Vereinbarung

nach § 93 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG)

zur Ergänzung

der Vereinbarung nach § 93 HmbPersVG über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS) vom 16. März 2022

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:

Nr. 1

Einrichtung eines neuen Workflows Polizei

Im Verfahren BMS wird ein neuer Workflow zur Abbildung des Auswahlprozesses Polizei mit erweiterten Anforderungen eingerichtet. Zur Abbildung dieses Workflows sind Ergänzungen zu den bestehenden Anlagen der Vereinbarung nach § 93 HmbPersVG über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS) vom 16. März 2022 (§93-Vereinbarung BMS) erforderlich. Diese Anlagen:

- 1.1 - Beschreibung der Verarbeitungstätigkeit
- 3.1 – Berechtigungskonzept
- 4.3 – Löschfristen
- 5.1 – Katalog der Schnittstellen

ergänzen die bestehenden Anlagen der §93-Vereinbarung BMS.

Sofern in diesen Anlagen 1.1, 3.1, 4.3 und 5.1 keine anderen Regelungen enthalten sind, gelten die Regelungen der §93-Vereinbarung BMS auch für den zusätzlichen Workflow Polizei.

Nr. 2

Schlussbestimmungen

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

Die Vereinbarung tritt am 1. November 2024 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.

Im Falle der Kündigung der Vereinbarung nach § 93 HmbPersVG über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS) vom 16. März 2022 tritt diese Vereinbarung wirkungsgleich mit dieser Vereinbarung außer Kraft.

In beiden Fällen werden die Partner der Vereinbarung unverzüglich Verhandlungen über den Abschluss einer neuen Vereinbarung aufnehmen.

Hamburg, den 14. Okt. 2024

Freie und Hansestadt Hamburg

für den Senat

Volker Wiedemann

dbb hamburg

beamtenbund und tarifunion

Thomas Treff

Deutscher Gewerkschaftsbund

-Bezirk Nord-

Olaf Schwede

Anlagen:

1.1 Ergänzung des bestehenden Anlage 1 – Beschreibung der Verarbeitungstätigkeit

3.1 Ergänzung der bestehenden Anlage 3 – Berechtigungskonzept

4.3 Ergänzung der bestehenden Anlage 4 – Löschkonzept

5.1 Ergänzung der bestehenden Anlage 5 – Katalog der Schnittstellen

.

Hamburg

Anlage 1.1 der Vereinbarung nach § 93 HmbPERSVG Vereinbarung über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS) – Ergänzung der bestehenden Anlage 1- Auswahlverfahren der Polizei

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:	22.07.2024	
	Ausfüllende Person:	Sacha Rülke	
	Telefonnummer:	040 / 4286-25112	
	Bezeichnung des Verfahrens:	Klicken Sie hier, um Text einzugeben.	
	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]:	Klicken Sie hier, um Text einzugeben.	
	Änderung bestehende Verarbeitung: **Überführung bestehende Verarbeitung in geltende Rechtslage nach DS-GVO:**	☒ ja ☐ ja	
	Neue Verarbeitung:	☐ ja	
	Abmeldung bestehende Verarbeitung[4]:		

[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

		☐ ja	
1. Grundsätzliche Angaben zur Verantwortlichkeit			
1.1	Verantwortliche Organisationseinheit[5] (optional):	Klicken Sie hier, um Text einzugeben.	
1.2	Vertreter der verantwortlichen Organisationseinheit (optional):	Klicken Sie hier, um Text einzugeben.	
1.3	Fachliche Leitstelle (bei IT-Verfahren) bzw. zuständige Stelle (bei nicht automatisierten Verfahren): Verantwortliche Führungskraft: Leitzeichen:	Klicken Sie hier, um Text einzugeben. Klicken Sie hier, um Text einzugeben. Klicken Sie hier, um Text einzugeben.	
1.4	Ansprechpartner, sofern nicht verantwortliche Führungskraft: Telefonnummer:	Klicken Sie hier, um Text einzugeben. Klicken Sie hier, um Text einzugeben.	
1.5	Name des Datenschutzbeauftragten (optional):	Klicken Sie hier, um Text einzugeben.	
1.6	Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt[6]: Auftragsnummer:	ELIGO Psychologische Personalsoftware GmbH	AVV Eligo

