KoPers

Datenschutzfolgenabschätzung mit Beschreibung der Verarbeitungsvorgänge

Anlage 1

Datenschutzfolgenabschätzung (Art. 35 DS-GVO)

Verarbeitungstätigkeit:

IT-Vorhabensnummer: APP-2817

IT-Kurzbezeichnung: KoPers Aktive und Passive

Zu Blatt-Nr.:

Von der Verzeichnisführenden Stelle auszufüllen!

Prüfpunkte		Ausführungen und Hinweise	
Allgemeines			
1.	Werden im Verfahren personenbezogene Daten automatisiert verarbeitet?	Wenn ja, dann weiter bei 2. Wenn nein, keine weitere Überprüfung notwendig	☒ ja ☐ nein
Erforderlichkeitsprüfung einer Datenschutzfolgenabschätzung („Schwellwertanalyse“)			
2.	Liegt ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen oder eines der folgenden Kriterien vor, welche auf die Erforderlichkeit der Durchführung einer DSFA hinweisen (Art. 35 Abs. 1 DS-GVO)? • der Einsatz einer neuen Technologie • die Verwendung neuer Vorgänge der Datenverarbeitung • die Verarbeitung einer hohen Anzahl von Daten • eine hohe Anzahl betroffener Personen	Wenn ja, Beschreibung und weiter bei 5. Wenn nein, weiter bei 3. Es werden in KoPers auch sensible Daten verarbeitet, wie z. B. religiöse Bekenntnisse, Gesundheitsdaten, sexuelle Orientierung ☐ ☐ ☒ ☒	☒ ja ☐ nein
3.	Liegt ein Tatbestand aus Art. 35 Abs. 3 DS-GVO vor? • Systematische und umfassende Bewertung persönlicher Aspekte • Umfangreiche Verarbeitung besondere Kategorien von personenbezogenen Daten • Überwachung öffentlich zugänglicher Bereiche	Wenn ja, Beschreibung und weiter bei 5. Wenn nein, weiter bei 4. ☐ ☒ ☐	☒ ja ☐ nein
4.	Liegt ein Erforderlichkeitsgrund gemäß den Vorgaben des Hamburgischen	Das Vorhalten von Daten im Personalinformationssystem mit Schutzbedarf „hoch“.	☒ ja ☐ nein

Prüfpunkte		Ausführungen und Hinweise	
	Beauftragten für Datenschutz und Informationsfreiheit vor (Art.35 Abs. 4 DS-GVO)?		
Vorbereitung			
5.	Wurde ein geeignetes Durchführungsteam erstellt, welches objektiv und zielgerichtet arbeiten kann?	Das Team sollte bestehen aus, • Personal mit Erfahrungen und Kompetenzen im Bereich des Datenschutzes, des Risikomanagements und des datenverarbeitungsprogrammspezifischen Prozessmanagements • Projektverantwortlichen und • Projektunabhängigen, welche die Objektivität wahren können Es wurde ein nicht institutionalisiertes Durchführungsteam aus Vertretern von Projekt KoPers und ZPD 3 in Arbeitsgruppenstruktur zusammengestellt.	☒ ja
6.	Wurde der Datenschutzbeauftragte der Einrichtung gem. Art. 35 Abs. 2 DS-GVO beratend hinzugezogen1?	☒ ja ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
7.	Wurden die Grundsätze für die Verarbeitung personenbezogener Daten betrachtet (Art. 5 DS-GVO)? ☒ Rechtmäßigkeit ☒ Treu und Glauben ☒ Transparenz ☒ Zweckbindung ☒ Datenminimierung ☒ Speicherbegrenzung	☒ ja ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
8.	Wurden die Rahmenbedingungen für die Durchführung festgelegt?	Erst dann weiter bei 9.	☒ ja
8.1	Wurde eine systematische Beschreibung der Verarbeitungstätigkeit mit Zweckbestimmung angefertigt[2]?	Die Verarbeitungsvorgänge müssen ausführlich und abschließend mit allen Datenflüssen beschrieben werden. Wesentlich ist es, die beabsichtigten Zwecke der Verarbeitungsvorgänge festzuhalten. ☒ ja ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
8.2	Wurden die Verarbeitungsvorgängen in Bezug auf ihren Zweck auf Notwendigkeit bzw. Verhältnismäßigkeit bewertet?	☒ ja ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	

