zeitlichen Ablaufs (inklusive Roadmap)

Übersicht der Verfahren

Folgende Verfahren werden durch das Projekt Oktagon SWAN umgesetzt:

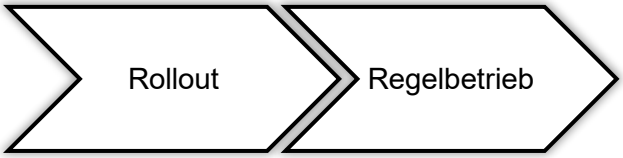
1. Zustimmung nach § 127 Abs. 1 TKG
2. Geringfügige bauliche Maßnahmen und Reparaturarbeiten nach § 127 Abs. 4 TKG
3. Aufgrabung mit Leitungsverlegung nach § 22 HWG
4. Aufgrabung ohne Leitungsverlegung nach § 22 HWG
5. Aufgrabung geringen Umfangs an bestehenden Leitungen nach HWG
6. Sondernutzungsverfahren nach HWG
7. Unerlaubte Sondernutzung nach HWG/FStrG
8. Benutzungserlaubnis nach § 4 GrünAnlG

Der Scope beinhaltet somit unterschiedliche Verfahrenstypen, die von Erlaubnis- bis hin zu Genehmigungsverfahren rangieren. Die Fallzahlen variieren somit ebenfalls und es wurde

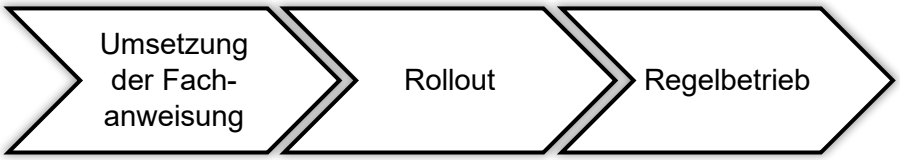
durch die Lenkungsgruppe des Programms Cupola eine Priorisierung für die Umsetzung festgelegt.

Übersicht der Qualifizierungsphasen

Im Rahmen der Einführung der Software Oktagon spielt eine nachhaltige und effektive Qualifizierung aller Beteiligten eine zentrale Rolle. Aus der Perspektive der Qualifizierungsplanung lassen sich folgende Phasen während der Einführung identifizieren:



Für den Bereich TAGS sind abweichend folgende Phasen vorgesehen:



Zielgruppen der Qualifizierung

Durch die unterschiedliche Strukturierung und Arbeitsweise der Bezirke und Dienststellen ergibt sich eine sehr heterogene Gruppe.

Anders als bei der Einführung von Oktagon Bau, wird es bei der Einführung von Oktagon SWAN keine expliziten Schulungen nach Rollenprofilen geben. Manche Zielgruppen haben bereits BACom genutzt und kennen die Arbeitsweise mit einer Software. Andere hingegen, arbeiten eher „traditionell“ mit Microsoft Word, abgespeicherten Texten bzw. Vorlagen und E-Mail. Für diese kann der Einstieg in das Arbeiten mit Oktagon herausfordernder sein.

Die Schulungen werden so gestaltet, dass bedarfsgerecht und dem zukünftigen Nutzungsgrad entsprechend qualifiziert wird. Es wird primär in Präsenz geschult. Begleitet wird die Präsenzschulung durch Online-Schulungsmaterial (Wiki, Handouts, Dokumentationen und Lernvideos). Vorteil des Letzteren ist, dass die Nutzer permanenten Zugriff auf diese Inhalte haben und sich diese auch mehrmals durchlesen bzw. ansehen, zu jeder Zeit stoppen oder die Dokumentation zur Schritt-für-Schritt Durchführung von Aktionen in Oktagon nutzen können.

