Bundesministerium
des Innern

Organisationskonzept elektronische Verwaltungsarbeit

Baustein Datenschutz und Personaldaten

Version 2.0
an die DSGVO und das neue BDSG angepasst sowie erweitert durch
Prof. Dr. Mario Martini
Dezember 2018

Fortschritt sichern
verwaltung-innovativ.de

Dokumentenhistorie

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck und Funktion des Dokuments

Für die öffentliche Verwaltung und ihre Beschäftigten kommt sie einem Herkulesakt gleich: die Umstellung von der analogen Arbeitsweise auf die elektronische Handhabung der Verwaltungsangelegenheiten.

Zentrale Grundsätze über die elektronische Aktenführung und das ersetzende Scannen hat das E-Government-Gesetz formuliert.[1] Es trat am 1. August 2013 in Kraft. Das Gesetz gibt den Behörden des Bundes (einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts) auf, seine Gebote bis 2020 umzusetzen. Dies schließt insbesondere auch den gesetzlichen Anspruch der Betroffenen auf Schutz ihrer personenbezogenen Daten gemäß der EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, „**DSGVO**“) und dem Bundesdatenschutzgesetz (BDSG) ein.[2]

Systeme zur elektronischen Verwaltungsarbeit erfassen, verarbeiten und übermitteln ggf. auf unterschiedliche Weise personenbezogene Daten. Diese Daten können als Primärinformationen in den elektronischen Dokumenten selbst, als Metadaten zu den Dokumenten, Vorgängen und Akten sowie als Bearbeitungs- und Protokollinformationen des elektronischen Geschäftsgangs vorliegen. Sie können dabei unterschiedliche Personen und Persönlichkeitsrechte betreffen.

Im Gegensatz zur Arbeit mit Papierakten stellen elektronische Systeme in der Regel Funktionalitäten bereit, die personenbezogene Daten ohne größeren Aufwand recherchierbar und verknüpfbar machen. Datenschutzrechtliche Gefahren treten insbesondere dann auf, wenn Unbefugte Zugang zu personenbezogenen Daten, die nicht für sie bestimmt sind, sowie wenn die Verwaltung Daten in unzulässiger Weise für Bewertungen oder Entscheidungen verarbeitet.

Dieses Dokument soll den Projektverantwortlichen in den öffentlichen Stellen und öffentlich-rechtlich organisierten Einrichtungen des Bundes eine praktische Hilfestellung zum Thema Datenschutz in Einführungsprojekten der elektronischen Akte und des IT-gestützten Geschäftsgangs sowie zur elektronischen Personalakte („**eP-Akte**“) bieten.

Das allgemeine Vorgehen bei der Planung und Umsetzung von Maßnahmen, welche die datenschutzrechtlichen Anforderungen einhalten sollen (Kapitel 3), orientiert sich an den bestehenden Regelungen und Leitlinien zum Datenschutz auf europäischer sowie auf Bundes- und Landesebene – u. a. an dem vom BSI vorgeschlagenen Vorgehen.[3]

* Besonderer Dank gilt den Forschungsreferenten im Programmbereich »Digitalisierung« am Deutschen Forschungsinstitut für öffentliche Verwaltung, die an der Überarbeitung des Werkes mitgewirkt haben, insbesondere *Leonie Born*, *Arne Brest, Jan Mysegades* – und ganz besonders *David Nink*.

[1] http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/E-Government/E-Government-Gesetz/e-government-gesetz_node.html

[2] Dieses Dokument legt seiner Darstellung die seit dem 25. Mai 2018 geltende Fassung des BDSG zugrunde. Bei Bedarf führt es zusätzlich zur Illustration die bis zum 24. Mai 2018 geltende Fassung des BDSG (Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 10 Abs. 2 des Gesetzes vom 31.10.2017 (BGBl. I S. 3618) auf („BDSG a. F.“).

[3] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01005.html

In Kapitel 4 behandelt der Baustein das Thema Datenschutz im Hinblick auf die Einführung einer eP-Akte. Die rechtlichen Rahmenbedingungen zum Umgang mit Personaldaten finden sich in Kapitel 2.10.

1.2 Einordnung in das Organisationskonzept „Elektronische Verwaltungsarbeit“

Der Datenschutz ist ein grundlegender Bestandteil jedes Einführungsprojekts im Bereich der elektronischen Verwaltungsarbeit. Daher ist er bereits in der Projektvorbereitungsphase unter Beteiligung von Interessenvertretern und Datenschutzbeauftragten zu berücksichtigen und zu planen.[4]

Vor diesem Hintergrund soll dieses Baustein-Dokument zum einen das Vorgehen beschreiben, das zu beachten ist, wenn die Verwaltung Daten verarbeitet. Zum anderen soll es für die Erfassung, Bewertung und Verwaltung von Datenschutzanforderungen verschiedene, allgemein verwendbare Vorlagen bereitstellen, die auf unterschiedliche Projektkontexte anpassbar sind.

Die allgemeinen Aspekte der elektronischen Aktenführung und des elektronischen Geschäftsgangs behandeln die jeweiligen Bausteine des Organisationskonzeptes. Der vorliegende Baustein referenziert sie jeweils an den jeweils geeigneten Stellen. Von besonderer Relevanz sind insbesondere

- die Grundbausteine („E-Akte“, „E-Vorgangsbearbeitung“, „E-Zusammenarbeit“ und „E-Fachverfahren“),
- der Projektleitfaden, an dessen Vorgehen sich das Szenario der Einführung einer elektronischen Personalakte (eP-Akte) in Kapitel 4 anlehnt, sowie
- die Bausteine „Scanprozess“, „E-Poststelle“ und „E-Langzeitspeicherung“.

Abbildung 1: Baukasten Organisationskonzept „Elektronische Verwaltungsarbeit“

[4] Siehe dazu auch im Baustein „Projektleitfaden“ die Anlage 3: Kommunikationsplan.

1.3 Mit der Datenschutz-Grundverordnung verbundene Neuerungen

Seit dem 25. Mai 2018 stellt die DSGVO die entscheidenden Weichen für das in der Bundesrepublik Deutschland geltende Datenschutzrecht. Das BDSG und das bereichsspezifische Datenschutzrecht ergänzen deren Regelungen.

Die DSGVO wälzt das Datenschutzrecht grundlegend um. Das liegt insbesondere an ihrer Rechtsform: Bei ihr handelt es sich um eine unionale Verordnung. Anders als die alte Datenschutzrichtlinie gilt die DSGVO deshalb in jedem Mitgliedstaat unmittelbar; einer mitgliedstaatlichen Umsetzung bedarf es nicht. Nationale Datenschutzregelungen darf der deutsche Gesetzgeber nur schaffen, wenn die DSGVO ihm ausdrücklich einen Regelungsspielraum eröffnet (ErwGrd 8 DSGVO).[5] Andernfalls untergrübe er den Geltungsanspruch der DSGVO und verstieße gegen das europarechtliche Normwiederholungsverbot. Die DSGVO enthält – für eine Verordnung an sich untypisch – zahlreiche Öffnungsklauseln. Aufgrund dieses Charakters als „Hybrid“ zwischen Richtlinie und Verordnung eröffnet die DSGVO den Mitgliedstaaten vergleichsweise weitreichende Regelungsspielräume.[6] Dies gilt namentlich für den Bereich der Datenverarbeitung durch öffentliche Stellen. Der Gesetzgeber hat von dieser Freiheit im neuen BDSG (in der seit dem 25. Mai 2018 geltenden Fassung) sowie in den bereichsspezifischen Regelungswerken umfassend Gebrauch gemacht. Die DSGVO einerseits und das BDSG andererseits stehen nicht beziehungslos nebeneinander. Das geltende Datenschutzrecht erschließt sich dem Normanwender nunmehr oftmals nur durch das Zusammenspiel beider Regelwerke.

Die DSGVO gilt im Grundsatz für öffentliche wie nicht-öffentliche Stellen gleichermaßen. Sie sieht Haftungsverpflichtungen für Verstöße gegen bestimmte Vorschriften (Art. 82) sowie empfindliche Sanktionsmöglichkeiten (Art. 83 ff.) vor. Behörden und sonstigen öffentlichen Stellen drohen indes keine Geldbußen. Das hat der deutsche Gesetzgeber kraft der Öffnungsklausel des Art. 83 Abs. 7 DSGVO so in § 43 Abs. 2 BDSG verfügt. Nichtsdestotrotz wird dem Aspekt der Compliance und der Stellung der Datenschutzbeauftragten auch bzw. gerade in Behörden eine gesteigerte Bedeutung zukommen.

