

# Beschreibung der Verarbeitungstätigkeit

(Bitte an die Verzeichnisführende Stelle absenden!)

Blatt-Nr.:

Von der Verzeichnisführenden  
Stelle auszufüllen!

**Nur auszufüllen, wenn personenbezogene Daten<sup>1</sup> 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:	Vorname, Nachname einfügen	
	Telefonnummer:	Telefonnummer einfügen	
	<b>Bezeichnung des Verfahrens:</b>	Auszahlungen von Leistungen nach dem AsylbLG mittels des Bezahlendienstes SocialCard	
	<b>Bezeichnung der Verarbeitung<sup>2</sup>:</b>	<input checked="" type="checkbox"/> Erheben <input checked="" type="checkbox"/> Erfassen <input type="checkbox"/> Organisieren <input type="checkbox"/> Ordnen <input checked="" type="checkbox"/> Speichern <input type="checkbox"/> Anpassen oder Verändern <input type="checkbox"/> Auslesen <input type="checkbox"/> Abfragen <input checked="" type="checkbox"/> Verwenden <input checked="" type="checkbox"/> Offenlegen durch Übermittlung, Verbreitung oder andere Form der Bereitstellung <input checked="" type="checkbox"/> Abgleichen oder Verknüpfen <input type="checkbox"/> Einschränken <input checked="" type="checkbox"/> Löschen <input type="checkbox"/> Vernichten	
	<b>Beginn der Verarbeitung<sup>3</sup>:</b>	Klicken Sie hier, um Text einzugeben.	
	<b>Änderung bestehende Verarbeitung:</b>	<input checked="" type="checkbox"/> ja, bisher wurden die Personen, die kein Konto haben, mit Bargeld versorgt  <input type="checkbox"/> ja	
	<b>Überführung bestehende Verarbeitung in geltende Rechtslage nach DS-GVO:</b>	<input type="checkbox"/> ja	
	<b>Neue Verarbeitung:</b>	<input type="checkbox"/> ja	
	<b>Abmeldung bestehende Verarbeitung<sup>4</sup>:</b>	<input type="checkbox"/> ja	
1. Grundsätzliche Angaben zur Verantwortlichkeit			
1.1	Verantwortliche Organisationseinheit <sup>5</sup> (optional):		

<sup>1</sup> Hinweis Nr. 1 der Anlage 1

<sup>2</sup> Hinweis Nr. 2 der Anlage 1

<sup>3</sup> Hinweis Nr. 3 der Anlage 1

<sup>4</sup> Hinweis Nr. 4 der Anlage 1

<sup>5</sup> Hinweis Nr. 5 der Anlage 1

1.2	Vertreter der verantwortlichen Organisationseinheit (optional):		
1.3	Fachliche Leitstelle (bei IT-Verfahren) bzw. zuständige Stelle (bei nicht automatisierten Verfahren): Verantwortliche Führungskraft: Leitzeichen:	fachliche Leitstelle einfügen Vorname, Nachname einfügen Leitzeichen einfügen	
1.4	Ansprechpartner, sofern nicht verantwortliche Führungskraft: Telefonnummer:	ggf. Ansprechpartner einfügen Telefonnummer einfügen	
1.5	Name des Datenschutzbeauftragten (optional):		
1.6	Name und Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt <sup>6</sup> : Auftragsnummer:		