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung[7]			
2.1	Beschreibung und Zweckbestimmung der Verarbeitung von Daten[8]	Beschreibung der Verarbeitung: Klicken Sie hier, um Text einzugeben. Beschreibung der Zweckbestimmung: Wählen Sie ein Element aus. Sonstiges: Klicken Sie hier, um Text einzugeben.	
2.2	Rechtsgrundlage (Zutreffendes bitte ankreuzen und ggf. erläutern):		
☐	Spezialgesetzliche Regelung außerhalb der DS-GVO	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Klicken Sie hier, um Text einzugeben.	
☐	Einwilligung des Betroffenen (Art. 6 Abs. 1 a DS-GVO):	*Bitte fügen Sie die Einwilligungsklausel und den Einwilligungsmechanismus hier ein* Klicken Sie hier, um Text einzugeben.	
☐	Kollektivvereinbarung (z.B. Vereinbarung gem. HmbPersVG, Tarifvertrag)	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Klicken Sie hier, um Text einzugeben.	
☐	Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 4 HmbDSG n.F.)	Klicken Sie hier, um Text einzugeben.	

[5] Hinweis Nr. 5 der Anlage 1

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

☐	Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§ 10 HmbDSG n.F. und national geregelt im BDSG):	Klicken Sie hier, um Text einzugeben.	
☐	Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b DS-GVO)	Klicken Sie hier, um Text einzugeben.	
☐	Weitere:	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Klicken Sie hier, um Text einzugeben.	
3. Beschreibung betroffener Personen- und Datenkategorien			
3.1	Beschreibung der betroffenen Personengruppen[9]:	Wählen Sie ein Element aus. Sonstige: Klicken Sie hier, um Text einzugeben. Beschreibung: Klicken Sie hier, um Text einzugeben.	
3.2	Beschreibung der Art der Daten[10] bzw. Datenkategorien	Wählen Sie ein Element aus. Sonstige: - Angaben zu Beteiligungen an unerlaubten Handlungen (Straftaten/Owi) - Angaben zu Körpermodifikationen - Girokontodaten (auf welches Bezüge überwiesen werden sollen) - Ergebnisse von Eignungstests - Ergebnisse von Tauglichkeitsuntersuchungen - Angabe zum Dienstzweigwunsch	
3.3	Werden besondere Kategorien[11] von Daten verarbeitet (Art. 9 Abs. 1 DS-GVO)?	☒ ja, welche? biometrische Daten ☐ nein Bewerbende müssen ihre Körpergröße angeben (Mindestgröße gemäß Einstellungsrichtlinie der Polizei)	
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	

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

	Interne Stelle (Organisationseinheit)	1.) LKA7012 (Sicherheitsüberprüfung) 2.) PERS32 (Personalabteilung/ Personalaktenführung) 3.) PERS23 (Personalabteilung/ Eignungsdiagnostik) 4.) J1 (Justizariat) 5.) MMI Prüfer (MMI = Multimodales Interview)	
	Art der Daten	zu 1.) - Identifikationsdaten - Adressdaten der letzten 5 Jahre zu 2.) - Identifikationsdaten - Adressdaten - elektronische Kommunikationsdaten - schulische und berufliche Daten - Daten zu Bankkonten - Ergebnisse von Eignungstests - Ergebnisse körperliche Tauglichkeit - Angabe zu Dienstzweigwunsch - Personenstandsdaten zu 3.) - Identifikationsdaten (nur Geburtsjahr & Geschlecht) - schulische und berufliche Daten - Ergebnisse von Eignungstests - Angabe zu Dienstzweigwunsch zu 4.) Bekommen alle Kategorien übermittelt, welche für das Widerspruchsverfahren benötigt werden. zu 5.) - Identifikationsdaten - Ergebnisse von Eignungstests bei kurzfristiger Wiederbewerbung - schulische und berufliche Daten	
	Zweck der Daten-Mitteilung	zu 1.) Durchführung der notwendigen Sicherheitsüberprüfung (SÜ) zu 2.) Erstellung einer Personalakte bei Einstellung zu 3.) Analyse und Auswertung der Wirksamkeit der Eignungstest zu 4.) Bearbeitung der Widersprüche/Eilverfahren zu 5.) Durchführung der MMI Prüfung	
4.3	Externe Empfänger und Dritte	☐ ja ☐ nein	