	Sachbearbeiter	Grundlagen	Gebühren	Light
Teilnehmerzahl AGS & Trasse	59*	23*	6*	55*
Teilnehmerzahl Sondernutzung	91	31	2	41
Zielgruppe	Personen, deren tägliche Aufgabe es ist, Anträge zu bearbeiten	Führungskräfte und Personen, die nur einen Überblick zu den Grund-funktionen von g2vb+ und der eAkte benötigen	Personen, die zukünftig ausschließlich Gebühren in Oktagon berechnen	Personen, die sich primär mit der Einsicht von Akten beschäftigen (z.B. Wegewarte, Baustellen-koordinatoren)
Schulungsdauer AGS & Trasse	3 Tage	1 Tag	1 Tag	Videotutorials
Schulungsdauer Sondernutzung	2 Tage	1 Tag	1Tag	Videotutorials
Format	Präsenz	Präsenz	Präsenz	Digital

** Enthält Hochrechnung für den Bezirk Nord, basierend auf den durchschnittlich gemeldeten Teilnehmer:innenzahlen der anderen Bezirke.*

Spitzenorganisationen und Personalräte haben die Möglichkeit an Qualifizierungsmaßnahmen teilzunehmen (siehe Vereinbarung nach § 93 HmbPersVG).

Die Schulungen werden bezirksübergreifend angeboten, aber für die Fachbereiche getrennt, sodass es zu fachlichem Austausch über Bezirksgrenzen kommen kann. Flankiert werden die Schulungen von bedarfsorientiert stattfindenden User-Sprechstunden und einem Supportteam, welches bei Fragen und Problemen unterstützen soll. Floorwalking ist ein weiteres, optionales Angebot, welches bei Bedarf vom IT-BBZ angeboten und koordiniert wird.

Ziele der Qualifizierung

Vor diesem Hintergrund ist das übergeordnete Ziel der Qualifizierungsmaßnahmen, die Anwenderinnen und Anwender entsprechend ihrer Rolle zu einer selbstständigen und sicheren Erledigung ihrer fachlichen Aufgaben zu befähigen:

- Allen Beteiligten wird in Schulungen der Umgang mit der neuen IT-Lösung vermittelt. Die Anwender werden entsprechend der tatsächlichen Nutzung mit dem erforderlichen Handwerkszeug ausgerüstet, um die tägliche Arbeit mit Oktagon aufnehmen zu können – über den Eingang des Antrages und die Antragsprüfung bis hin zum Versenden des Bescheids.
- Die Anwender haben in praxisnahen und computergestützten Schulungen die Möglichkeit, sich an die neue Software schrittweise heranzutasten und konkrete Vorgänge des Antragsverfahrens in Oktagon auszuprobieren.
- Als sinnvolle Ergänzung fördert das Programm Cupola den Austausch und die Vernetzung untereinander. Die Teilnehmenden können sich über Fragen und Herausforderungen, die sie im Zusammenhang mit der Digitalisierung ihres Arbeitsplatzes bewegen, austauschen und ihre Erfahrungen mit anderen teilen.

- Durch eine individuelle Begleitung der Anwenderinnen und Anwender an ihrem Arbeitsplatz wird sichergestellt, dass auf Fragen, die sich bei der Anwendung der neuen IT-Lösung in der Anfangszeit ergeben, direkt reagiert werden kann.
- Die Lernangebote werden barrierefrei angeboten.
- Die Zusammenlegung von Trasse und Aufgrabeschein (TAGS) und die in diesem Rahmen entwickelte neue Fachanweisung (veränderter Genehmigungsprozess) bedarf eines etwas erweiterten Rahmens bzgl. der Schulungen. Diese zusätzlichen fachlichen Informationen werden den zuständigen Anwendern parallel zu den Oktagon Qualifizierungsmaßnahmen vermittelt. Geplant ist eine gemeinsame fachliche (neue Fachanweisung) und technische Schulung (Oktagon).

Schulungen während des Rollouts und im Regelbetrieb

Alle Teilnehmer des Bereichs TAGS werden noch vor der offiziellen Einführung der neuen Fachanweisung geschult. Das Projekt DigITAll wird für diesen Bereich eine für Prozessfragen zuständige Ressource als SPOC (eine benannte Person als Single Point of Contact) zur Verfügung stellen. Diese wird auch den Mitarbeitern vor Ort zur Verfügung stehen.