## 2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung<sup>7</sup>

2.1	Beschreibung und Zweckbestimmung der Verarbeitung von Daten <sup>8</sup>	<p>Beschreibung der Verarbeitung:</p> <p>Die Daten von Asylsuchenden werden im Fachverfahren Fachverfahren einfügen aufgenommen und der Leistungsanspruch nach dem AsylbLG ermittelt. Die Leistungen nach dem AsylbLG werden ab dem auf die sogenannte SocialCard (=Bezahldienst: Produkt der Bietergemeinschaft aus Publk GmbH und Secupay AG) als normale Überweisung ausgezahlt. Damit eine Überweisung aus dem Fachverfahren Fachverfahren einfügen über das Buchhaltungssystem der Behörde einfügen vorgenommen werden kann, muss jedem Asylsuchenden eine SocialCard mit einer IBAN zugewiesen werden. Die für die Zahlung benötigten Stammdaten der Asylsuchenden werden dazu manuell in das Portal des Bezahldienstes übertragen, so dass eine personenbezogene IBAN erzeugt wird, die für künftige Zahlungen von Leistungsansprüchen nach dem AsylbLG zur Verfügung steht. Die IBAN muss dazu im Fachverfahren Fachverfahren einfügen manuell übernommen werden. In der Folge einer normalen Anordnung wird die Auszahlung über Software zur Zahlungsabwicklung einfügen ausgelöst.</p> <p>Beschreibung der Zweckbestimmung: Wählen Sie ein Element aus.</p> <p>Sonstiges:</p>	
-----	--	---	--

<sup>6</sup> Hinweis Nr. 6 der Anlage 1

<sup>7</sup> Hinweis Nr. 7 der Anlage 1

<sup>8</sup> Hinweis Nr. 8 der Anlage 1

		<p>1. Behörde einfügen: Gewährung von Leistungen nach dem AsylbLG</p> <p>2. auszahlende Behörde einfügen: Durchführung der Auszahlung der vom Behörde einfügen angeordneten Leistungen nach dem AsylbLG auf die SocialCard</p>	
2.2	Rechtsgrundlage (Zutreffendes bitte ankreuzen und ggf. erläutern):		
<input type="checkbox"/>	Spezialgesetzliche Regelung außerhalb der DS-GVO	<i>Bitte benennen: Vorschrift, Paragraph, Absatz, Satz</i>	
<input type="checkbox"/>	Einwilligung des Betroffenen (Art. 6 Abs. 1 a DS-GVO):	<i>Bitte fügen Sie die Einwilligungsklausel und den Einwilligungsmechanismus hier ein</i>	
<input type="checkbox"/>	Kollektivvereinbarung (z.B. Vereinbarung gem. LPersVG, Tarifvertrag)	<i>Bitte benennen: Vorschrift, Paragraph, Absatz, Satz</i>	
<input checked="" type="checkbox"/>	Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 4 LDSG (BW))	Art. 6 Absatz 1 Unterabsatz 1 Buchstabe e DSGVO; § 4 LDSG (BW) i.V.m. AsylbLG Die Erfüllung der fachlichen Aufgaben, die der Bezahlendienst unterstützt, wurde der Behörde einfügen nach § 2 Abs. 3 bzw. Abs. 4 FlüAG übertragen. Für Behörde einfügen ergibt sich die Zuständigkeit aus Vorschrift einfügen (Buchführung), Vorschrift einfügen (IT-Verfahren) sowie Vorschrift einfügen (Zahlungen).	
<input checked="" type="checkbox"/>	Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§ 15 LDSG (BW) und national geregelt im BDSG):	Verarbeitung von Beschäftigtendaten der User, §15 Abs. 1, 2, 8 LDSG (BW), Art. 88 DS-GVO	
<input type="checkbox"/>	Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b DS-GVO)		
<input type="checkbox"/>	Weitere:	<i>Bitte benennen: Vorschrift, Paragraph, Absatz, Satz</i>	
<b>3. Beschreibung betroffener Personen- und Datenkategorien</b>			
3.1	Beschreibung der betroffenen Personengruppen <sup>9</sup> :	<p>Beschäftigte und Leistungsempfänger und Leistungsempfängerinnen nach dem AsylbLG</p> <p>Beschreibung:</p>	