[1] Anlage 1: Hinweis Nr. 2

[2] Anlage 1: Hinweis Nr. 3

Prüfpunkte		Ausführungen und Hinweise	
8.3	Wurde ein Rechte- und Rollen-Konzept bzw. Berechtigungskonzept erstellt?	Rechte, Rollen und Pflichten der beteiligten Akteure müssen festgehalten werden. ☒ ja ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
8.4	Wurde eine Risikoprüfung mit der Schutzbedarfsfeststellung durchgeführt?	☒ ja[3] ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben. Erläuterungen: Dazu gehören der mögliche Umgang mit Risiken und die Feststellung des Schutzbedarfs. Für den Umgang mit Risiken gibt es u.a. folgende Möglichkeiten: • Risiko minimieren, • Risiko akzeptieren, • Risiko vermeiden oder • Risiko übertragen Für die Schutzbedarfskategorien kann sich am BSI orientiert werden. Folgende Kategorien sind sinnvoll: • normal • hoch • sehr hoch	
8.5	Wurden die folgenden Datenschutzziele betrachtet?	Die drei unabdingbaren Schutzziele gemäß BSI wurden betrachtet: ☒die Vertraulichkeit, ☒die Verfügbarkeit ☒die Integrität der Daten. Darüber hinaus wurden die Gewährleistungsziele nach bestehendem Datenschutzrecht betrachtet: ☒ die Datenminimierung, ☒ die Intervenierbarkeit, ☒ die Transparenz, ☒ die Nichtverkettung.	☒ ja ☐ nein
Durchführung			
9.	Wurden alle möglichen Risikoquellen identifiziert und	Zu Risikoquellen gehören u.a. externe Angreifer, Technikversagen (berücksichtigen, dass Fehler auch erst	☒ ja ☐ nein

[3] Anlage 1: Hinweis Nr.1

Prüfpunkte		Ausführungen und Hinweise	
	mit einem Schutzziel (s. Punkt 8.5) versehen?	während des laufenden Betriebs auftreten können) und menschliches Versagen des Anwenders. Siehe Risikoanalyse gem. § 9 HmbDSG (alte Fassung) vom 21.03.2018.	
10.	Wurde jedes identifizierte Risiko bewertet?	s. Punkt 8.4 Ausführung zu Schutzbedarfsfeststellung Die Bewertung erfolgt unter der Beachtung von Eintrittswahrscheinlichkeit, Höhe und Schwere des Schadens. Klicken Sie hier, um Text einzugeben.	☒ ja ☐ nein
11.	Wurde der Umgang mit dem jeweiligen Risiko festgelegt?	s. Punkt 8.4 Ausführung zu Umgang mit Risiken Entscheidet man sich dafür, ein Risiko zu akzeptieren, muss eine verantwortliche Person dies unterzeichnen. Es muss überprüft werden, ob diese Entscheidung wirklich wirksam ist. Es wird die Entscheidung getroffen, alle Restrisiken zu tragen. Die mit dem Verfahren verbundenen Gefahren werden durch die beschriebenen technischen und organisatorischen Maßnahmen wirksam beherrscht.	☒ ja ☐ nein
12.	Sind Maßnahmen (Technische und Organisatorische Maßnahmen TOMs) für die Risiken abgeleitet worden[4]?	Maßnahmen können aus bereits eingesetzten Maßnahmen abgeleitet werden. Die Maßnahmen dürfen nicht gegen rechtliche Vorgaben verstoßen und im Rahmen der zugewiesenen Ressourcen ausgewählt werden.	☒ ja ☐ nein
12.1	**Pseudonymisierung** (z.B. Verwendung Personalnummer oder E-Mail ohne Nennung von Klarnamen)	Für die Erfordernisse der Bewirtschaftung bzw. Sachbearbeitung sind die Originaldaten zwingend erforderlich. Die Inhalte von Statistiken sind grundsätzlich kumulativer Art. Ein Rückschluss auf Einzelpersonen ist ausgeschlossen.	
12.2	**Verschlüsselung** (z.B. Umwandlung in eine nicht lesbare Form durch elektronische Codes)	Verschlüsselung der Datenbank mit Oracle TDE, Verschlüsselung der Client-Anbindung über https.	
12.3	Gewährleistung der **Verfügbarkeit** (z.B. über SSLA mit IT-Dienstleister absicherbar)	Verfügbarkeit: Montag bis Donnerstag 7-17 Uhr und Freitag 7-15 Uhr, vertraglich mit Dataport vereinbart	
12.4	Gewährleistung der **Integrität** (z.B. über Berechtigungs-/ Zugriffskonzepte)	Siehe KoPers-Berechtigungs- und Zugriffskonzept.	
12.5	Gewährleistung der **Vertraulichkeit** (z.B. über Einschränkung bei Zugriffsrechten)	Siehe KoPers-Berechtigungs- und Zugriffskonzept.	