Während des Rollouts werden die Oktagon-Schulungen für die zu qualifizierenden Nutzer vom IT-BBZ durchgeführt und Schulungsunterlagen von diesem zur Verfügung gestellt. Die Teilnehmerlisten werden von den Ansprechpartnern in den Bezirken an das Projekt geschickt und von diesem aggregiert an das Schulungszentrum weitergeleitet. Die terminliche Organisation bzw. Buchung der Kurse für die genannten Zielgruppen läuft während des Rollouts über das IT-BBZ. Das Projekt übernimmt hier eine koordinierende und unterstützende Funktion.

Die Reihenfolge in welcher die Mitarbeiter geschult werden und Oktagon ausgerollt wird steht gegenwärtig noch nicht fest.

Zusätzlich zu den bestehenden Maßnahmen sollen während des Rollouts und zu Beginn des Regelbetriebs Austauschformate wie beispielsweise Sprechstunden und weitere Unterstützungsformate wie Floorwalking sowie digitale Lernmittel zur Verfügung gestellt werden, um den Übergang des Gelernten in die Arbeitspraxis zu unterstützen.

Im Regelbetrieb werden bei einem Neueinstieg in die Arbeitsbereiche oder bei einem anderweitigen Bedarf sachgemäß erneut (Nach-)Schulungen angeboten, um die nötige Qualifizierung für die entsprechende Tätigkeit sicherzustellen.

Evaluierung

Im Rahmen der Schulungen führt das IT-BBZ eine standardisierte, anonyme Befragung der Teilnehmer durch. Ziel der Befragung ist die Verbesserung der Schulungsangebote und des Schulungsmaterials für die nachfolgenden Schulungsphasen. Neben der Evaluierung durch das IT-BBZ sollen die Qualifizierungen nach einem Praxiszeitraum erneut evaluiert werden, um das erlernte Wissen im Kontrast zur Arbeitsrealität erfassbar zu machen.