[5] Dazu ausführlich *Kühling/Martini et al.*, Die Datenschutz-Grundverordnung und das nationale Recht, 2017, S. 6 ff.

[6] Dazu *Kühlung/Martini et al.*, Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 2 ff.

2 Allgemeine Aspekte des Datenschutzes in der elektronischen Aktenführung und Vorgangsbearbeitung

2.1 Datenschutzrechtliche Grundsätze

Datenschutz hat die Aufgabe, garantierte und unveräußerliche Persönlichkeitsrechte zu verteidigen, die der Einzelne sowohl gegenüber dem Staat als auch gegenüber anderen gesellschaftlichen Akteuren genießt: Sein Ziel ist es, natürliche Personen bei der Verarbeitung ihrer Daten wirksam zu schützen und dadurch deren persönliche Entfaltung zu ermöglichen (Art. 8 Abs. 1 GrCh, Art. 16 Abs. 1 AEUV, Art. 1 DSGVO).

2.1.1 Grundsätze der DSGVO

Wirksamer Datenschutz impliziert nach der Wertordnung der DSGVO insbesondere die Transparenz und Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 lit. a DSGVO), die Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO, vgl. Kapitel 2.3) sowie Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO).

Das Konzept der **Datenminimierung** (Art. 5 Abs. 1 lit. c DSGVO) fußt auf dem Grundgedanken, dass Daten, die nicht erhoben oder anderweitig verarbeitet werden, das Recht auf informationelle Selbstbestimmung nicht verletzen können. Die datenverarbeitende Stelle hat daher den Umgang mit personenbezogenen Daten auf das Maß zu begrenzen, das für den Zweck der Verarbeitung erforderlich ist. Das ist Ausfluss des Prinzips der Verhältnismäßigkeit. Das deutsche Konzept der **Datensparsamkeit** bzw. **Datenvermeidung** (vgl. § 3a BDSG a. F.) ging im alten Regelungsregime sogar noch einen Schritt weiter: Es waren möglichst keine personenbezogenen Daten oder – wo das nicht möglich ist – möglichst wenige personenbezogene Daten zu verwenden.

2.1.2 Verhältnis zum BDSG und zur Datenschutzrichtlinie Polizei und Justiz

Das BDSG gilt uneingeschränkt für öffentliche Stellen des Bundes[7] und für nichtöffentliche Stellen (Private), sofern diese unter den in § 1 Abs. 1 S. 2 BDSG beschriebenen Anwendungsbereich fallen.

Öffentliche Stellen des Bundes sind ausweislich § 2 Abs. 1 BDSG:

- Behörden des Bundes,
- Organe der Rechtspflege des Bundes,
- andere öffentlich-rechtlich organisierte Einrichtungen im Bundesbereich (z. B. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts unter Bundesaufsicht),
- bestimmte Vereinigungen öffentlicher Stellen des Bundes und bestimmte von diesen beherrschte Unternehmen, Gesellschaften oder Einrichtungen, auch in privater Rechtsform.

Wenn öffentliche Stellen des Bundes grenzüberschreitend innerhalb der Europäischen Union tätig sind, galten für sie bisher die §§ 4b und 4c BDSG a. F.. Seit

[7] Siehe zur bisherigen Rechtslage auch § 18 BDSG a. F. (Durchführung des Datenschutzes in der Bundesverwaltung).

dem 25. Mai 2018 sind insofern – neben Art. 2 und 3 – die Art. 44-50 DSGVO maßgeblich. Im Geltungsbereich der RL (EU) 2016/680 hält das neue BDSG in §§ 78-81 Regelungen bereit.

Datenverarbeitungen der Ermittlungs- und Strafverfolgungsbehörden unterfallen der *Richtlinie (EU) 2016/680* („Justiz und Inneres" – JI-RL). Als Richtlinie gilt sie – anders als die DSGVO – gegenüber Behörden und Bürgern grundsätzlich nicht unmittelbar. Der deutsche Gesetzgeber muss ihre Vorgaben vielmehr in nationales Recht umsetzen. Er hat dies über (die allgemeinen Bestimmungen im ersten Teil des BDSG, §§ 1–21, sowie) §§ 45–84 BDSG getan. Im Verhältnis zum alten Recht bringen sie zahlreiche neue Pflichten mit entsprechendem Erfüllungsaufwand mit sich. Im Bereich des Bundes betrifft dies vorrangig das Zollkriminalamt, die Zollverwaltung, die Bundespolizei, das Bundeskriminalamt, den Generalbundesanwalt und die Bundesgerichte.

2.1.3 Bereichsspezifisches Datenschutzrecht

Der Schutz personenbezogener Daten erschöpft sich normativ keineswegs in der DSGVO und im BDSG. Vielmehr enthalten darüber hinaus sehr viele Einzelgesetze Bestimmungen zum Umgang mit speziellen Arten personenbezogener Daten, etwa:

- das Sozialgesetzbuch (SGB),
- das Bundesverfassungsschutzgesetz (BVerfSchG),
- das Bundespolizeigesetz (BPolG),[8]
- das Telekommunikationsgesetz (TKG),
- das Telemediengesetz (TMG),
- das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz),[9]
- das Gesetz über den militärischen Abschirmdienst (MADG),
- das Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (SÜG).

Das Zweite Datenschutz-Anpassungs- und –Umsetzungsgesetz wird das bereichsspezifische Datenschutzrecht in weiten Teilen an die neue Rechtslage anpassen.[10]

Für die Personalakten[11] in den Stellen und Einrichtungen des Bundes gelten insbesondere:

- das Bundesbeamtengesetz (BBG),
- das Bundespersonalvertretungsgesetz (BPersVG),

[8] Für die Landespolizei halten die Vorschriften der Landesdatenschutzgesetze sowie der Polizeigesetze vergleichbare Regelungen vor.

[9] Hieran plant die Bundesregierung derzeit signifikante Änderungen, vgl. den Entwurf des geplanten Zweiten Gesetzes zur Erhöhung der Sicherheit in informationstechnischen Systemen (IT-Sicherheitsgesetz 2.0), vgl. https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/

[10] BT-Drucks. 19/4674.

[11] Im Kontext der eP-Akte ist zwischen Personaldaten und *Personalaktendaten* zu unterscheiden (siehe dazu Kapitel 2.10). In dem Bereich sind daher auch unterschiedliche Regelwerke einschlägig.

- das Soldatengesetz (SG).

Für die Landes- und Kommunalbehörden beanspruchen z. T. abweichende landesrechtliche Regelungen Geltung. Das Beamtenstatusgesetz (BeamtStG) formuliert insoweit bundeseinheitliche Mindestvorgaben.

Das BDSG versteht sich als **Auffanggesetz**, das in denjenigen Fällen zur Anwendung kommt, in denen keine spezialgesetzlichen Bestimmungen des Bundes zu personenbezogenen Daten vorliegen (vgl. § 1 Abs. 2 BDSG). Im Verhältnis zur DSGVO folgt dies bereits aus deren unmittelbarer Wirkung.

2.2 Verbot mit Erlaubnisvorbehalt (Art. 6 Abs. 1 DSGVO; bislang §§ 4, 4a, 28 BDSG a. F.)

Für die Verarbeitung personenbezogener Daten (Art. 4 Nr. 1 und 2 DSGVO) formuliert das Datenschutzrecht als allgemeinen Grundsatz ein Verbot mit Erlaubnisvorbehalt (Art. 6 Abs. 1 UAbs. 1 DSGVO): Wer Daten verarbeitet, z. B. erhebt, erfasst, organisiert, ordnet, speichert, anpasst oder verändert, durch Übermittlung und Verbreitung offenlegt oder in anderer Form verknüpft, löscht, vernichtet oder bearbeitet, handelt rechtswidrig, es sei denn,

- die betroffene Person hat in die Verarbeitung der sie betreffenden personenbezogenen Daten **eingewilligt** (Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO) oder
- es besteht eine **gesetzliche Verarbeitungserlaubnis**.