	Externe Stelle	1.) ELIGO Psychologische Personalsoftware GmbH / Testanbieter Eignungsdiagnotik 2.) Universitätsklinikum Eppendorf - Athletikum KdöR / Durchführung Sporttest 3.) Personalärztlicher Dienst (PÄD) 4.) Staatsanwaltschaften 5.) Personalabteilungen Öffentlicher Dienst/ Bundeswehr	
	Art der Daten	zu 1.) Ergebnisse von Eignungstests & Erfassungsnummer aus BMS zu 2.) Identifikationsdaten & Erfassungsnummer aus BMS zu 3.) Identifikationsdaten & Erfassungsnummer aus BMS zu 4.) Identifikationsdaten, Adressdaten, Angaben zu möglichen Straftaten zu 5.) NUR im Bedarfsfall: Identifikationsdaten, Adressdaten	
	Zweck der Daten-Mitteilung	zu 1.) -Bereitstellung eines Onlinetestverfahrens für die Bewerber - Auswertung und Rückübermittlung der Ergebnisse ins BMS (für Evaluationszwecke ggf. Erweiterung um Alter/Geschlecht - weitere Anonymisierung bleibt bestehen) zu 2.) Bestandteil der Eignungsprüfung zu 3.) Bestandteil der Eignungsprüfung zu 4.) Bestandteil der Eignungsprüfung zu 5.) Bestandteil der Eignungsprüfung	
4.4	Geplante Datenübermittlung in Drittstaaten (außerhalb der EU) bzw. internationale Organisation	☐ ja ☐ nein	
	Drittstaat bzw. internationale Organisation	Klicken Sie hier, um Text einzugeben.	
	Art der Daten	Klicken Sie hier, um Text einzugeben.	
	Zweck der Daten Mitteilung	Klicken Sie hier, um Text einzugeben.	
	Welche geeigneten Garantien gem. Art. 46 DS-GVO werden im Zusammenhang mit der Übermittlung gegeben?	Garantien bestehen durch: ☐ verbindliche interne Datenschutzvorschriften, ☐ von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln	

		☐ von einer Aufsichtsbehörde genehmigte Vertragsklauseln	
	Bei Nichtvorliegen eines Angemessenheitsbeschlusses nach Art. 45 Abs. 3 DS-GVO und geeigneter Garantien nach Art. 46 DS-GVO: Welcher Ausnahmetatbestand nach Art. 49 Abs. 1 DS-GVO wird erfüllt?	Wählen Sie ein Element aus.	
5. Regelfristen für die Löschung der Daten[13]			
	Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Löschungsfristen?	☒ ja, falls ausgewählt bitte benennen: Bei absolut ungeeigneten Bewerbenden werden die erhobenen Daten so lange aufbewahrt, bis sie aufgrund der Altersgrenze als Bewerbende nicht mehr in Frage kommen. ☐ nein	
	Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:	Die Daten werden gemäß Löschkonzept (Anlage 4) und Ergänzung Löschkonzept der Polizei (Anlage 4.3) anonymisiert bzw. gelöscht.	
6. Mittel der Verarbeitung (optional) **Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?[14]**			
	Bezeichnung: Hersteller: Funktionsbeschreibung: Bereitstellung:	Elektronisches Eignungs- und Auswahlverfahren (eEAV) ELIGO Psychologische Personalsoftware GmbH Eine Software zur Durchführung von digitalen Eignungs- und Auswahltests ☐ Eigenentwickelte/ individuelle Software ☒ Standard-Software ☐ Cloud-Services ☐ Sonstige: Klicken Sie hier, um Text einzugeben.	
7. Zugriffsberechtigte Personengruppen (vereinfachtes Berechtigungskonzept)[15]			
	Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte Berechtigungskonzept:	Gemäß des Berechtigungskonzepts (Anlage 3) sowie der Ergänzung zum Berechtigungskonzept (Anlage 3.1).	
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?	☐ ☐ nein	
8.2	Die allgemeine Zielsetzung aus dem Rahmensicherheitskonzept wurde sichergestellt.	☐ ja ☐ nein, Abweichungen erläutern: Klicken Sie hier, um Text einzugeben.	