[4] Anlage 2: Erläuterungen zu den TOMs

Prüfpunkte		Ausführungen und Hinweise	
12.6	Gewährleistung der **Belastbarkeit der Systeme** (z.B. über Zurverfügungstellung einer ausreichenden Bandbreite und entsprechender Hardwareausstattung)	Gewährleistung der Belastbarkeit der Systeme durch entsprechende Hardwaredimensionierung und parallele Strukturen (u. a. unter Einsatz von Loadbalancing)	
12.7	Verfahren zur **Wiederherstellung der Verfügbarkeit** personenbezogener Daten nach einem physischen oder technischen Zwischenfall (siehe SLA (Notfallkonzept) mit Dataport)	Kontinuierliche Sicherung der KoPers-Datenbank (Oracle R_Man-Sicherung).	
12.8	Verfahren **regelmäßiger Überprüfung**, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (z.B. Nachweis per Zertifizierung)	Stichprobenprüfung der eingerichteten Benutzerrechte auf der Basis von KoPers-Auswertungen	
12.9	**Datenminimierung** (z.B. es werden nur notwendige Daten erhoben und verarbeitet)	Für die Erfordernisse der Bewirtschaftung bzw. Sachbearbeitung sind die im vorliegenden Datenkatalog aufgeführten Daten zwingend erforderlich.	
12.10	**Intervenierbarkeit** (z.B. durch die Verarbeitung zwingend erforderlicher Daten)	Merkblatt anlässlich DSGVO (Einsichtnahme, Einspruchsrecht, „keine Verwendung für weitere Zwecke“)	
12.11	**Transparenz** (z.B. durch Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzeptes)	Merkblatt anlässlich DSGVO (Einsichtnahme, Einspruchsrecht, „keine Verwendung für weitere Zwecke)	
12.12	**Nichtverkettung** (z.B. durch programmtechnische Unterlassung von Schnittstellen)	Verkettung für weiter personalwirtschaftliche Zwecke erforderlich, z. B. Zeitwirtschaftssystem SP Expert – siehe auch Merkblatt anlässlich DSGVO (Einsichtnahme, Einspruchsrecht, „keine Verwendung für weitere Zwecke)	
13.	Wurden die Rahmenbedingungen für die Umsetzung festgelegt?	Folgendes sollte festgelegt werden: • die Verantwortlichen für die Umsetzung, • der Zeitpunkt bis zur Umsetzung und • die zur Verfügung stehenden Mittel Verantwortlich ist die Projektleitung ePers. Zeitplanung und stufenweise Umsetzung, Mittel gemäß Bürgerschaftsdrucksachen E-Pers.	☒ ja ☐ nein
Umsetzung der Maßnahmen			
14.	Konnten alle Maßnahmen umgesetzt werden?	Wenn ja, weiter bei 17. Wenn nein, weiter bei 15. Aufgrund der getroffenen Maßnahmen sind die Risiken beherrschbar.	☒ ja ☐ nein