Bei der Datenverarbeitung *durch öffentliche Stellen* unterliegt die Einwilligung (Art. 7 DSGVO) sehr strengen Voraussetzungen. Die DSGVO stuft sie typischerweise als nicht „freiwillig“ ein.[12] Denn sie erfolgt unter dem Damoklesschwert anderweitiger hoheitlicher Eingriffsmaßnahmen und damit in einer Konstellation, die ein Machtgefälle zwischen den handelnden Akteuren auslöst. Auch deshalb sind bei der Datenverarbeitung im Verhältnis zwischen Staat und Bürger gesetzliche Verarbeitungserlaubnisse von besonderer Relevanz. Die DSGVO konzipiert fünf gesetzliche Erlaubnistatbestände.

2.2.1 Gesetzliche Verarbeitungserlaubnisse der Union

Die Union behält sich grundsätzlich selbst vor, zu bestimmen, unter welchen Voraussetzungen es zulässig ist, personenbezogene Daten zu verarbeiten. Für drei Tatbestände hat sie unmittelbar eine Erlaubnis ausgesprochen: Die Verarbeitung ist erforderlich,

- um einen Vertrag mit der betroffenen Person zu erfüllen oder vorvertragliche Maßnahmen auf Anfrage der betroffenen Person durchzuführen (Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO),
- um *lebenswichtige Interessen* der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6 Abs. 1 UAbs. 1 lit. d DSGVO) oder
- um unter Berücksichtigung der Interessen, Grundrechte und Grundfreiheiten der betroffenen Person *berechtigte Interessen* des Verantwortlichen oder eines Dritten zu wahren (Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO).

[12] Vgl. ausführlich *Martini/Wenzel*, DVBl 2017, 749 (753). Siehe dazu auch ErwGrd 43 DSGVO.

2.2.2 Gesetzliche Verarbeitungserlaubnisse der Mitgliedstaaten

Ausnahmsweise dürfen auch die **Mitgliedstaaten** (zusätzlich zur Union) kraft ihrer eigenen Regelungshoheit selbst Verarbeitungsbefugnisse schaffen. Das gilt namentlich in zwei Fällen. Sie betreffen klassische Kernbereiche staatlicher Aufgabenerfüllung, die der Regelungsbefugnis der Union Grenzen setzen: Die Verarbeitung ist erforderlich,

- um eine *rechtliche Verpflichtung* des Verantwortlichen[13] zu erfüllen (Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO) oder
- eine Aufgabe wahrzunehmen, die *im öffentlichen Interesse* liegt oder in *Ausübung öffentlicher Gewalt* erfolgt (Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO).[14]

Von diesen Befugnissen hat die Bundesrepublik vor allem in **§ 3 BDSG** Gebrauch gemacht. Die Vorschrift gestattet öffentlichen Stellen die Verarbeitung, wenn dies „zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist“. Die Vorschrift deckt sich weitgehend mit den ehemaligen Erlaubnistatbeständen in § 13 Abs. 1 und § 14 Abs. 1 BDSG a. F.[15]

Anders als das alte BDSG (§ 4 Abs. 2 BDSG a. F.) verpflichten die DSGVO und das neue BDSG nicht dazu, personenbezogene Daten zunächst zwingend beim Betroffenen selbst zu erheben. Ein **Direkterhebungsgrundsatz existiert somit nicht länger**.

Ob der Verantwortliche die Daten beim Betroffenen oder Dritten erhebt, wirkt jedoch auf die **Informationspflicht** zurück: Erhebt er die Daten beim Betroffenen selbst, bestimmt sich diese nach Art. 13 DSGVO, andernfalls nach Art. 14 DSGVO (siehe Kapitel 2.7). Im Rahmen ihrer Informationspflicht muss die datenerhebende Stelle dem Betroffenen mitteilen, zu welchem Zweck sie die Daten erhebt. Ist der Betroffene gegenüber einer öffentlichen Stelle zur Auskunft verpflichtet (z. B. bei amtlichen Statistiken), so ist ihm mitzuteilen, nach welchen Rechtsvorschriften das der Fall ist. Er ist auch darüber aufzuklären, ob er ohne die von ihm verlangten Auskünfte seine Ansprüche nicht durchsetzen kann oder ihm sonstige Rechtsvorteile entgehen.

Möchte der Verantwortliche besondere Arten personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO bzw. § 22 BDSG (bislang § 3 Abs. 9 BDSG a. F.), z. B. Gesundheitsdaten, verarbeiten, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen (Art. 9 Abs. 2 lit. a DSGVO).

---

[13] „Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, Art. 4 Nr. 7 DSGVO; vgl. auch unten im Glossar, Kapitel 6. Im vorliegenden Dokument ist also regelmäßig die öffentliche Stelle gemeint.

[14] Der inhaltsgleiche § 3 BDSG macht von der Öffnungsklausel bzw. dem Regelungsauftrag in Art. 6 Abs. 3 i. V. m. Abs. 1 UAbs. 1 lit. e DSGVO Gebrauch.

[15] *Frenzel*, in: Paal/Pauly, BDSG § 3, Rn. 1 ff., insbesondere Rn. 10, sieht in § 3 BDSG einen Verstoß gegen das unionsrechtliche Normwiederholungsverbot und empfiehlt öffentlichen Stellen, entsprechende Verarbeitungen nicht auf § 3 BDSG, sondern auf Art. 6 Abs. 1 UAbs. 1 lit. c bzw. lit. e DSGVO zu stützen und dies auch jeweils so zu zitieren. Diese Auffassung überzeugt nicht. Denn Art. 6 Abs. 3 S. 1 DSGVO gibt zu erkennen, dass Rechtsgrundlagen im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO einer eigenen Verarbeitungsgrundlage im nationalen oder unionalen Recht bedürfen, die zu Art. 6 Abs. 1 und Abs. 1 lit. e DSGVO hinzutritt („die Rechtsgrundlage […] wird festgelegt durch a) Unionsrecht oder b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt“). Praktische Relevanz entfaltet § 3 BDSG daneben für den Geltungsbereich der RL (EU) 2016/680.

Abbildung 2: System der Verarbeitungserlaubnisse der DSGVO

2.2.3 Sonderfall Datenübermittlung (Art. 20, 44 ff. DSGVO, §§ 25, 74, 78 ff. BDSG; bislang §§ 4b, 4c, 15, 16, 27, 28, 39 BDSG a. F.)

Anders als das BDSG a. F. (vgl. §§ 3 Abs. 4, §§ 15, 16 BDSG a. F.) schlägt die DSGVO die einzelnen Verarbeitungsformen grundsätzlich über einen Leisten: Sie trennt nicht zwischen Erhebung, Speicherung, Veränderung und Übermittlung. Die Übermittlung personenbezogener Daten (innerhalb der Union)[16] behandelt sie grundsätzlich als eine von mehreren Verarbeitungsformen (vgl. Art. 4 Nr. 2 DSGVO). Somit bestimmt die allgemeine Regelung des Art. 6 DSGVO i. V. m. § 3 BDSG maßgeblich darüber, inwieweit öffentlichen Stellen eine Datenübermittlung zulässig ist (siehe hierzu schon Kapitel 2.2). Ein Transfer von Daten lässt sich daher bspw. durch eine Einwilligung des Betroffenen legitimieren (Art. 6 Abs. 1 S. 1 lit. a BDSG). § 25 BDSG ergänzt auf der Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO die gesetzlichen Verarbeitungsgrundlagen.

2.2.3.1 Datenübermittlung im Inland

Übermittelt eine Behörde Daten **an eine öffentliche Stelle**, ist dies zulässig, soweit das erforderlich ist, um die Aufgaben der übermittelnden oder datenempfangenden Stelle zu erfüllen und die Tatbestandsvoraussetzungen des § 23 BDSG vorliegen (§ 25 Abs. 1 BDSG).

Inwieweit Behörden Daten an nicht-öffentliche Stelle übermitteln dürfen, bestimmt sich nach § 25 Abs. 2 BDSG. Die Vorschrift lässt eine Datenübermittlung insbesondere zu, wenn der Dritte als Datenempfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hat und der Betroffene keine schutzwürdigen Interessen am Ausschluss der Übermittlung hat (§ 25 Abs. 2 S. 1 Nr. 2 BDSG). Der Betroffene ist in diesen Fällen zu informieren. Dies gilt nicht, wenn er schon auf andere Weise von der Übermittlung Kenntnis erlangt hat oder die öffentliche Sicherheit einer Unterrichtung im Wege steht.