[13] Hinweis Nr. 13 der Anlage 1
[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 ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
8.4	Es wurden die Schutzbedarfsfeststellung und die Risikoprüfung gem. Art. 32 DS-GVO mittels Datenbank (Tool Schutzbedarfsfeststellung) durchgeführt und die Ergebnisse gem. Nutzungshinweisen ausgedruckt bzw. elektronisch gespeichert. Alternativ wurde analog (auf Papier) gem. der Darstellung aus dem BSI-Standard 200-2 eine Risikoprüfung durchgeführt.	☐ ja ☐ nein	
8.5	Es wurden die Erforderlichkeitsprüfung („Schwellwertanalyse“) und ggf. die Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO durchgeführt.	☐ ja ☐ 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 nicht bei Dataport gehostet werden: Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMs laut Anlage 2 sichergestellt.	☐ Es liegt kein Verfahren vor, das bei Dataport gehostet wird. ☐ Die Anlage 2 wurde ausgefüllt und liegt vor.	
8.8	Es liegen schriftlich vor	☐ interne Verhaltensregeln ☐ Schwellwertanalyse ☐ DSFA ☐ Risikoprüfung/ Schutzbedarfsfeststellung ☐ IT-Sicherheitskonzept ☐ Datenschutzkonzept ☐ Wiederanlauf- bzw. Notfallkonzept ☐ Sonstiges: Klicken Sie hier, um Text einzugeben.	
9. Datenübertragbarkeit[18] (Datenportabilität)			
	Nur bei - auf Grundlage einer Einwilligung- (s. 2.2) zur Verfügung gestellten Daten: Ist der Export der verarbeiteten Daten an den Betroffenen oder andere Dienste in einem gängigen, standardisierten Format möglich?	☐ ja, Format: Klicken Sie hier, um Text einzugeben. ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	

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

.

10. Informationen der Betroffenen[19]			
	Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?		
11. Sonstiges			
	Anmerkungen:	Die datenschutzrechtliche Betrachtung und Dokumentation zur Auftragsverarbeitung des Eignungs- und Auswahltestanbieters E-LIGO wurde separat vorgenommen und ist hier insofern nicht näher beschrieben.	

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

[19] Hinweis Nr. 19 der Anlage 1

.

Anlage 1**:**

Hinweise zum Formular

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

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

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

.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

.

.

Anlage 2

Übersicht und Erläuterungen zu den technischen und organisatorischen Maßnahmen

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

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

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

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

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

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

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

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

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

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

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

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

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

Maßnahmen zur Pseudonymisierung personenbezogener Daten

Hierzu zählen u. a.:

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

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

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

für den Schutz personenbezogener Daten eingesetzt werden.

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

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

Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste

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

Hierzu zählen u. a.:

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

.

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

Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste

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

Hierzu zählen u. a.:

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

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

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

Hierzu sind u. a. folgende Maßnahmen erforderlich:

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

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

Hierzu zählen u. a.:

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

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

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

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

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten

.

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

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

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

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

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

.
Anlage 3

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

Grundwerte nach DS-GVO	Definierte Technische und Organisatorische Maßnahmen (TOMs) nach § 64 BDSG	Ergriffene Technische und Organisatorische Maßnahmen (TOMs) der FHH
Datenminimierung Art. 5 Abs. 1 lit.c DS-GVO	-	Verwaltungsvorschrift IT-Projekte (bei kleineren IT-Projekten wird diese VV sinngemäß angewendet) Richtlinie über Mindestanforderungen an die Sicherheit der Datenverarbeitung auf UNIX-Rechnern (UNIX-Richtlinie)
Gewährleistung der **Integrität** Art. 32 Abs. 1 lit. b DS-GVO	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport, z.B. AD_Gruppenkonzept AD_Namenskonzept 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), z.B.Virenschutzkonzept FHH (ondataport.de), Bewertung und Verteilung Sicherheitspatches_FHH.pdf (ondataport.de), Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Geschäftsbestimmungen der Behörden (Revisionfähige Prozessbeschreibungen, Überprüfbarkeit des Verwaltungshandelns) Vorgaben zum Endgerätebetrieb
	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 Telekommunikationsrichtlinie (ondataport.de)
	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 3.1 der Vereinbarung nach § 93 HmbPersVG Vereinbarung über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS) – Ergänzung der bestehenden Anlage 3 - für Auswahlverfahren der Polizei