Prüfpunkte		Ausführungen und Hinweise	
15.	Wurden alternative Maßnahmen identifiziert und umgesetzt?	Wenn ja, weiter bei 17. Wenn nein, weiter bei 16. Klicken Sie hier, um Text einzugeben.	☐ ja ☐ nein
16.	Wurde die Aufsichtsbehörde gem. Art. 36 DS-GVO konsultiert und nach ihren Empfehlungen gehandelt?	Bleiben Restrisiken, müssen diese aufgeführt werden. Klicken Sie hier, um Text einzugeben.	☐ ja ☐ nein

Anlage 1: Hinweise zum Formular

Hinweis Nr.1
Bei Überführung in neue Rechtslage: Es kann die bereits im Rahmen der Risikoanalyse durchgeführte Schutzbedarfsfeststellung übernommen werden und muss nicht neu durchgeführt werden.

Hinweis Nr. 2
Der Datenschutzbeauftragten hat nicht die Aufgabe, die DSFA anzustoßen, durchzuführen oder das Ergebnis zu beurteilen. Der Datenschutzbeauftragte steht mit Rat zur Seite und überwacht die Durchführung gem. Artikel 35 DS-GVO.

Hinweis Nr. 3
Die Beschreibung kann beispielsweise in einer Tabelle (Phase des Prozess, detaillierte Beschreibung der Phase, relevante Informationssysteme, weitere unterstützende Werte) verbal erfolgen oder als Datenfluss-Diagramm grafisch.

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>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 Depseudonymisierungsvorgänge

- zufällige Erzeugung der Zuordnungstabellen oder der in eine algorithmische Pseudonymisierung 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 Lebenszyklus
- 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

Beschreibung der Verarbeitungsvorgänge

Blatt-Nr.:

300, 1.301, 1.303, 1.304, 1.307, 1.308 1.313, 1.314, 1.315, 1.318 , 1.319

(Bitte an die Verzeichnisführende Stelle absenden!)

Nur auszufüllen, wenn personenbezogene Daten[5] verarbeitet werden!

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

Allgemeines			
	Datum:	Klicken Sie hier, um ein Datum einzugeben.	
	Ausfüllende Person:		
	Telefonnummer:		
	Bezeichnung des Verfahrens:	KoPers Aktive und Passive	
	Bezeichnung der Verarbeitung[6]:	☐ Erheben ☒ Erfassen ☒ Organisieren ☒ Ordnen ☒ Speichern ☐ Anpassen oder Verändern ☒ Auslesen ☒ Abfragen ☒ Verwenden ☒ Offenlegen durch Übermittlung, Verbreitung oder andere Form der Bereitstellung ☐ Abgleichen oder die Verknüpfen ☐ Einschränken ☒ Löschen ☐ Vernichten	
	Beginn der Verarbeitung[7]:	01. Oktober 2014	

[5] Hinweis Nr. 1 der Anlage 1
[6] Hinweis Nr. 2 der Anlage 1
[7] Hinweis Nr. 3 der Anlage 1

	Änderung bestehende Verarbeitung : **Überführung bestehende Verarbeitung in geltende Rechtslage nach DS-GVO:**	☐ ja ☒ ja	
	Neue Verarbeitung:	☐ ja	
	Abmeldung bestehende Verarbeitung[8]:	☐ ja	
1. Grundsätzliche Angaben zur Verantwortlichkeit			
1.1	Verantwortliche Organisationseinheit[9] (optional):	Behörden, Ämter, Hochschulen und Landesbetriebe der Freien und Hansestadt Hamburg	
1.2	Vertreter der verantwortlichen Organisationseinheit (optional):	Klicken Sie hier, um Text einzugeben.	
1.3	Fachliche Leitstelle (bei IT-Verfahren) bzw. zuständige Stelle (bei nicht automatisierten Verfahren): Verantwortliche Führungskraft: Leitzeichen:	ZPD – HR-Systemhaus Geschäftsbereichsleitung HR Systemhaus ZPD 3	
1.4	Ansprechpartner, sofern nicht verantwortliche Führungskraft: Telefonnummer:	Klicken Sie hier, um Text einzugeben.	
1.5	Name des Datenschutzbeauftragten (optional):	Behördliche Datenschutzbeauftragte zu 1	