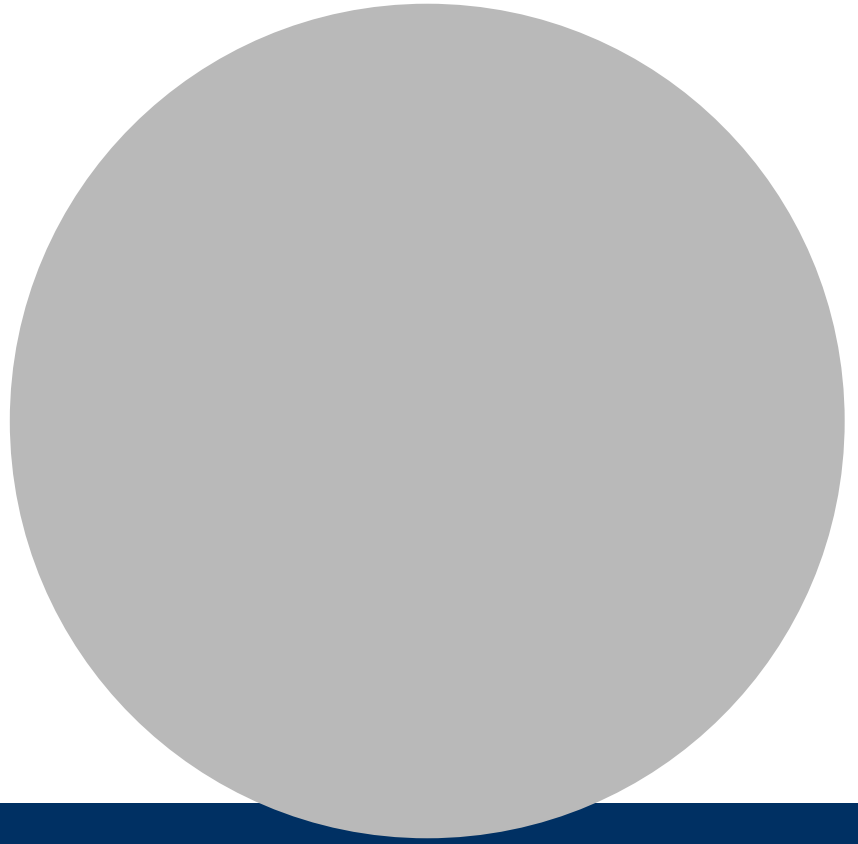
PROGRAMM CUPOLA

Qualifizierungskonzept Hunderegister

Stand: Februar 2022

Hamburg

QUALIFIZIERUNG ÜBERSICHT



Hamburg

ZIEL DER ANGEBOTE

NUTZERINNEN UND NUTZER KÖNNEN IHRE AUFGABEN EIGENSTÄNDIG IM NEUEN HUNDEREGISTER BEARBEITEN.

HIERZU WERDEN QUALIFIZIERUNGSANGEBOTE ZUR EINARBEITUNG BEREITGESTELLT SOWIE ANGEBOTE, DIE IM VERLAUF DER AUFGABENERFÜLLUNG UNTERSTÜTZEN.

ZIELGRUPPEN HUNDEREGISTER

Veterinärmedizinerinnen und -mediziner der Bezirke

Mitarbeitende der Kundenzentren

Polizeivollzugsdienststellen

Sachbearbeitung, Teamleitende & Führungskräfte

Hundekontroll-dienst

ZIELGRUPPEN HUNDEREGISTER

Sachbearbeitung

- Hauptanwendungsgruppe der neuen IT-Lösung.
- können alle Einträge im Hunderegister lesen und bearbeiten.
- haben Zugriff auf den Posteingang zum Online-Dienst. Eingeschränkt können sie neue Vorgänge nur einsehen und bearbeiten, wenn sie regional über die Ihnen zugeordnete Dienststelle berechtigt sind.

Teamleitende & Führungskräfte

- nutzen die Fachanwendung eher auf dem Supervisionslevel und steuern die Arbeit der Sachbearbeiter*innen.
- haben einen rein lesenden Zugriff auf vorhandene Registereinträge und damit auf die erstellten Dokumente sowie die zu Personen / Hunden erfassten Daten.

ZIELGRUPPEN HUNDEREGISTER

Mitarbeitende der Kundenzentren

- bearbeiten die analogen An- und Abmeldebegehren sowie Datenänderungen der Hamburger*innen vor Ort und pflegen diese live in das Hunderegister ein. Darüber hinaus dürfen Sie keine Eintragungen tätigen oder Änderungen vornehmen.
- können nur definierte Einträge im Hunderegister lesen und bearbeiten.

Veterinärmediziner:innen der Bezirke

- prüfen Daten und im Hunderegister hinterlegte Informationen für ihre Arbeit, bezirksabhängig obliegt ihnen auch die Aktualisierung der Daten.
- können alle Einträge im Hunderegister lesen, haben aber keinen Zugriff auf den Statistikbereich oder den Online-Dienst-Posteingang.

ZIELGRUPPEN HUNDEREGISTER

Hundekontrolldienst

- im gesamten Stadtgebiet Hamburg als Kontroll- und Vollzugsorgan zuständig und nutzt das Hunderegister mit lesendem Zugriff als Datenbank. Es werden u.a. der Leinenzwang sowie die rechtmäßige Haltung von Hunden, die als gefährlich eingestuft worden sind, überprüft.
- rein lesender Zugriff auf vorhandene Registereinträge und damit auf die erstellten Dokumente sowie die zu Personen / Hunden erfassten Daten.

Polizeivollzugsdienststellen

- können im Rahmen der Verfolgung von Straftaten und Ordnungswidrigkeiten konkrete Abfragen zu hunderelevanten Sachverhalten über das Hunderegister durchführen.
- können hierfür einzelne Datensätze aus dem Register entsprechend der gesetzlichen Vorgaben abfragen und diese ausschließlich lesen.