Projekt “Bewerbungsmanagementsystem Einführung“

Berechtigungskonzept

AK Einstellungsstelle Polizei Hamburg

AK02 – Überseering 35, 3. Stock

Version: 1.1

Stand: 24.07.2024

Rollen und Rechte auf Metaebene

- AK Einstellungsstelle Polizei Hamburg -

Inhalt

1 Übersicht

Dieses Dokument beschreibt die Rechte der Rollen in der BeeSite auf Metaebene. Die Rechte beziehen sich hierbei jeweils auf die Objekte **Projekt**, **Vakanz**, **Stellenanzeige** und **Bewerbung**.

Rolle	Kurzbezeichnung
Administrator = FL ZPD	**A**
Recruiter	**R**
Grundsatz	**G**
Hotline	**HL**
Dienststellenleitung Einstellungsstelle AK02	**DSL**
Sachgebietsleitung Einstellungsstelle AK02	**SGL**
Justizariat J22	**J**
Personalrat	**PR**
Schwerbehindertenvertretung	**SBV**
Gleichstellungsbeauftragte	**GSB**
Personalsachbearbeiter (PERS3)	**PSB**

2 Projekt

Recht	Konstante	A	R	G	HL	DSL	SGL	J	PR	SBV	GSB	PSB
Anlegen	OBJECT_ACTION_PROJECT_NEW	x										
Einsehen	OBJECT_ACTION_PROJECT_READ	x	x									
Bearbeiten	OBJECT_ACTION_PROJECT_EDIT	x										
Einsicht alle Projekte	OBJECT_ACTION_PROJECT_INSPECT	x	x									
Auflisten	OBJECT_ACTION_PROJECT_LIST_VIEW	x	x									
Vakanz anlegen	OBJECT_ACTION_PROJECT_VACANCY_CREATE	x	x									
Vakanz-Desktop	OBJECT_ACTION_PROJECT_VACANCY_DESKTOP	x	x									
Bewerbungen Export	OBJECT_ACTION_PROJECT_CANDIDATE_EXPORT	x										
Erinnerung hinzufügen	OBJECT_ACTION_PROJECT_REMINDER_CREATE	x										
Historie einsehen	OBJECT_ACTION_PROJECT_HISTORY_READ	x										

3 Vakanz

Recht	Konstante	A	R	G	HL	DSL	SGL	J	PR	SBV	GSB	PSB
Anlegen	OBJECT_ACTION_VACANCY_NEW	x	x				x					
Einsehen	OBJECT_ACTION_VACANCY_READ	x	x			x	x	x	x	x	x	x
Bearbeiten	OBJECT_ACTION_VACANCY_EDIT	x	x				x					
Weiterleiten	OBJECT_ACTION_VACANCY_FORWARD	x	x				x					
Als Vorlage speichern	OBJECT_ACTION_VACANCY_SET_TEMPLATE	x	x				x					
Als Vorlage benutzen	OBJECT_ACTION_VACANCY_USE_TEMPLATE	x	x				x					
Verschieben	OBJECT_ACTION_VACANCY_CHANGE_RELATED_PROJECT	x	x				x					
Kopieren	OBJECT_ACTION_VACANCY_COPY	x	x				x					
Besitzer ändern	OBJECT_ACTION_VACANCY_CHANGE_OWNER	x	x				x					
Auflisten	OBJECT_ACTION_VACANCY_LIST_VIEW	x	x			x	x	x	x	x	x	x
Stellenanzeigen-Desktop	OBJECT_ACTION_VACANCY_JOBAD_DESKTOP	x	x				x					