[8] Hinweis Nr. 4 der Anlage 1
[9] Hinweis Nr. 5 der Anlage 1

1.6	Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt[10]: Auftragsnummer:	Dataport AöR, Altenholzer Straße 10 – 14 , 24161 Altenholz Rahmenvertrag 4992	

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung[11]			
2.1	Beschreibung und Zweckbestimmung der Verarbeitung von Daten[12]	Beschreibung der Verarbeitung: Bewirtschaftung der Tarifbeschäftigten, einschließlich Empfänger der Zusatzversorgung und Beamtinnen und Beamten einschließlich Versorgungsempfänger, der Behörden, Ämter, Hochschulen und Landesbetriebe der Freien und Hansestadt Hamburg, Abrechnung und Zahlbarmachung der Gehälter und Bezüge, Erfüllung gesetzlicher Meldeverpflichtungen, Abführung von Sozialversicherungsbeiträgen und Steuern, Pfändungssachbearbeitung, Sachbearbeitung der Familienkasse und Nachversicherung sowie das Führen und Übermitteln gesetzlich vorgegebener Statistiken an die zuständigen Stellen. Beschreibung der Zweckbestimmung: Lohn-, Gehalts- und Bezügeabrechnung Sonstiges: Personalverwaltung	
2.2	Rechtsgrundlage (Zutreffendes bitte ankreuzen und ggf. erläutern):		
☒	Spezialgesetzliche Regelung außerhalb der DS-GVO	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* § 85 Abs. 1 HmbBG (für die Tarifbeschäftigten i. V. m. § 10 HmbDSG)	
☒	Einwilligung des Betroffenen (Art. 6 Abs. 1 a DS-GVO):	*Altersvermögensgesetz, EStG (Riester-Rente), Einwilligungserklärung des Personalamtes*	

[10] Hinweis Nr. 6 der Anlage 1
[11] Hinweis Nr. 7 der Anlage 1
[12] Hinweis Nr. 8 der Anlage 1

☒	Kollektivvereinbarung (z.B. Vereinbarung gem. HmbPersVG, Tarifvertrag)	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* *Vereinbarung gemäß § 93 HmbPersVG*	
☒	Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 4 HmbDSG n.F.)	Klicken Sie hier, um Text einzugeben.	
☒	Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§ 10 HmbDSG n.F. und national geregelt im BDSG):	§ 85 HmbBG§ 85 Abs. 1 HmbBG (für die Tarifbeschäftigten i. V. m. § 10 HmbDSG)	
☒	Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b DS-GVO)	Erfüllung der dem Arbeitgeber obliegenden Verpflichtungen aus dem Arbeitsvertrag bei den Tarifbeschäftigten.	
☐	Interessenabwägung (Art. 6 Abs. 1 f DS-GVO)	*Bitte benennen Sie die vorrangigen Interessen:* Klicken Sie hier, um Text einzugeben.	
☐	Weitere:	*Bitte benennen: Vorschrift, Paragraph, Absatz, Satz* Klicken Sie hier, um Text einzugeben.	
3. Beschreibung betroffener Personen- und Datenkategorien			
3.1	Beschreibung der betroffenen Personengruppen[13]:	Beschäftigte Versorgungsempfänger, Hinterbliebene Sonstige: Ehe- und Lebenspartner. ggf. auch ehemalige und Kinder von Beschäftigten können betroffen sein, Betreuer, Abzweigungsempfänger (Kindergeld)	