[16] Für die Datenübermittlung an Drittländer oder internationale Organisationen sehen die Art. 44 ff. DSGVO Sonderregelungen vor. Sie sollen sicherstellen, dass auch bei der Übermittlung in Länder außerhalb der EU ein adäquates Schutzniveau gewährleistet ist, welches das informationelle Selbstbestimmungsrecht vor Aushöhlung schützt.

Wollen Behörden **besondere Kategorien personenbezogener Daten** (Art. 9 DSGVO) übermitteln, sind ergänzend die Vorgaben des § 25 Abs. 3 BDSG zu beachten.

2.2.3.2 Datenübermittlung ins Ausland

Der Datenverkehr **zwischen den Mitgliedstaaten der Europäischen Union** und **den anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum** im Anwendungsbereich des Unionsrechts ist genauso zu behandeln wie der inländische.

Die Übermittlung personenbezogener Daten an **Drittländer (außerhalb der EU) oder an internationale Organisationen** bestimmt sich nach abweichenden Vorgaben. Diese legt das fünfte Kapitel der DSGVO fest (vgl. zum alten Recht §§ 4b und 4c BDSG a. F.): Die Art. 44 ff. DSGVO lassen eine Datenübermittlung in ein „Drittland" zu, wenn der Betroffene kein schutzwürdiges Interesse daran hat, die Übermittlung auszuschließen, und insbesondere in dem Drittland ein angemessenes Datenschutzniveau gewährleistet ist. Ob ein solches angemessenes Datenschutzniveau herrscht, stellt die EU-Kommission durch einen förmlichen Beschluss fest (Art. 45 DSGVO) – für den Datentransfer zwischen der Europäischen Union und den USA bspw. durch den sog. Privacy Shield. Daten in nicht sichere Drittländer zu übermitteln, untersagt die DSGVO nicht generell, bindet dies aber grundsätzlich an geeignete Garantien. Diese können insbesondere in verbindlichen internen Datenschutzvorschriften (sog. Binding Corporate Rules (Art. 46 Abs. 2 lit. b i. V. m. Art. 47 DSGVO) oder in Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DSGVO) bestehen, die ein angemessenes Datenschutzniveau absichern. Im öffentlichen Bereich kann eine Datenübermittlung an Drittländer insbesondere über Art. 49 Abs. 1 lit. d DSGVO gerechtfertigt sein, wonach „wichtige öffentliche Interessen" eine solche Übermittlung rechtfertigen. Dies umfasst insbesondere den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständig sind (ErwGrd 112).

Übermitteln Verantwortliche personenbezogene Daten an ein Drittland, so ist dies im Verzeichnis der Verarbeitungstätigkeiten (Verfahrensverzeichnis, siehe Kapitel 2.9) zu dokumentieren (Art. 30 Abs. 1 lit. e bzw. Abs. 2 lit. c DSGVO).

Für Datenübermittlungen, die im Geltungsbereich der Richtlinie (EU) 2016/680 – also im Rahmen der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung – erfolgen, gelten § 74 BDSG (innerhalb der EU) bzw. §§ 78 ff. BDSG (Übermittlung in Drittstaaten).

2.2.4 Sonderfall besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO, § 22 BDSG; bislang § 3 Abs. 9 BDSG a. F.)

Besondere Arten personenbezogener Daten zeichnen sich durch intensive Ausstrahlungen in die Privatsphäre aus. Der erhöhten persönlichkeitsrechtlichen Sensibilität begegnet die Rechtsordnung mit gesonderten Schutznormen.

2.2.4.1 Definition

Art. 9 Abs. 1 DSGVO (bislang § 3 Abs. 9 BDSG a. F.) definiert als besondere Kategorien personenbezogener Daten:

Angaben über

- die rassische bzw. ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Gesundheit,
- Sexualleben oder sexuelle Orientierung sowie
- genetische Daten oder biometrische Daten zur eindeutigen Identifizierung einer Person.

2.2.4.2 Grundsätzliches Verarbeitungsverbot – Art. 9 Abs. 1 DSGVO

Die DSGVO schränkt die Möglichkeiten, besondere Kategorien personenbezogener Daten zu verarbeiten, besonders stark ein. Ihre Verarbeitung ist grundsätzlich untersagt (Art. 9 Abs. 1 DSGVO).

2.2.4.3 Ausnahmen – Art. 9 Abs. 2 DSGVO

Von dem grundsätzlichen Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO lässt der Unionsgesetzgeber aber zahlreiche Ausnahmen zu. Diese finden sich in Art. 9 Abs. 2 DSGVO. Danach gilt das Verbot aus Abs. 1 in folgenden Fällen nicht:

- ausdrückliche Einwilligung der betroffenen Person,
- besondere arbeits- oder sozialrechtliche Gründe,
- Schutz lebenswichtiger Interessen,
- Verarbeitung durch eine Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht bei Vorliegen geeigneter Datenschutzgarantien, wenn der Betroffene in regelmäßigen Kontakt mit ihr steht,
- die betroffene Person hat die Daten selbst offensichtlich öffentlich gemacht,
- Erforderlichkeit für Rechtsansprüche oder gerichtliche Tätigkeiten,
- erhebliches öffentliches Interesse,
- Erforderlichkeit für Gesundheitsvorsorge oder Arbeitsmedizin,
- öffentliche Gesundheit, insbesondere im Bereich Gesundheitsversorgung sowie Arzneimittel und Medizinprodukte bei Vorliegen geeigneter Datenschutzgarantien, insbesondere des Berufsgeheimnisses,
- Archiv-, wissenschaftliche, historische Forschungs- sowie statistische Zwecke.

Der neue § 22 BDSG enthält weitere Zulässigkeitstatbestände, die den Katalog des Art. 9 Abs. 2 konkretisieren. Sie machen von den Öffnungsklauseln des Art. 9 Abs. 2 lit. b, g, h und i DSGVO Gebrauch. Öffentlichen Stellen ist eine Verarbeitung besonderer Kategorien personenbezogener Daten auf der Grundlage des § 22 Abs. 1 Nr. 1 BDSG dann zulässig,

- wenn sie erforderlich ist, um die Rechte auszuüben, die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsen, und den diesbezüglichen Pflichten nachzukommen (§ 22 Abs. 1 Nr. 1 lit. a BDSG),

- zum Zweck der Gesundheitsvorsorge, um die Arbeitsfähigkeit des Beschäftigten zu beurteilen, für die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder wenn dies aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden (§ 22 Abs. 1 Nr. 1 lit. b BDSG), oder
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (§ 22 Abs. 1 Nr. 1 lit. c).

Sofern die Interessen des Verantwortlichen an der Datenverarbeitung die Interessen der betroffenen Person überwiegen, ist eine Verarbeitung nach § 22 Abs. 1 Nr. 2 BDSG außerdem zulässig, wenn sie erforderlich ist

- aus Gründen eines erheblichen öffentlichen Interesses (§ 22 Abs. 1 Nr. 2 lit. a BDSG),
- um eine erhebliche Gefahr für die öffentliche Sicherheit abzuwehren (§ 22 Abs. 1 Nr. 2 lit. b BDSG),
- um erhebliche Nachteile für das Gemeinwohl abzuwenden oder erhebliche Belange des Gemeinwohls zu wahren (§ 22 Abs. 1 Nr. 2 lit. c BDSG) oder
- aus zwingenden Gründen der Verteidigung oder um über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen zu erfüllen (§ 22 Abs. 1 Nr. 2 lit. d BDSG).