Kandidaten-Desktop	OBJECT_ACTION_VACANCY_CANDIDATE_DESKTOP	x	x				x					
Bewerbung anlegen	OBJECT_ACTION_VACANCY_CANDIDATE_CREATE	x	x				x					
Stellenanzeige anlegen	OBJECT_ACTION_VACANCY_JOBAD_CREATE	x	x				x					
Erinnerung hinzufügen	OBJECT_ACTION_VACANCY_REMINDER_CREATE	x	x				x					
Terminübersicht	OBJECT_ACTION_VACANCY_EVENT_LIST_VIEW_ALL	x										
Historie ansehen	OBJECT_ACTION_VACANCY_HISTORY_READ	x	x				x					
Kandidaten Export	OBJECT_ACTION_VACANCY_CANDIDATE_EXPORT	x										
Workflow ändern	OBJECT_ACTION_VACANCY_EDIT_CANDIDATE_WORKFLOW_TYPE	x	x				x					
Status ändern		x	x				x					

4 Stellenanzeige

Recht	Konstante	A	R	G	HL	DSL	SGL	J	PR	SBV	GSB	PSB
Anlegen	OBJECT_ACTION_JOBAD_NEW	x	x				x					
Einsehen	OBJECT_ACTION_JOBAD_READ	x	x	x	x	x	x	x	x	x	x	x
Bearbeiten	OBJECT_ACTION_JOBAD_EDIT	x	x				x					
Weiterleiten	OBJECT_ACTION_JOBAD_FORWARD	x	x				x					
Als Vorlage speichern	OBJECT_ACTION_JOBAD_SET_TEMPLATE	x	x				x					
Als Vorlage benutzen	OBJECT_ACTION_JOBAD_USE_TEMPLATE	x	x				x					
Auflisten	OBJECT_ACTION_JOBAD_LIST_VIEW	x	x	x	x	x	x	x	x	x	x	x
Erinnerung hinzufügen	OBJECT_ACTION_JOBAD_REMINDER_CREATE	x	x				x					
Historie ansehen	OBJECT_ACTION_JOBAD_HISTORY_READ	x	x		x		x					

Dokument erzeugen	OBJECT_ACTION_JOBAD_CREATE_DOCUMENT											
Status ändern		x	x				x					

5 Bewerbung

Recht	Konstante	A	R	G	HL	DSL	SGL	J	PR	SBV	GSB	PSB
Neu anlegen	OBJECT_ACTION_CANDIDATE_NEW	x	x	x			x					
Einsehen	OBJECT_ACTION_CANDIDATE_READ	x	x	x	x	x	x	x	x	x	x	x
Bearbeiten	OBJECT_ACTION_CANDIDATE_EDIT	x	x	x	x		x					
Weiterleiten	OBJECT_ACTION_CANDIDATE_FORWARD	x	x	x			x		x	x	x	x
Kontaktieren	OBJECT_ACTION_CANDIDATE_CONTACT	x	x	x	x		x					
Kontaktieren (Massenaktion)	OBJECT_ACTION_CANDIDATE_CONTACT_MASS	x	x				x					
Vakanz ändern	OBJECT_ACTION_CANDIDATE_CHANGE_RELATED_VACANCY	x	x				x					
Auflisten	OBJECT_ACTION_CANDIDATE_LIST_VIEW	x	x	x	x	x	x	x	x	x	x	x
Sichtbar in Bewerbersuche	OBJECT_ACTION_CANDIDATE_GREATGROUPS	x	x		x		x					
Bewerbung kopieren	OBJECT_ACTION_CANDIDATE_COPY	x	x				x					
FE-Account anlegen	OBJECT_ACTION_CANDIDATE_CREATE_ACCOUNT	x	x		x		x					
Kommentar löschen	OBJECT_ACTION_CANDIDATE_COMMENT_DELETE	x	x		x		x					
Kommentar einsehen	OBJECT_ACTION_CANDIDATE_COMMENT_READ	x	x	x	x	x	x	x	x	x	x	x
Kommentar anlegen	OBJECT_ACTION_CANDIDATE_COMMENT_NEW	x	x	x	x	x	x	x	x	x	x	x
Kommentar senden	OBJECT_ACTION_CANDIDATE_COMMENT_SAVE_AND_SEND				x							
Stellenanzeige ändern	OBJECT_ACTION_CANDIDATE_CHANGE_RELATED_JOBAD	x	x				x					
Vollständige Doublettenliste	OBJECT_ACTION_CANDIDATE_DOUBLETLIST_SHOWALL	x			x							
Junkmail lesen	OBJECT_ACTION_CANDIDATE_JUNKMAIL_READ	x	x		x		x					