<sup>9</sup> Hinweis Nr. 9 der Anlage 1

3.2	Beschreibung der Art der Daten <sup>10</sup> bzw. Datenkategorien	<p>Identifikations- und Adressdaten Sonstige: Beschreibung für Asylsuchende im Bezahlendienst: Personendaten (Name, Geburtsdatum, Geburtsort, Staatsangehörigkeit und vergleichbare Daten) Kontaktdaten (Adresse, E-Mail-Adresse, Telefonnummer und vergleichbare Daten) Legitimationsdaten (Ausweis- und Melde-daten); Aktenzeichen Fachverfahren einfügen; Verfügungsrahmen als Schieberegler; IBAN (mit Übertrag nach Fachverfahren einfügen)</p> <p>Übergabe der Daten von Asylsuchenden an Software zur Zahlungsabwicklung einfügen: Name und Adressdaten, IBAN</p> <p>Übergabe der Daten von Asylsuchenden an Bundesbank: Name</p> <p>Beschreibung für Beschäftigte: Name, Vorname, E-Mailadresse</p>	
3.3	Werden besondere Kategorien <sup>11</sup> von Daten verarbeitet (Art. 9 Abs. 1 DS-GVO)?	<input type="checkbox"/> ja, welche? Wählen Sie ein Element aus. <input checked="" type="checkbox"/> nein	
<b>4. Datenweitergabe und deren Empfänger<sup>12</sup></b>			
4.1	Eine Datenübermittlung findet statt oder ist geplant.	<input checked="" type="checkbox"/> ja, siehe 2.1 <input type="checkbox"/> nein	
4.2	Interne Empfänger innerhalb der verantwortlichen Stelle	<input type="checkbox"/> ja <input checked="" type="checkbox"/> nein	
	Interne Stelle (Organisationseinheit)		
	Art der Daten		
	Zweck der Daten-Mitteilung		
4.3	Externe Empfänger und Dritte	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein	
	Externe Stelle	Publk GmbH, secupay AG, Bundesbank, Nortal	
	Art der Daten	Siehe 3.2	
	Zweck der Daten-Mitteilung	Publk GmbH, secupay AG: Bereitstellung der SocialCard und Auszahlung der Leistungen nach dem AsylbLG   Bundesbank: Auszahlung der Leistung	

<sup>10</sup> Hinweis Nr. 10 der Anlage 1

<sup>11</sup> Hinweis Nr. 11 der Anlage 1

<sup>12</sup> Hinweis Nr. 12 der Anlage 1

4.4	Geplante Datenübermittlung in Drittstaaten (außerhalb der EU) bzw. internationale Organisation	<input type="checkbox"/> ja <input checked="" type="checkbox"/> nein	
	Drittstaat bzw. internationale Organisation		
	Art der Daten		
	Zweck der Daten Mitteilung		
	Welche geeigneten Garantien gem. Art. 46 DS-GVO werden im Zusammenhang mit der Übermittlung gegeben?	Garantien bestehen durch:  <input type="checkbox"/> verbindliche interne Datenschutzvorschriften, <input type="checkbox"/> von der Kommission oder von einer Aufsichtsbehörde angenommene Standard-datenschutzklauseln <input type="checkbox"/> 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.	
<b>5. Regelfristen für die Löschung der Daten<sup>13</sup></b>			
	Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Lösungsfristen?	<input checked="" type="checkbox"/> ja, falls ausgewählt bitte benennen:  10 Jahre ab letztem Zeitpunkt der Kartennutzung Kommunen: § 39 Abs. 2 GemHVO/Regierungspräsidien: Anlage 7 zu Nr. 19.3 zu §§ 70 bis 79 LHO AufbewBest auswählen  Für den Zahlungsdienstleister gilt die von der BaFin vorgegebene Aufbewahrungsfrist von 10 Jahren - auch in Insolvenzfällen. <input type="checkbox"/> nein	
	Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:	Die Daten werden vollständig 10 Jahre nach der letzten Verwendung gem. der o.g. Rechtsgrundlagen gelöscht.	
<b>6. Mittel der Verarbeitung (optional) Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?<sup>14</sup></b>			
	Bezeichnung: Hersteller: Funktionsbeschreibung: Bereitstellung:	Bezahldienst SocialCard Publk GmbH Siehe... <input type="checkbox"/> Eigenentwickelte/ individuelle Software <input checked="" type="checkbox"/> Standard-Software <input type="checkbox"/> Cloud-Services <input checked="" type="checkbox"/> Sonstige:	