Verarbeitet der Verantwortliche besondere Kategorien personenbezogener Daten, so muss er angemessene und spezifische Maßnahmen ergreifen, welche die Rechte und Interessen des Betroffenen wahren (vgl. Art. 9 Abs. 2 lit. b, g, h, i und j DSGVO, § 22 Abs. 2 S. 1 BDSG). § 22 Abs. 2 S. 2 BDSG listet deren Inhalt und Umfang sowie konkrete Beispiele für entsprechende Maßnahmen – nicht abschließend – auf. Zu ihnen gehören insbesondere

- technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
- Maßnahmen, die gewährleisten, dass nachträglich überprüft und feststellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
- Sensibilisierung der derjenigen, die an den Verarbeitungsvorgängen beteiligt sind,
- Benennung eines Datenschutzbeauftragten,
- Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
- Pseudonymisierung personenbezogener Daten,
- Verschlüsselung personenbezogener Daten,
- Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Ver-

fügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

- ein Verfahren, das die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig, bewertet, überprüft und evaluiert,
- spezifische Verfahrensregelungen, welche die Vorgaben des BDSG sowie der Verordnung (EU) 2016/679 in solchen Fällen sicherstellen, in denen Daten an Dritte übermittelt oder für andere Zwecke verarbeitet werden

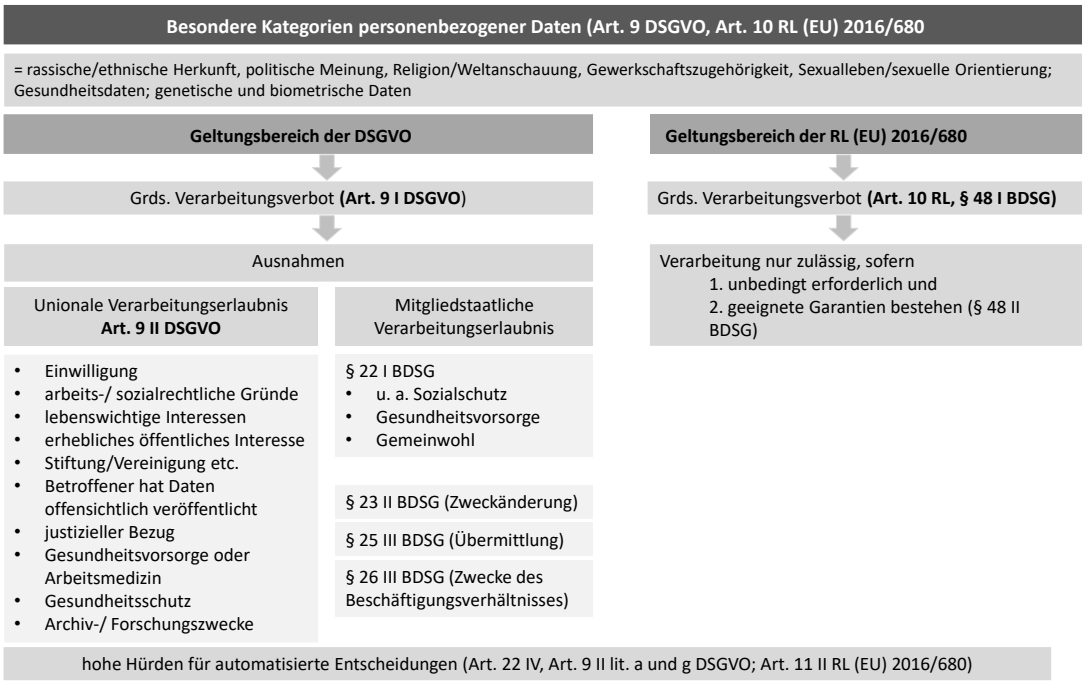

Abbildung 3: Besondere Kategorien personenbezogener Daten

Die Pflicht, für jede Datenverarbeitung geeignete technische und organisatorische Maßnahmen – auch im Hinblick auf die Datensicherheit – zu treffen, ergibt sich zudem bereits aus den allgemeinen Vorschriften des Art. 24 Abs. 1 und 2, Art. 25 Abs. 1 und 2 und Art. 32 Abs. 1 und 4 DSGVO (vgl. Kapitel 2.4).

2.3 Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO; bislang §§ 14, 28 BDSG a. F.)

Öffentliche Stellen dürfen personenbezogene Daten verarbeiten, soweit dies erforderlich ist, um Aufgaben zu erfüllen, die in der Zuständigkeit der verantwortlichen Stelle liegen (§ 3 BDSG).

Sie dürfen die Daten aber grundsätzlich nur zu den Zwecken verarbeiten, für die sie erhoben wurden (Zweckbindungsgrundsatz, Art. 5 Abs. 1 lit. b DSGVO). Der Zweckbindungsgrundsatz der DSGVO ist jedoch weniger strikt als derjenige des BDSG a. F.; er lässt zahlreiche Ausnahmen zu (Art. 6 Abs. 4 DSGVO).[17]

[17] *Albers*, in: BeckOK DatenschutzR DS-GVO, Art. 6, Rn. 68, liest ihn daher als Zweckfestlegungs- und Zweckkompatibilitätsgebot.

2.3.1 Zweckkompatible Verarbeitung

Ob die Verarbeitung dem ursprünglichen Erhebungszweck entspricht, hat der Verantwortliche auf der Grundlage eines **Kompatibilitätstests** zu ermitteln. Dessen Kriterien bestimmt der Unionsgesetzgeber in Art. 6 Abs. 4 lit. a bis e DSGVO. Die Vereinbarkeit zwischen dem Erhebungszweck und dem Zweck der Weiterverarbeitung, bestimmt sich insbesondere,

- daran, inwieweit zwischen den Zwecken der Erhebung und der beabsichtigten Weiterverarbeitung der personenbezogenen Daten eine Verbindung besteht,
- nach dem Zusammenhang der Datenerhebung, insbesondere dem Verhältnis zwischen betroffener Person und Verantwortlichem,
- nach der Art der personenbezogenen Daten, insbesondere ob die Verarbeitung besondere Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO umfasst,
- nach den möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- inwieweit geeignete Garantien bestehen, welche den Schutz der personenbezogenen Daten gewährleisten. Dazu kann insbesondere die Verschlüsselung oder Pseudonymisierung gehören.

Wie die Kriterien des Art. 6 Abs. 4 belegen, ist im Rahmen des Kompatibilitätstests nicht nur die Zweckvereinbarkeit in einem engeren Sinne zu prüfen. Es findet vielmehr eine umfassende Interessenabwägung statt.[18] Die Kriterien des Art. 6 Abs. 4 DSGVO sind zugleich nicht abschließend. Die Zweckkompatibilität kann sich somit grundsätzlich auch aus anderen Gesichtspunkten ergeben oder durch sie ausschließen lassen.

Ergibt eine Gesamtabwägung eindeutig, dass der Erhebungszweck und der Weiterverarbeitungszweck kompatibel ist, ist die Entscheidung über die Zulässigkeit der Weiterverarbeitung der betreffenden Daten gefallen: Die Verarbeitung ist dann zulässig (sofern sie sich auf einen der Rechtfertigungsgründe des Art. 6 Abs. 1 DSGVO stützen kann). Als Ausnahme vom Zweckbindungsgrundsatz ist Art. 6 Abs. 4 DSGVO aber eng auszulegen.[19] Archivzwecke, wissenschaftliche sowie historische Forschungszwecke und statistische Zwecke privilegiert die DSGVO jedoch: Diese gelten kraft Gesetzes als mit dem ursprünglichen Zweck vereinbar (Art. 5 Abs. 1 lit. b Hs. 2 i. V. m. Art. 89 Abs. 1 DSGVO).

2.3.2 Zweckinkompatible Verarbeitung

Erweist sich die Verarbeitung als mit dem ursprünglichen Erhebungszweck **inkompatibel**, steigt die Rechtfertigungslast. Art. 6 Abs. 4 DSGVO belegt die Verarbeitung personenbezogener Daten für einen **anderen als den ursprünglichen Erhebungszweck** mit eigenen Zulässigkeitsvoraussetzungen.

2.3.2.1 Art. 6 Abs. 4 DSGVO

Zweckinkompatible Weiterverarbeitungen sind nur zulässig, wenn

- der Betroffene eingewilligt hat oder

[18] *Martini/Wenzel*, DVBl 2017, 749 (752).

[19] So auch *Buchner/Petri,* in: Kühling/Buchner, DS-GVO, Art. 6, Rn. 186.

- die Verarbeitung auf einer unionalen oder nationalen Rechtsvorschrift beruht, die eine notwendige und verhältnismäßige Maßnahme zum Schutz der Schutzziele des Art. 23 Abs. 1 DSGVO (u. a. nationale Sicherheit; Landesverteidigung; öffentliche Sicherheit; Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten; Strafvollstreckung) darstellt.