[13] Hinweis Nr. 9 der Anlage 1

3.2	Beschreibung der Art der Daten[14] bzw. Datenkategorien	Mitarbeiterdaten Sonstige: Daten von Ehe- und Lebenspartnern und Kindern Beschäftigter Beschreibung: Ggf. Schwerbehinderung, Daten zu Pfändungen, Daten für die Beihilfe, Gewährung familienbezogener Bezügebestandteile, Festsetzung von Kindergeld.	
3.3	Werden besondere Kategorien[15] von Daten verarbeitet (Art. 9 Abs. 1 DS-GVO)?	☒ ja, welche? Z. B.: Schwerbehinderung Gesundheitsdaten religiöse und weltanschauliche Überzeugungen ☐ nein	
4. Datenweitergabe und deren Empfänger[16]			
4.1	Eine Datenübermittlung findet statt oder ist geplant.	☒ ja ☐ nein	
4.2	Interne Empfänger innerhalb der verantwortlichen Stelle	☒ ja ☐ nein	
	Interne Stelle (Organisationseinheit)	ZPD für die zentralen Prozesse, Personalamt und andere Behörden und Ämter der FHH (Arbeitgeber FHH)	
	Art der Daten	Beschäftigtendaten	
	Zweck der Daten-Mitteilung	Abrechnung, Auswertungen, Berichte, Beihilfe, Pfändungen, Familienkasse, Haushalt, Dienstunfallbearbeitung, Nachversicherung, interner Arbeitsmarkt/Mobilität,	

[14] Hinweis Nr. 10 der Anlage 1
[15] Hinweis Nr. 11 der Anlage 1
[16] Hinweis Nr. 12 der Anlage 1

		Erfüllung gesetzlicher Meldeverpflichtungen, Nachversicherung/Versorgungsausgleich.	
4.3	Externe Empfänger und Dritte	☒ ja ☐ nein	
	Externe Stelle	Dataport, Familien- und Sozialgerichte, Gläubiger, Sozialversicherungsträger wie die gesetzliche Krankenkassen, Rentenversicherungsträger, Unfallkassen, Versicherungen, , Kasse Hamburg, Bundeszentralamt für Steuern, ZfA/Riester, Institutionen für vermögenswirksame Leistungen, Hamburger Verkehrsverbund, Versicherungsmathematiker	
	Art der Daten	Beschäftigtendaten	
	Zweck der Daten-Mitteilung	Datenverarbeitung im Auftrag, Gesetzliche Meldeverfahren, Vermögenswirksame Leistungen, Jobticket, Erstellung versicherungsmathematischer Rückstellungsgutachten	
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[17]			
	Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Löschungsfristen?	☒ ja, falls ausgewählt bitte benennen: Siehe KoPers-Löschkonzept ☐ nein	
	Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:	Siehe KoPers-Löschkonzept	
6. Mittel der Verarbeitung (optional) **Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?[18]**			
	Bezeichnung: Hersteller: Funktionsbeschreibung: Bereitstellung:	KoPers P&I AG, Wiesbaden Personalinformationssystem ☐ Eigenentwickelte/ individuelle Software ☒ Standard-Software ☐ Cloud-Services ☐ Sonstige: Klicken Sie hier, um Text einzugeben.	
7. Zugriffsberechtigte Personengruppen (vereinfachtes Berechtigungskonzept)[19]			

[17] Hinweis Nr. 13 der Anlage 1
[18] Hinweis Nr. 14 der Anlage 1
[19] Hinweis Nr. 15 der Anlage 1

	Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte Berechtigungskonzept:	Siehe Berechtigungskonzept KoPers und SAP (ggf. als Anlage beifügen)	
8. Sicherheit der Verarbeitung (Risikoprüfung), Datenschutz-Folgenabschätzung und Technische und organisatorische Maßnahmen[20]			
8.1	Hinsichtlich der Datensicherheitsmaßnahmen wurde der Bereich IT-Sicherheit (z.B. InSiBe der OE) eingebunden?	☒ ja ☐ nein	
8.2	Die allgemeine Zielsetzung aus dem Rahmensicherheitskonzept wurde sichergestellt.	☒ ja ☐ nein, Abweichungen erläutern: Klicken Sie hier, um Text einzugeben.	
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?[21]	☒ ja (ggf. Betriebs-/Herstellerkonzept beifügen) Lt. P&I AG sind die TOM nach Art. 25 und 32 DSGVO in der Vertragsergänzung vom 21. 03.2018 enthalten (Vertrag liegt bei Dataport vor). ☐ 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 Schutzbedarfsfeststellung und Risikoprüfung wurden nach HmbDSG durchgeführt. Eine erneute Schutzbedarfsfeststellung sowie Risikoprüfung erfolgt, sobald sich wesentliche Änderungen im Verfahren ergeben. • Allgemeine Datensicherheitsbeschreibung (Dataport); • Umfassendes Datensicherheitskonzept (Dataport); • Wiederanlauf- bzw. Notfallkonzept (Dataport)…..	