<sup>13</sup> Hinweis Nr. 13 der Anlage 1

<sup>14</sup> Hinweis Nr. 14 der Anlage 1

		Es handelt sich um eine Dienstleistung.	
<b>7. Zugriffsberechtigte Personengruppen (vereinfachtes Berechtigungskonzept)<sup>15</sup></b>			
	Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte Berechtigungskonzept:	Berechtigte User sind Mitarbeitende in der Behörde Behörde einfügen; Personen von Pubk und secupay. Personen, die nicht am Verfahren beteiligt sind, dürfen nach Hinterlegung der Kontaktdaten durch die verantwortliche Stelle Behörde einfügen beim Bezahlendienst Benutzerkennungen beantragen. Details siehe Anlage (ggf. als Anlage beifügen)	
<b>8. Sicherheit der Verarbeitung (Risikoprüfung), Datenschutz-Folgenabschätzung und Technische und organisatorische Maßnahmen<sup>16</sup></b>			
Nachfolgende Angaben betreffen vorwiegend die Sicherheitsmaßnahmen der eingeschalteten Dienstleister (Pubk GmbH und secupay AG).			
8.1	Hinsichtlich der Datensicherheitsmaßnahmen wurde der Bereich IT-Sicherheit eingebunden?	<input type="checkbox"/> ja, <input checked="" type="checkbox"/> nein,  Es handelt sich um eine Dienstleistung, die IT-Sicherheit wurde in der Leistungsbeschreibung eingefordert (u.a. BSI-Zertifizierung liegt vor) – vgl. 8.2., Secupay AG ist BaFin überwacht	
8.2	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? <sup>17</sup>	<input checked="" type="checkbox"/> ja (siehe TOMs der Bietergemeinschaft), Fachverfahren einfügen und Software zur Zahlungsabwicklung einfügen werden im Rechenzentrum von Rechenzentrum einfügen <sup>2</sup> betrieben – hier gelten die bekannten TOMs eines BSI-zertifizierten Rechenzentrums <input type="checkbox"/> nein, Begründung:	TOMs – siehe Anlage 2 (pdf-Datei)
8.3	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.	<input checked="" type="checkbox"/> ja, siehe Formular „Schutzbedarfsfeststellung“ <input type="checkbox"/> nein Bitte Ergebnis der Risikoprüfung als Anlage beifügen.	
8.4	Es wurden die Erforderlichkeitsprüfung („Schwellwertanalyse“)	<input checked="" type="checkbox"/> ja, Ergebnis der Erforderlichkeitsprüfung („Schwellwertanalyse“) und ggf. die durchgeführte DSFA als Anlage beifügen <input type="checkbox"/> nein	