Auch die Schutzziele des Art. 23 Abs. 1 DSGVO sind eng auszulegen; eine abstrakte „Verwaltungsvereinfachung“ ist regelmäßig kein Schutzziel in diesem Sinne.[20] Allenfalls Art. 23 Abs. 1 lit. e DSGVO („sonstiger wichtiger Ziele“) kommt als Rechtfertigungsgrund in Betracht. Auch hier reichen aber rein finanzielle Einsparungen nicht aus.

2.3.2.2 Ausfüllung des Rahmens durch das BDSG

Für öffentliche Stellen hat der deutsche Gesetzgeber in **§ 23 BDSG** gesetzliche Ausnahmen vom Zweckbindungsgrundsatz formuliert. Sie machen von der Möglichkeit des Art. 6 Abs. 4 DSGVO Gebrauch: Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist im Rahmen der Aufgabenerfüllung einer öffentlichen Stelle – unabhängig von Art. 6 Abs. 4 DSGVO – auch zulässig in Fällen,

- in denen die *Verarbeitung im Interesse der betroffenen Person* liegt und kein Anlass zu der Annahme besteht, dass die Person ihre Einwilligung in Kenntnis des anderen Zwecks verweigern würde („mutmaßliche Einwilligung“; Abs. 1 Nr. 1),
- in denen tatsächliche Anhaltspunkte dafür bestehen, dass die *Angaben der betroffenen Person nicht richtig* sind und deshalb einer Überprüfung bedürfen (Abs. 1 Nr. 2),
- in denen anderenfalls *erhebliche Nachteile für das Gemeinwohl* oder eine *Gefahr für die öffentliche Sicherheit* bzw. die *nationale Sicherheit* oder Verteidigung, eine *schwerwiegende Beeinträchtigung der Rechte einer anderen Person* eintreten oder *Straftaten bzw. Ordnungswidrigkeiten* oder Maßnahmen zur *Vollstreckung oder zum Vollzug strafrechtlicher Sanktionen* drohen, die sich nicht anders abwehren lassen (Abs. 1 Nr. 3-5),
- der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen (Abs. 1 Nr. 6).

Die Tatbestände in § 23 Abs. 1 BDSG stehen in der festen Tradition des alten Rechts: Sie orientieren sich in Aufbau und Inhalt an dem Katalog des § 14 Abs. 2 BDSG a. F..

Ist keiner der Tatbestände des § 23 BDSG einschlägig, ist die Datenverarbeitung zu einem anderen Zweck als demjenigen, zu dem die personenbezogenen Daten erhoben wurden, unzulässig.

[20] In jedem Fall ist das Anliegen, bestimmten Verantwortlichen den mit der Erfüllung einzelner Betroffenenrechte verbundenen Aufwand zu ersparen, für sich genommen kein tauglicher Beschränkungszweck, vgl. *Bäcker*, in: Kühling/Buchner, DS-GVO, Art. 23, Rn. 12. Materielle Grenze der Beschränkung von Betroffenenrechten ist der Verhältnismäßigkeitsgrundsatz.

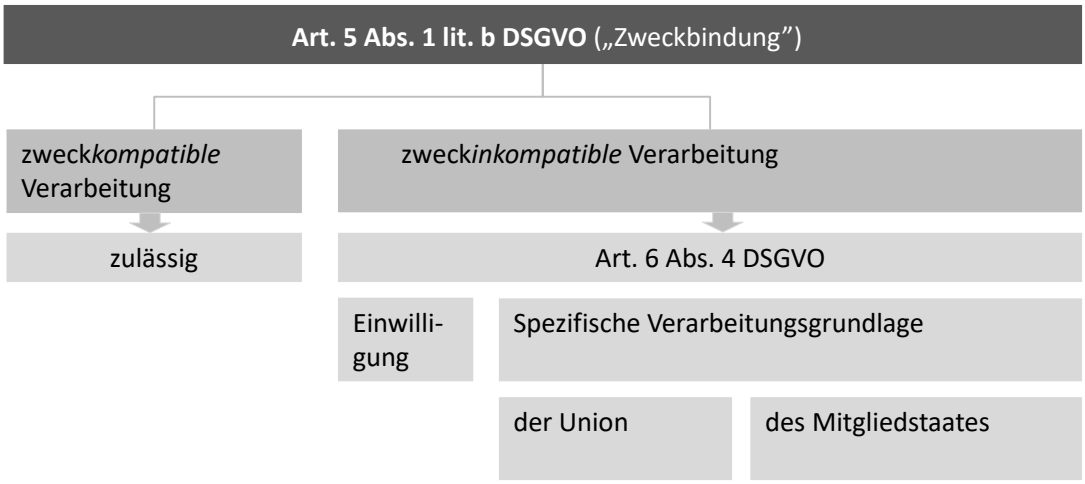

Abbildung 4: Zweckbindungsgrundsatz nach der DSGVO

Auch für die Weiterverarbeitung besonderer Kategorien personenbezogener Daten kann der Gesetzgeber per Gesetz von der Beachtung des Zweckbindungsgrundsatzes dispensieren (Art. 6 Abs. 4 DSGVO). Von dieser Möglichkeit hat der deutsche Gesetzgeber in § 23 Abs. 2 BDSG Gebrauch gemacht: Zulässig ist hiernach eine zweckinkompatible Weiterverarbeitung, sofern die Voraussetzungen des § 23 Abs. 1 BDSG vorliegen (siehe dazu Kapitel 2.3.2) und ein Ausnahmetatbestand nach Art. 9 Abs. 2 DSGVO oder nach § 22 BDSG vorliegt.

2.4 Technische und organisatorische Sicherung des Datenschutzes sowie der Datensicherheit (Art. 24, 25 und 32 DSGVO; bislang §§ 3a, 9, 9a, 10 BDSG a. F.)

2.4.1 Grundpflichten des Verantwortlichen (Art. 24 und 25 DSGVO)

Datenschutzes ist keine „End-of-pipe-Aufgabe". Verantwortliche müssen vielmehr schon bei der Konzeption von IT-Systemen die Belange des Datenschutzes berücksichtigen („**Privacy by Design**" – Art. 25 Abs. 1 DSGVO). Sie müssen ihre Verarbeitung an den Datenschutzgrundsätzen (Art. 5 DSVO) ausrichten und deren Einhaltung durch geeignete technische und organisatorische Maßnahmen absichern, um ein (dem Risiko) angemessenes Schutzniveau für die Betroffenen zu gewährleisten (Art. 25 Abs. 1 DSGVO). Der Unionsgesetzgeber verlangt dem Verantwortlichen dabei zugleich keine Maßnahmen ab, welche die Grenze der Verhältnismäßigkeit überschreiten. Vielmehr sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen in Rechnung zu stellen. Welche Maßnahmen schlussendlich notwendig sind, hängt sowohl von der Art der Daten als auch von der Aufgabe, den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen der Verarbeitung ab.

2.4.2 Anforderungen an die Datensicherheit (Art. 32-34 DSGVO)

2.4.2.1 Art. 32 DSGVO

Ein besonderes Maß an Schutzmaßnahmen verlangt der Unionsgesetzgeber Verantwortlichen und Auftragsverarbeitern mit Blick auf die Datensicherheit ab (Art. 32 Abs. 1 DSGVO). Sie haben mit dieser Zielrichtung geeignete technische und organisatorische Maßnahmen zu treffen. Diese schließen typischerweise[21] ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO);
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (Art. 32 Abs. 1 lit. b DSGVO);
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DSGVO);
- ein Verfahren, um die Wirksamkeit der technischen und organisatorischen Maßnahmen, welche die Sicherheit der Verarbeitung gewährleisten sollen, regelmäßig zu überprüfen, zu bewerten und zu evaluieren (Art. 32 Abs. 1 lit. d DSGVO). Insbesondere diese Anforderung eines dreiteiligen Sicherheitskonzepts integriert eine bedeutende Neuerung der technisch-organisatorischen Seite des Datenschutzes im Vergleich zur alten Rechtslage: Ohne es explizit zu benennen, legt die Regelung Verantwortlichen und Auftragsverarbeitern de facto nahe, ein IT-Sicherheitsmanagementsystem (Information Security Management System, **ISMS**) zu etablieren.[22]