ZIELGRUPPEN HUNDEREGISTER

ADMIN Behörde

- kann alle Einträge im Hunderegister lesen und bearbeiten sowie auf den Statistikbereich zugreifen.
- hat Zugriff auf den Posteingang zum Online-Dienst. Hier können sie alle Vorgänge nur einsehen und bearbeiten, wenn sie regional über die Ihnen zugeordnete Dienststelle berechtigt sind.
- Zugriff auf den Admin-Bereich, um die Benutzer zu pflegen, Stammdaten zu ändern, etc.

AUFBAU & UMSETZUNG DER QUALIFIZIERUNGSANGEBOTE

02

Hamburg

RAHMENBEDINGUNGEN

QUALIFIZIERUNGSANGEBOTE SIND ZIELGRUPPENSPEZIFISCH.

QUALIFIZIERUNGSMAßNAHMEN ORIENTIEREN SICH AN DEN PROZESSSCHRITTEN DER BEARBEITUNG.

ANGEBOTE SIND PRAXISNAH UND BIETEN MÖGLICHKEIT ZUM ERPROBEN DER NEUEN SOFTWARE.

QUALIFIZIERUNG DER BETEILIGTEN PERSONEN FINDET IN FORM VON ELEARNING STATT.

Kombination aus 3-std. Schulung (Sachbearbeitung), 1,5-std. Präsentation (Mitarbeitende Kundenzentrum), Erklär-Videos und Skype-Sprechstunden. Qualifizierungsangebot durch User Experience Designer und Anforderungsmanager mit Kenntnissen zu Altverfahren in BACom.

INDIVIDUELLE QUALIFIZIERUNGSBEDARFE WERDEN DURCH MODULAREN AUFBAU DER ANGEBOTE UND MÖGLICHKEIT VON NACHSCHULUNGEN BERÜCKSICHTIGT.

Angebot der Nachschulungen wird in Schulungsterminen kommuniziert, Termin in erster Woche nach Einführung. Darüber hinaus dauerhaft verfügbare Qualifizierungsangebote wie Erklärvideos und Textanleitungen.

FÜR DIE SCHULUNGEN UND ERKLÄRVIDEOS WIRD EIN FEEDBACK EINGEHOLT.

QUALIFIZIERUNGSMODULE NACH ZIELGRUPPEN

	Sachbe-arbeitung	Führungs-kräfte	Admin Behörde	Externe Mitarbei-tende (EA)	Veterinär-mediziner-Innen Behörde	Hunde-kontroll-dienst	Polizei-vollzugs-dienststellen
Überblick und Grundlagen	X	X	X	X	X	X	
Anmeldung Hund inkl. Dokumente	X			X	(X)		
Datenänderung inkl. Dokumente	X						
Erlaubnisse inkl. Dokumente	X						
Vorfälle, Verstöße, Anordnungen	X						
Abmeldung inkl. Dokumente	X			X			
Posteingang inkl. Klärung	X						
Statistikbereich Hunderegister							
Datenabruf Polizei							X
Admin-Aufgaben Behörde			X				

QUALIFIZIERUNGSMODULE NACH FORMAT

	Dauerhafte Verfügbarkeit			Qualifizierungsangebote zur Einführung	
	Videoanleitung	**Textanleitung**		**Onlineschulung Sachbearbeitung**	**Präsentation Mitarbeitende Kundenzentren**
Überblick und Grundlagen	X	X		X	X
Anmeldung Hund inkl. Dokumente	X	X		X	X
Datenänderung inkl. Dokumente	X	X		X	X
Erlaubnisse inkl. Dokumente	X	X		X	-
Vorfälle, Verstöße, Anordnungen	X	X		X	-
Abmeldung Hund inkl. Dokumente	X	X		X	X
Posteingang inkl. Klärung	X	X		X	-
Statistikbereich Hunderegister	-	X		-	-
Datenabruf Polizei	-	X		-	-
Admin-Aufgaben Behörde	-	X		-	-

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Hamburg