<sup>15</sup> Hinweis Nr. 15 der Anlage 1

<sup>16</sup> Hinweis Nr. 16 der Anlage 1

<sup>17</sup> Hinweis Nr. 17 der Anlage 1

	und ggf. die Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO durchgeführt.		
8.5	<p>Bei Verfahren, die bei IT-Dienstleister einfügen gehostet werden:</p> <p>Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMs der Behörde einfügen sichergestellt (bitte einfügen – vgl. Muster Anlage 4 – auf Basis der TOMs der Freien und Hansestadt Hamburg).</p>	<p><input checked="" type="checkbox"/> Es liegt ein Verfahren (Software zur Zahlungsabwicklung einfügen und Fachverfahren einfügen) vor, das bei IT-Dienstleister einfügen gehostet wird.</p>	
8.7	<p>Bei Verfahren, die <u>nicht</u> bei IT-Dienstleister aus Ziff. 8.5 einfügen gehostet werden:</p> <p>Die Gewährleistung der Grundwerte nach BSI-Grundschutz und DS-GVO für die Sicherheit der Verarbeitung werden durch die TOMs laut Anlage 2 sichergestellt.</p>	<p><input checked="" type="checkbox"/> Es liegt kein Verfahren (Bezahldienst SocialCard) vor, dass nicht bei IT-Dienstleister aus Ziff. 8.5 einfügen gehostet wird, vgl. 8.3. Verantwortliche für die Verarbeitung im Webportal ist Publk GmbH sowie Secupay AG.</p> <p>Webportal des Bezahldienstes: Das Webportal wird im BSI auditierten Cloudrechenzentrum der SAP in Frankfurt a.M. gehostet. Das Rechenzentrum ist nach BSI-C5 auditiert, zudem ist es SOC2 und ISO27001 zertifiziert.</p> <p>Das Processing, die Zuordnung der Zahlungen und die Autorisierung der User laufen über den Secupay. Secupay, als Teil des Bezahldienstes, ist ein von der BaFIN lizenziertes Unternehmen (<a href="https://portal.mvp.bafin.de/database/ZahlInst-Info/zahlinst.do?id=126737">https://portal.mvp.bafin.de/database/ZahlInst-Info/zahlinst.do?id=126737</a>) und wird daher auch entsprechend bei der IT-Sicherheit und Verfügbarkeit von der Finanzaufsicht überwacht.</p> <p><input type="checkbox"/> Die Anlage 3 wurde ausgefüllt/ergänzt und liegt vor.</p>	
8.8	Es liegen schriftlich vor	<p><input type="checkbox"/> interne Verhaltensregeln (<i>bitte ggf. ankr.</i>)</p> <p><input checked="" type="checkbox"/> Schwellwertanalyse</p> <p><input checked="" type="checkbox"/> DSFA für den Bezahldienst SocialCard</p> <p><input checked="" type="checkbox"/> Risikoprüfung/ Schutzbedarfsfeststellung</p> <p><input checked="" type="checkbox"/> IT-Sicherheitskonzept</p> <p><input checked="" type="checkbox"/> Datenschutzkonzept</p> <p><input checked="" type="checkbox"/> Wiederanlauf- bzw. Notfallkonzept</p> <p><input type="checkbox"/> Sonstiges:</p>	

9. Datenübertragbarkeit <sup>18</sup> (Datenportabilität)			
	<p>Nur bei - auf Grundlage einer Einwilligung- (s. 2.2) zur Verfügung gestellten Daten:</p> <p>Ist der Export der verarbeiteten Daten an den Betroffenen oder andere Dienste in einem gängigen, standardisierten Format möglich?</p>	<p><input type="checkbox"/> ja, Format: Excel und Word</p> <p><input checked="" type="checkbox"/> nein, Begründung: Es wird keine Einwilligung seitens der o.g. verantwortlichen Stellen eingeholt.</p>	
10. Informationen der Betroffenen <sup>19</sup>			
	<p>Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?</p>	<p>Die Nutzer:innen bekommen die Nutzungshinweise sowie AGB des Bezahlendienstes in verschiedenen Sprachen.</p> <p>Die Datenschutzhinweise von Publk GmbH und Secupay AG auf folgenden Seiten.</p> <p><a href="#">SocialCard - Datenschutz</a></p> <p><a href="#">Datenschutz   (secupay.com)</a></p> <p>Siehe die einschlägigen Datenschutzhinweise der Behörde im Rahmen der Bearbeitung der Anträge nach dem AsylbLG.</p>	
11. Sonstiges			
	Anmerkungen:	Klicken Sie hier, um Text einzugeben.	

.....  
Verantwortlicher

.....  
Datum

.....  
Unterschrift

<sup>18</sup> Hinweis Nr. 18 der Anlage 1

<sup>19</sup> 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:

<b>Erheben</b>	Beschaffen von Daten über eine betroffene Person. Gezielte Verwandlung eines unbekanntes Datums in ein Bekanntes. Setzt aktives Handeln des Verantwortlichen voraus. Gilt nicht, wenn der/dem Verantwortlichen eine Information aufgezwungen wird.
<b>Erfassung</b>	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.
<b>Organisieren</b>	Strukturelle Neuordnung/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.
<b>Ordnen</b>	Sinnvoll strukturierte Ablage der gespeicherten personenbezogenen Daten auf dem Datenträger, z.B. nach Alphabet.
<b>Speichern</b>	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.
<b>Anpassen</b>	Beispiel für Veränderung. Aktualisierung/Angleichung der personenbezogenen Daten an die realen Lebensumstände, z.B. Änderung der Wohnanschrift.
<b>Verändern</b>	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.
<b>Auslesen</b>	Bewusste Kenntnisnahme über die auf einem Datenträger befindlichen personenbezogenen Daten/Abfragen von Informationen. Daten werden aus einem Datenträger ausgelesen, um sie einer weiteren Bearbeitung zugänglich zu machen.
<b>Abfragen</b>	Gezielte Informationssuche auf einem Datenträger und Kenntnisnahme dieser/Gewinnung von Daten. Zum Beispiel mithilfe der Eingabe eines Suchbegriffs.
<b>Verwenden</b>	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.
<b>Offenlegen</b>	Vorgang, der dazu führt, dass Daten für andere zugänglich gemacht werden und sie diese auslesen oder abfragen können. Bekanntgabe bekannter gespeicherter Daten an Dritte.
<b>- durch Übermittlung</b>	Gezielte Weitergabe von Daten an einen oder mehrere Empfänger.

- <b>durch Verbreitung</b>	Ungezielte Weitergabe an unbestimmte Adressaten z.B. Öffentlichkeit.
- <b>durch andere Form der Bereitstellung</b>	Passive Form der Offenlegung. Bereithaltung der Daten zum potenziellen Gebrauch, z.B. für eine Einsicht.
<b>Abgleichen</b>	Vergleich mehrerer zusammengehöriger bekannter, nicht am selben Ort gespeicherter Daten. Abweichungen oder Übereinstimmungen können festgestellt werden.
<b>Verknüpfen</b>	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).
<b>Einschränken</b>	Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken (Art. 4 Nr. 3). Entspricht der Sperrung von Daten.
<b>Löschen</b>	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.
<b>Vernichten</b>	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.

## Übersicht und Erläuterungen zu den technischen und organisatorischen Maßnahmen

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

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

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

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

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

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

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

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

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

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

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

#### 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 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 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 personenbezogenen 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 Notfallhandbuchs
- Integration des Notfallmanagements in Geschäftsprozesse
- Durchführung von Notfallübungen
- Erprobung von Wiederanlaufszszenarien

#### 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 Folgendes 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

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

*Bitte fügen Sie nachfolgend Ihre entsprechenden Sicherheits-, Betriebskonzepte, Richtlinien, Leitlinien, Verwaltungsvorschriften, etc. ein. Die in kursiv eingefügten Ausführungen sind lediglich Beispiele und sofern unzutreffend zu streichen bzw. zu ergänzen.*

Grundwerte nach DS-GVO	Definierte Technische und Organisatorische Maßnahmen (TOMs) nach § 64 BDSG	Ergriffene Technische und Organisatorische Maßnahmen (TOMs) der Behörde einfügen
<p><b>Datenminimierung</b> Art. 5 Abs. 1 lit.c DS-GVO</p>	-	<p><i>Verwaltungsvorschriften IT-Projekte Richtlinie über Mindestanforderungen an die Sicherheit der Datenverarbeitung auf UNIX-Rechnern (UNIX-Richtlinie)</i></p>
<p>Gewährleistung der <b>Integrität</b> Art. 32 Abs. 1 lit. b DS-GVO</p>	<p>Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BDSG)</p>	<p><i>Sicherheits- und Betriebskonzept Richtlinie zur Verwaltung von Passwörtern Grundschutzkonzept für die Informations- und Kommunikationstechnik Geschäftsordnungsbestimmungen der Behörden</i></p>
	<p>Datenintegrität (§ 64 Abs. 3 Nr. 11 BDSG)</p>	<p><i>Informationssicherheitsleitlinie Sicherheitskonzept der Behörde Sicherheits- und Betriebskonzept IT-Dienstleister Richtlinie zur Verwaltung von Passwörtern Geschäftsbestimmungen der Behörden</i></p>
	<p>Datenträgerkontrolle (§ 64 Abs. 3 Nr. 2 BDSG)</p>	<p><i>Sicherheits- und Betriebskonzept IT-Dienstleister Richtlinie der Behörde über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich Entsorgungs-Richtlinie</i></p>
	<p>Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)</p>	<p><i>Sicherheits- und Betriebskonzept IT-Dienstleister Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörde</i></p>
	<p>Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BDSG)</p>	<p><i>Sicherheits- und Betriebskonzept IT-Dienstleister Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der Behörde über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich</i></p>
	<p>Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)</p>	<p><i>Sicherheits- und Betriebskonzept IT-Dienstleister</i></p>