2.4.2.2 Melde- und Benachrichtigungspflichten (Art. 33 und 34 DSGVO)

2.4.2.2.1. Meldepflicht gegenüber der Aufsichtsbehörde (Art. 33 DSGVO)

Kommt es trotz der Schutzmaßnahmen, die Art. 32 DSGVO fordert, zu einer Datenschutzverletzung (Art. 4 Nr. 12 DSGVO), aufgrund derer der Verantwortliche ein Risiko für die Rechte und Freiheiten der Betroffenen nicht ausschließen kann, so muss er die Datenschutzverletzung der zuständigen Aufsichtsbehörde unverzüglich[23] melden (Art. 33 Abs. 1 S. 1 DSGVO).[24] In der Meldung an die Aufsichtsbehörde muss der Verantwortliche folgende Informationen bereitstellen:

---

[21] Die in Art. 32 Abs. 1 Hs. 2 DSGVO aufgezählten Schutzmaßnahmen sind gesetzliche Regelbeispiele. Im konkreten Anwendungsfall kann der wirksame Schutz Betroffener weitere Maßgaben gebieten. Vgl. Martini, in: Paal/Pauly, DS-GVO Art. 32, Rn. 30 ff.

[22] A. A. *Schläger*, in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, 2018, Teil G, Rn. 5 f. (S. 478). Die Kommentarliteratur zu Art. 32 DSGVO liest aus der Norm keine explizite Pflicht heraus, ein ISMS zu implementieren. Dem Verordnungsgeber war es aber ein Anliegen, Datensicherheits- bzw. IT-Sicherheitsmanagement und Datenschutzmanagement auch normativ einander anzunähern und zusammenzubringen. Die entsprechenden Anforderungen gehen spürbar über die sog. "Acht Gebote" der alten Rechtslage (vgl. die Anlage zu § 9 BDSG a. F.) – Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, zweckbezogenes Trennungsgebot – hinaus. Obligatorisch ist insbesondere eine *regelmäßige* interne Kontrolle, wie wirksam die technischen und organisatorischen Maßnahmen sind – etwa anhand von Penetrationstests, die einen Systemangriff simulieren, (vgl. *Jandt*, in: Kühling/Buchner, DS-GVO Art. 32, Rn. 29; *Martini*, in: Paal/Pauly, DS-GVO Art. 32, Rn. 44).

[23] Die Meldung sollte zumindest innerhalb von 72 Stunden erfolgen (Art. 33 Abs. 1 S. 2 DSGVO; ErwGrd 85 DSGVO).

[24] Auftragsverarbeiter müssen Datenschutzverletzungen an den Verantwortlichen melden (Art. 33 Abs. 2 DSGVO) und ihn bei dessen Meldung an die Aufsichtsbehörde unterstützen (Art. 28 Abs. 3 lit. f DSGVO).

- die Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze (Art. 33 Abs. 3 lit. a DSGVO);
- die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3 lit. c DSGVO);
- die Maßnahmen, die er ergriffen oder vorgeschlagen hat, um die Verletzung des Schutzes personenbezogener Daten zu beheben und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen (Art. 33 Abs. 3 lit. d DSGVO).

Zudem muss er den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen (Art. 33 Abs. 3 lit. b DSGVO) angeben.

2.4.2.2.2. Benachrichtigung Betroffener

Zieht die Datenschutzverletzung voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten der **Betroffenen** nach sich, das der Verantwortliche nicht unverzüglich eindämmen kann (Art. 34 Abs. 3 lit. b), so hat er nicht nur die Aufsichtsbehörde, sondern auch jene unmittelbar über die Datenschutzverletzung zu benachrichtigen (Art. 34 Abs. 1 DSGVO). Dabei muss er sich einer einfachen und klaren Sprache bedienen (Art. 34 Abs. 2 DSGVO i. V. m. Art. 12 DSGVO).

Der Umfang der Benachrichtigung entspricht in weiten Teilen dem der Meldung an die Aufsichtsbehörden (Art. 34 Abs. 2 DSGVO). Anders als im Falle des Art. 33 DSGVO muss er die Betroffenen jedoch nur über die Art der Verletzung des Schutzes ihrer Daten informieren (Art. 34 Abs. 2 DSGVO); Informationen über die Kategorien und die ungefähre Zahl der betroffenen Personen, die betroffenen Kategorien und die ungefähren Zahl der betroffenen personenbezogenen Datensätze muss die Benachrichtigung (so aber Art. 3 Abs. 3 lit. a DSGVO für die Meldung an die Behörden) aber nicht enthalten.

Wäre es unverhältnismäßig aufwendig, die betroffenen Personen zu benachrichtigen, reicht stattdessen eine „öffentliche Bekanntmachung oder ähnliche Maßnahme“ aus, um die Betroffenen adäquat („vergleichbar wirksam“) zu informieren (Art. 34 Abs. 3 lit. c DSGVO).

2.5 Datenschutz-Folgenabschätzung (Art. 35 Abs. 1 DSGVO; bislang Vorabkontrolle nach §§ 4d Abs. 5 und 6 BDSG a. F.)

Vor besonders risikobehafteten Verarbeitungsvorgängen hat der Verantwortliche deren Folgen umfassend zu analysieren (Art. 35 Abs. 1 DSGVO; zu Inhalt und Vorgehensweise vgl. auch die Kapitel 3.1, 4.7.3 und 5.1). Dies ist Ausfluss des risikobasierten Ansatzes, der im neuen unionalen Datenschutzrecht deutlich sichtbarer hervortritt.

Anders als die Vorabkontrolle des alten Rechts (§ 4d Abs. 5 BDSG a. F.) – die im neuen Datenschutzregime ersatzlos entfällt – ist die Pflicht, eine Datenschutz-Folgenabschätzung vorzunehmen nicht auf automatisierte Verfahren beschränkt. Sie erfasst vielmehr **alle Verarbeitungen mit hohem Risiko**.

2.5.1 Voraussetzungen

Ob das hohe Risiko, an welches Art. 35 Abs. 1 die Pflicht zur Datenschutz-Folgenabschätzung knüpft, besteht, bestimmt sich nach einer Prognoseentscheidung: Es kommt darauf an, ob mit hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten natürlicher Personen droht. Droht ein hoher Schaden, genügt eine geringe Eintrittswahrscheinlichkeit. Bei hoher Wahrscheinlichkeit genügt spiegelbildlich bereits ein geringer zu erwartender Schaden.

Ein hohes Risiko kann sich aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ergeben; neue Technologien implizieren regelmäßig ein hohes Risiko (Art. 35 Abs. 1 S. 1 DSGVO). **Typische Risiken**, die mit einer Verarbeitung personenbezogener Daten einhergehen, sind die Vernichtung, der Verlust, die Veränderung oder die unbefugte Offenlegung personenbezogener Daten bzw. der unbefugte Zugang zu ihnen sowie die Diskriminierung von Personen, finanzielle Verluste, Rufschädigung oder Profilbildung mit Standortdaten (vgl. ErwGrd 85 S. 1 DSGVO).

Eine Datenschutz-Folgenabschätzung ist insbesondere erforderlich

- bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf eine automatisierte Verarbeitung (einschließlich Profiling) gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- wenn ein System in reichem Umfang besonderer Kategorien personenbezogene Daten im Sinne des Art. 9 Abs. 1 DSGVO oder personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO verarbeitet sowie
- wenn der Verarbeitungsprozess damit einhergeht, öffentlich zugängliche Bereiche systematisch zu überwachen.

Die Aufsichtsbehörden erstellen und veröffentlichen Listen derjenigen Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung obligatorisch ist (**Positivlisten**).[25] Umgekehrt können sie auch Listen von Verarbeitungsarten herausgeben, für die eine Datenschutz-Folgenabschätzung nicht erforderlich ist (**Negativlisten**).

Inhaltliche Orientierung bieten daneben auch die „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 wahrscheinlich ein hohes Risiko mit sich bringt“ der Art.-29-Datenschutzgruppe bzw. des Europäischen Datenschutzausschusses.[26]

[25] Eine abgestimmte Liste der DSK für den nicht-öffentlichen findet sich hier unter https://www.lfd.niedersachsen.de/download/134415/DSFA_Muss-Liste_fuer_den_nicht-oeffentlichen_Bereich.pdf. Die einzelnen Aufsichtsbehörden der Länder haben überwiegend auch eigene Listen veröffentlicht. Die entsprechende Liste des BfDI findet sich unter https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/ListeVerarbeitungsvorgaenge.html.