[20] Hinweis Nr. 16 der Anlage 1
[21] Hinweis Nr. 17 der Anlage 1

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. ☐ Die Anlage 2 wurde ausgefüllt und liegt vor.	
8.8	Es liegen schriftlich vor	☒ interne Verhaltensregeln ☒ ggf. DSFA ☒ Risikoprüfung/ Schutzbedarfsfeststellung ☒ allg. Datensicherheitsbeschreibung (bei Dataport) ☒ umfassendes Datensicherheitskonzept (bei Dataport) ☒ Wiederanlauf- bzw. Notfallkonzept (bei Dataport) ☐ Sonstiges: Klicken Sie hier, um Text einzugeben.	
9. Datenübertragbarkeit[22] (Datenportabilität)			

[22] Hinweis Nr. 18 der Anlage 1

	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: je nach Fallgestaltung elektronische Schnittstelle, Zuständigkeit der jeweiligen Personalverwaltung. ☐ nein, Begründung: Klicken Sie hier, um Text einzugeben.	
10. Informationen der Betroffenen[23]			
	Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?	Siehe Merkblätter zu Art. 13 EU-DSGVO	
11. Sonstiges			
	Anmerkungen:	Klicken Sie hier, um Text einzugeben.	

Anlage 1**:**

Hinweise zum Formular

Hinweis Nr. 1

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

Hinweis Nr. 2

Gemeint ist, welche Verarbeitungstätigkeiten durch das Verfahren berührt werden.

Hinweis Nr. 3

Geplanter oder tatsächlicher Beginn der Verarbeitung von personenbezogenen Daten. Dabei ist schon die erstmalige Übertragung oder Speicherung von Daten relevant.

[23] Hinweis Nr. 19 der Anlage 1

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).

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.

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.

Hinweis Nr. 15

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

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

Hinweis Nr. 16

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

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

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

Hinweis Nr. 17

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

Hinweis Nr. 18

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

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

Hinweis Nr. 19

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

Anlage 2

Übersicht und Erläuterungen zu den technischen und organisatorischen Maßnahmen

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

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

Trotz der Formulierung „wenn möglich“ stellt die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO hier den Regelfall dar.

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

Eine Verarbeitung darf erst erfolgen, wenn der Verantwortliche seiner Pflicht nach Art. 24 DS-GVO nachgekommen ist. Darunter fallen neben den Verpflichtungen nach Art. 12 und 25 DS-GVO auch diejenigen nach Art. 32 DSGVO zur Bestimmung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das betrifft primär Fragen der Sicherheit der Verarbeitung, schließt somit aber auch Maßnahmen zur Gewährleistung von Betroffenenrechten ein. In das Verzeichnis ist eine allgemeine, einfach nachvollziehbare Beschreibung der für diesen Zweck getroffenen Maßnahmen aufzunehmen.

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

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

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

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

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

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

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

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

Maßnahmen zur Pseudonymisierung personenbezogener Daten

Hierzu zählen u. a.:

- Festlegung der durch Pseudonymisierung zu ersetzenden identifizierenden Daten
- Definition der Pseudonymisierungsregel, ggf. anknüpfend an Personal-, Kunden- oder Patienten-Kennziffern
- Autorisierung: Festlegung der Personen, die zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind
- Festlegung der zulässigen Anlässe für Pseudonymisierungs- und Depseudonymisie-rungsvorgänge
- zufällige Erzeugung der Zuordnungstabellen oder der in eine algorithmische Pseudony-misierung eingehenden geheimen Parameter

- Schutz der Zuordnungstabellen bzw. geheimen Parameter sowohl gegen unautorisierten Zugriff als auch gegen unautorisierte Nutzung
- Trennung der zu pseudonymisierenden Daten in die zu ersetzenden identifizierenden und die weiteren Angaben

Maßnahmen zur Verschlüsselung personenbezogener Daten

(z. B. in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport)

Schlüssel können flüchtig (z. B. für die Dauer eines Kommunikationsvorgangs) oder statisch (mittel- oder langfristig) für den Schutz personenbezogener Daten eingesetzt werden.