		<i>Geschäftsordnungsbestimmungen der Behörde</i>
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BDSG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister Berechtigungskonzepte des jeweiligen Fachverfahren Grundsätze des Verwaltungshandelns nach Beamtenstatusgesetz bzw. Tarifvertrag (Verschwiegenheitspflicht)</i>
	Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)	<i>Betriebskonzept des jeweiligen Fachverfahrens Geschäftsordnungsbestimmungen der Behörde</i>
	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister Richtlinie der Behörde über die Sicherheit der Datenverarbeitung auf Endgeräten</i>
	Zugangskontrolle (§ 64 Abs. 3 Nr. 1 BDSG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister Grundschutzkonzept für die Informations- und Kommunikationstechnik, Geschäftsordnungsbestimmungen der Behörden</i>
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	<i>Informationssicherheitsleitlinie der Behörde Rahmen-Sicherheitskonzept der Behörde Sicherheits- und Betriebskonzept IT-Dienstleister, Geschäftsordnungsbestimmung der Behörde (Vertretungsregelungen, Vier-Augen-Prinzip)</i>
Gewährleistung der <b>Verfügbarkeit</b> Art. 32 Abs. 1 lit. b DS-GVO	Verfügbarkeitskontrolle (§ 64 Abs. 3 Nr. 13 BDSG)	<i>Informationssicherheitsleitlinie der Behörde Rahmen-Sicherheitskonzept der Behörde Sicherheits- und Betriebskonzept IT-Dienstleister Geschäftsordnungsbestimmungen der Behörde</i>
	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister Richtlinie der Behörde über die Sicherheit der Datenverarbeitung auf Endgeräten</i>
	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	<i>Informationssicherheitsleitlinie der Behörde Rahmen-Sicherheitskonzept der Behörde Sicherheits- und Betriebskonzept IT-Dienstleister Grundschutzkonzept für die Informations- und Kommunikationstechnik Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)</i>

	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	Informationssicherheitsleitlinie der Behörde Rahmen-Sicherheitskonzept der Behörde Sicherheits- und Betriebskonzept IT-Dienstleister Geschäftsordnungsbestimmungen der Behörde (Vertretungsregelungen, Vier-Augen-Prinzip)
Gewährleistung der <b>Vertraulichkeit</b> 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 BDSG)	Sicherheits- und Betriebskonzept IT-Dienstleister Richtlinie zur Verwaltung von Passwörtern Richtlinie Behörde Grundsatzkonzept für die Informations- und Kommunikationstechnik Geschäftsordnungsbestimmungen der Behörde (Rechte..., Berechtigungskonzept...)
	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	Sicherheits- und Betriebskonzept IT-Dienstleister Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörde
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BDSG)	Sicherheits- und Betriebskonzept IT-Dienstleister Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der Behörde über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	Sicherheits- und Betriebskonzept IT-Dienstleister Sicherheits- und Betriebskonzept Behörde Geschäftsordnungsbestimmungen der Behörde
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BDSG)	Sicherheits- und Betriebskonzept IT-Dienstleister 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 Behörde