Historie ansehen	OBJECT_ACTION_CANDIDATE_OVERALL_HISTORY_READ	x	x	x	x	x	x	x	x	x	x	
Termin vereinbaren	OBJECT_ACTION_CANDIDATE_EVENT_INVITATION	x	x		x		x					
Termin vereinbaren (Massenaktion)	OBJECT_ACTION_CANDIDATE_EVENT_INVITATION_MASS	x	x				x					
Einladungsübersicht	OBJECT_ACTION_CANDIDATE_EVENT_LIST_VIEW_ALL	x	x		x		x					
Anhangstyp ändern	OBJECT_ACTION_CANDIDATE_FILE_CHANGE_ATTACHMENT_TYPE	x	x		x		x					
Dossier öffnen	OBJECT_ACTION_OPEN_DOSSIER	x	x	x	x	x	x	x	x	x	x	x
Datei hochladen	OBJECT_ACTION_CANDIDATE_EVENT_INVITATION_FILE_UPLOAD	x	x	x	x		x					
Datei herunterladen	OBJECT_ACTION_CANDIDATE_DOWNLOAD_UPLOADED_ATTACHMENTS	x	x	x	x		x					
Dokument erzeugen	OBJECT_ACTION_CANDIDATE_CREATE_DOCUMENT	x	x	x	x		x					
Dokument erzeugen (Massenaktion)	OBJECT_ACTION_CANDIDATE_CREATE_DOCUMENT_MASS	x	x									
Erinnerung hinzufügen	OBJECT_ACTION_CANDIDATE_REMINDER_CREATE	x	x	x	x		x					
HR-Ranking	OBJECT_ACTION_CANDIDATE_RANKING_HR											
FB-Ranking	OBJECT_ACTION_CANDIDATE_RANKING_DEPARTMENT											
Export CSV	OBJECT_ACTION_CANDIDATE_EXPORT_CSV	x	x		x		x					
Export CSV (Massenaktion)	OBJECT_ACTION_CANDIDATE_EXPORT_CSV_MASS	x			x							
Talentpool hinzufügen	OBJECT_ACTION_CANDIDATE_ADD_TO_POOL_MASS	x	x				x					
Bewerbungsvergleich	OBJECT_ACTION_CANDIDATE_COMPARE_MATRIX_MASS											

Anlage 4.3 der Vereinbarung nach § 93 HmbPERSVG Vereinbarung über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS) – Ergänzung der bestehenden Anlage 4.2 - für Auswahlverfahren der Polizei

Projekt

Bewerbermanagement Einführung (BMS)