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

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

Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste

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

Hierzu zählen u. a.:

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

- Durchführung von internen oder externen Sicherheitsaudits
- logische oder physikalische Trennung der Datenverarbeitung z. B. nach verantwortlichen Stellen, den verfolgten Verarbeitungszwecken und nach Gruppen betroffener Personen
- sicheres, rückstandsfreies Löschen von Daten bzw. Vernichten von Datenträgern nach Ablauf der Aufbewahrungsfristen, Festlegungen zu Löschverfahren und zur Beauftragung von Dienstleistern

Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste

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

Hierzu zählen u. a.:

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

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

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

Hierzu sind u. a. folgende Maßnahmen erforderlich:

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

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

Hierzu zählen u. a.:

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

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

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

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

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten

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

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

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

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

- differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen

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

Anlage 3

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

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

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

Gewährleistung der **Verfügbarkeit** Art. 32 Abs. 1 lit. b DS-GVO	Verfügbarkeitskontrolle (§ 64 Abs. 3 Nr. 13 BSDG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden Richtlinie Regelwerk ELDORADO
	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO
	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL)Rahmen-Sicherheitskonzept der FHH (RaSiKo)Sicherheits- und Betriebskonzept Rechenzentrum DataportGeschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)
Gewährleistung der **Vertraulichkeit** Art. 32 Abs. 1 lit. b DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	Freigabe-Richtlinie Service-Level-Agreements Richtlinie zur Datensicherheit im IuK-Bereich
	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept)

		Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzepte der jeweiligen Fachverfahren Grundsätze des Verwaltungshandelns nach Beamtenstatusgesetz bzw. Tarifvertrag (Verschwiegenheitspflicht)
	Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)	Betriebskonzept des jeweiligen Fachverfahrens Geschäftsordnungsbestimmungen der Behörden

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

Transparenz Art. 5 Abs. 1 lit. a DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	Freigabe-Richtlinie Service-Level-Agreements Richtlinie zur Datensicherheit im IuK-Bereich
	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie zur Verwaltung von Passwörtern Richtlinie FHH Portal Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Geschäftsordnungsbestimmungen der Behörden (Rechte im Filesystem, Berechtigungskonzept Zugriff auf Sharepoint)
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum DataportVorgaben für das Haushalts- und KassenrechtRichtlinie zur Verwaltung von PasswörternGeschäftsordnungsbestimmungen der Behörden
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Sicherheits- und Betriebskonzept FHH Netz Geschäftsordnungsbestimmungen der Behörden
	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept) Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)

Verfahren **regelmäßiger Überprüfung**, **Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen** **Maßnahmen** Art. 32 Abs. 1 lit. d DS-GVO	-	turnusmäßige Überarbeitung der Richtlinien der FHH (PDCA-Modell im RaSiKo, IS-LL) turnusmäßige Überarbeitung des Sicherheitskonzeptes durch Dataport
Verfahren zur schnellen **Wiederherstellung der Verfügbarkeit** personenbezogener Daten nach einem physischen oder technischen Zwischenfall Art. 32 Abs. 1 lit. c DS-GVO	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	Sicherheits- und Betriebskonzept Rechenzentrum Dataport Richtlinie der FHH über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie Regelwerk ELDORADO
Gewährleistung der **Belastbarkeit der Systeme** Art. 32 Abs. 1 lit. b DS-GVO	Verfügbarkeitskontrolle (§ 64 Abs. 3 Nr. 13 BSDG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden Richtlinie Regelwerk ELDORADO
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	Informationssicherheitsleitlinie der FHH (IS-LL) Rahmen-Sicherheitskonzept der FHH (RaSiKo) Sicherheits- und Betriebskonzept Rechenzentrum Dataport Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)

<u>Definitionen der Grundwerte nach DS-GVO:</u>

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