	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	<i>Informationssicherheitsleitlinie der Behörde  Rahmen-Sicherheitskonzept der Behörde  Sicherheits- und Betriebskonzept IT-Dienstleister  Grundschutzkonzept für die Informations- und Kommunikationstechnik  Richtlinie zur Datensicherheit im IuK-Bereich  Richtlinie zur Verwaltung von Passwörtern  Geschäftsordnungsbestimmungen der Behörden (Vertretungsregelungen, Vier-Augen-Prinzip)</i>
<b>Intervenierbarkeit</b> Art. 5 Abs. 1 lit. d,f DS-GVO	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister  Richtlinie der Behörde über die Sicherheit der Datenverarbeitung auf Endgeräten</i>
<b>Nichtverkettung</b> Art. 5 Abs. 1 DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	<i>Freigabe-Richtlinie  Service-Level-Agreements  Richtlinie zur Datensicherheit im IuK-Bereich</i>
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister  Berechtigungskonzept des jeweiligen Verfahrens  Richtlinie der Behörde über die Sicherheit der Datenverarbeitung auf Endgeräten  Richtlinie zur Datensicherheit im IuK-Bereich</i>
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister  Sicherheits- und Betriebskonzept Behörde  Geschäftsordnungsbestimmungen der Behörde</i>
	Trennbarkeit (§ 64 Abs. 3 Nr. 14 BSDG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister  Berechtigungskonzepte der jeweiligen Fachverfahren  Grundsätze des Verwaltungshandelns nach Beamtenstatusgesetz bzw. Tarifvertrag (Verschwiegenheitspflicht)</i>
	Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)	<i>Betriebskonzept des jeweiligen Fachverfahrens  Geschäftsordnungsbestimmungen der Behörde</i>
<b>Transparenz</b> Art. 5 Abs. 1 lit. a DS-GVO	Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)	<i>Freigabe-Richtlinie  Service-Level-Agreements  Richtlinie zur Datensicherheit im IuK-Bereich</i>
	Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BSDG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister  Richtlinie zur Verwaltung von Passwörtern  Grundschutzkonzept für die Informations- und Kommunikationstechnik  Geschäftsordnungsbestimmungen der Behörden (Rechte..., Berechtigungskonzept Zugriff...)</i>

	Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister Vorgaben für das Haushalts- und Kassenrecht Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörde</i>
	Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BSDG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister Berechtigungskonzept des jeweiligen Verfahrens Richtlinie der Behörde über die Sicherheit der Datenverarbeitung auf Endgeräten Richtlinie zur Datensicherheit im IuK-Bereich</i>
	Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister Sicherheits- und Betriebskonzept Behörde Geschäftsordnungsbestimmungen der Behörde</i>
	Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)	<i>Informationssicherheitsleitlinie der Behörde Rahmen-Sicherheitskonzept der Behörde Sicherheits- und Betriebskonzept IT-Dienstleister Grundschutzkonzept für die Informations- und Kommunikationstechnik Richtlinie zur Datensicherheit im IuK-Bereich Richtlinie zur Verwaltung von Passwörtern Geschäftsordnungsbestimmungen der Behörde (Vertretungsregelungen, Vier-Augen-Prinzip)</i>
Verfahren <b>regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen</b> Art. 32 Abs. 1 lit. d DS-GVO	-	<i>turnusmäßige Überarbeitung der Richtlinien der Behörde turnusmäßige Überarbeitung des Sicherheitskonzeptes durch IT-Dienstleister</i>
Verfahren zur schnellen <b>Wiederherstellung der Verfügbarkeit</b> personenbezogener Daten nach einem physischen oder technischen Zwischenfall Art. 32 Abs. 1 lit. c DS-GVO	Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)	<i>Sicherheits- und Betriebskonzept IT-Dienstleister Richtlinie der Behörde über die Sicherheit der Datenverarbeitung auf Endgeräten</i>
Gewährleistung der <b>Belastbarkeit der Systeme</b> Art. 32 Abs. 1 lit. b DS-GVO	Verfügbarkeitskontrolle (§ 64 Abs. 3 Nr. 13 BSDG)	<i>Informationssicherheitsleitlinie der Behörde Rahmen-Sicherheitskonzept der Behörde Sicherheits- und Betriebskonzept IT-Dienstleister Geschäftsordnungsbestimmungen der Behörde</i>
	Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)	<i>Informationssicherheitsleitlinie der Behörde Rahmen-Sicherheitskonzept der Behörde Sicherheits- und Betriebskonzept IT-Dienstleister Geschäftsordnungsbestimmungen der Behörde (Vertretungsregelungen, Vier-Augen-Prinzip)</i>

### 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 Störfall 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