Löschfristen

AK Einstellungsstelle Polizei Hamburg

AK02 – Überseering 35, 3. Stock

Version: 1.1

Stand: 24.07.2024

II. Löschfristen

Objekt	Beispiel, Anwendungsfall	Auslöser	Aktion	Start[1]	Frist[2]	Allgemeines, Hintergrund
Bewerbung (extern)	Status wird auf „absolut ungeeignet“ gesetzt.	Statuswechsel auf „Absolut ungeeignet“	Wiedervorlage	Status gesetzt	mindestens[3] 400 Tage	Grundsätzlich sind Bewerberdaten zu löschen, sobald ihre Speicherung für die Bewerbung nicht mehr erforderlich ist. Die Löschroutine muss deshalb grundsätzlich zeitnah erfolgen. Die Daten eines Bewerbenden, der am Ende des Bewerbungs-prozesses den Status „absolut ungeeignet“ erhält, dürfen gemäß des - § 10 HmbDSG, § 85 HmbBG bis zu 3 Jahre - teilweise sogar darüber hinaus - gespeichert werden. Mit dieser Ausnahme stellt die AK Einstellungsstelle der Polizei Hamburg sicher, dass absolut ungeeignete Personen von einer Wiederbewerbung ausgeschlossen werden können, solange diese nicht die gesetzliche Altersgrenze erreicht haben. Diese Bewerbungen werden durch den Status „absolut ungeeignet“ auf eine Wiedervorlageliste gesetzt, um diese in regelmäßigen Abständen zu überprüfen. Ist nach einer Prüfung kein Grund mehr gegeben, die Daten des Bewerbenden weiter im Status „absolut ungeeignet“ aufzubewahren, bekommt der Bewerbende den Status „Anonymisieren“ und wird mit einer Frist von 30 Tagen anonymisiert. Folgende Ausnahmen sind zulässig: - > 3 Wiederbewerbungen innerhalb von 5 Jahren - Feststellung einer persönlichen oder charakterlichen Nichteignung

[1] Startzeitpunkt, ab dem die Regellöschfrist läuft

[2] Frist = Regellöschfrist (Aufbewahrungsfrist). Die Aufbewahrungszeit einer Bewerbung sollte in der Regel sechs Monate nicht überschreiten. Die Abweichung hier ergibt sich aus der längeren Einspruchsfrist des Beamtenrechts. Für Angestellte gilt: Ein abgelehnter Bewerber muss derzeit eine Diskriminierung im Bewerbungsverfahren innerhalb von zwei Monaten nach der Ablehnung schriftlich geltend machen. Eine daran anschließende Klage muss gemäß § 61 Abs. 1 ArbGG i.V.m. § 15 AGG innerhalb von drei Monaten, nachdem der Anspruch schriftlich geltend gemacht worden ist, erhoben werden

[3] Das „mindestens“ ist wie folgt zu verstehen: Im Widerspruchs- bzw. Klagefall wird die betreffende Vakanz von Hand durch den Recruiter oder Administrator auf den Status „Rechtsstreit“ gesetzt. Das weitere Hochzählen der Löschfrist wird damit ausgesetzt, bis das Verfahren entschieden ist. Daraufhin wird vom Recruiter oder Administrator der neue Status „Rechtsstreit beendet“ gesetzt. Das System ermittelt nun die Differenz zwischen der Regellöschfrist 400 Tage und der Dauer vom Beginn der Ausschreibung bis zum Statuswechsel „Rechtsstreit beendet“, um die verbleibende Speicherdauer zu ermitteln. Die Anzahl der verbleibenden Speichertage beträgt aus Gründen der Verfahrensdokumentation mindestens 30 Tage, ggf. füllt das System die verbleibenden Speichertage entsprechend auf

Anlage 5.1 der Vereinbarung nach § 93 HmbPERSVG Vereinbarung über den laufenden Betrieb, die Nutzung und die Weiterentwicklung des IT-Verfahrens Bewerbungsmanagementsystem (BMS) – Ergänzung der bestehenden Anlage 5 - für Auswahlverfahren der Polizei

BMS

Katalog der Schnittstellen

Lfd. Nr.	Bezeichnung der Schnittstelle	Fachlicher Hintergrund	Art der Schnittstelle	Transport	Liefersystem	Zielsystem	Periodizität	Arten der Daten
3	ELIGO-Eignungsdiagnostikexport	Die Erfassungs-nummer aus dem BMS wird im Einstellungsverfahren an ELIGO für die Eignungs- und Auswahltests übergeben, sodass die Bewerbenden dort ihren Einstellungstest durchführen. Die Testergebnisse werden von ELIGO für das BMS zur Abholung bereitgestellt, sodass die Ergebnisse im BMS am Bewerbenden gespeichert werden können.	Webservice	XML	BMS – für Erfassungsnummer ELIGO – für Testergebnisse	ELIGO – für Testerstellung für Erfassungsnummer BMS – für Testergebnisse	Täglich während der Verfahrenszeiträume	Erfassungsnummer Nummerische Testergebnisse und Ergebnis: bestanden/nicht bestanden