[26] Siehe *Art.-29-Datenschutzgruppe*, WP 248. Der Europäische Datenschutzausschuss hat die Arbeitspapiere und Positionen der Art.-29-Gruppe ausdrücklich bestätigt und übernommen. Alle Leitlinien und Empfehlungen sind abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en. Auch die Datenschutzkonferenz hat Kurzpapiere zur Datenschutz-Folgenabschätzung sowie zum Risikobegriff herausgegeben; abrufbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html.

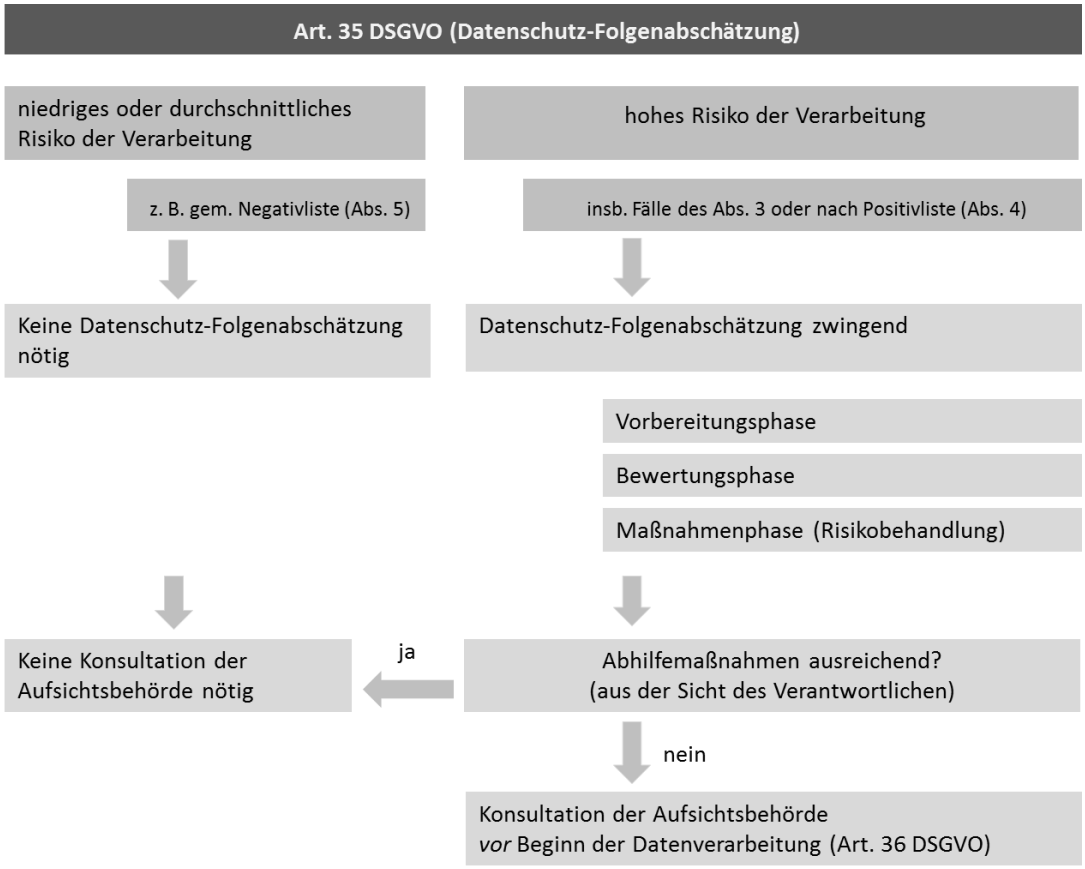

Abbildung 5: Notwendigkeit und Ablauf einer Datenschutz-Folgenabschätzung (Überblick)

Insbesondere für Datenverarbeitungen, die im öffentlichen Interesse liegen bzw. die in Ausübung öffentlicher Gewalt erfolgen, normiert Art. 35 Abs. 10 DSGVO eine Öffnungsklausel: Die Mitgliedstaaten können davon von dem Erfordernis einer Folgenabschätzung dispensieren, wenn zwei Voraussetzungen vorliegen, nämlich wenn

- die Rechtsgrundlage der Verarbeitung sich auf Art. 6 Abs. 1 UAbs. 1 lit. c oder e stützt
- und bereits im Zusammenhang mit dem Erlass dieser Rechtsgrundlage (z. B. bei einer Gesetzesfolgenabschätzung) eine Datenschutz-Folgenabschätzung, z. B. eine Gesetzesfolgenabschätzung, erfolgte,.

Für Datenverarbeitungen im **Geltungsbereich der Richtlinie (EU) 2016/680** hat der deutsche Gesetzgeber mit § 67 BDSG die Pflicht normiert, eine Datenschutz-Folgenabschätzung durchzuführen. Diese erstreckt sich jedoch nur auf neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden. Hinsichtlich ihres Aufbaus und Inhalts orientiert sich diese Folgenabschätzung zudem stark an Art. 35 DSGVO.[27]

2.5.2 Verfahren

Für die Durchführung der Datenschutz-Folgenabschätzung ist die datenverarbeitende Stelle selbst verantwortlich. Sie holt den Rat ihres Datenschutzbeauftrag-

[27] Vgl. BT-Drs. 18/11325, S. 117.

ten ein – sofern ein solcher benannt wurde (Art. 35 Abs. 2 DSGVO). Darin liegt ein Unterschied zum alten Recht: Für die Vorabkontrolle (§ 4d Abs. 5 und 6 BDSG a. F.) war bislang der Datenschutzbeauftragte zuständig. Siehe dazu im Einzelnen Kapitel 3.1.

2.6 Datenverarbeitung im Auftrag (Art. 28 DSGVO; bislang §§ 3 Abs. 7, 11 BDSG a. F.)

Entschließt sich eine Stelle, Tätigkeiten an Dritte auszulagern, die auch die Verarbeitung personenbezogener Daten beinhalten, ist sie besonderen technischen und organisatorischen (Zulässigkeits-)Anforderungen unterworfen. Denn jede Einschaltung weiterer Personen in den Verarbeitungsprozess birgt ein zusätzliches Risiko für das Recht auf informationelle Selbstbestimmung der Betroffenen.

2.6.1 Wesen der Auftragsverarbeitung

Ein wichtiges Instrument des Verantwortlichen, Datenverarbeitungen nicht in eigener Person bzw. im eigenen Unternehmen vornehmen zu müssen, ist die Auftragsverarbeitung: Der Verantwortliche kann mit ihrer Hilfe die Verarbeitungsprozesse auf einen Außenstehenden auslagern. Auftragsverarbeiter kann jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle sein, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSGVO). Damit ist der Kern der Auftragsverarbeitung benannt: Der Auftragsverarbeiter verarbeitet die Daten nicht aus eigenem Antrieb und eigenem Gutdünken, sondern führt einen Auftrag des Verantwortlichen aus. Aus diesem Grunde unterliegt er dabei auch den Weisungen des Verantwortlichen (vgl. Art. 29; Art. 28 Abs. 2 UAbs. 1 S. 2 lit. a DSGVO). Nur der Verantwortliche bestimmt über die Zwecke und Mittel der Verarbeitung (vgl. auch Art. 28 Abs. 10 DSGVO).

Beispiele für die Datenverarbeitung im Auftrag sind:

- der Betrieb eines Rechenzentrums im Auftrag,
- die Entsorgung von Datenträgern,
- der technische Betrieb einer virtuellen Poststelle.

Überlässt der Verantwortliche dem Auftragnehmer (also dem Auftragsverarbeiter) personenbezogene Daten zu einem solchen Zweck, findet aus datenschutzrechtlicher Sicht keine Datenübermittlung statt. Es bedarf dann auch keines Rechtfertigungsgrundes im Sinne des Art. 6 DSGVO. Der Auftragnehmer ist nicht Dritter i. S. d. Art. 4 Nr. 10 DSGVO. Darin liegt die zentrale **Privilegierungswirkung**, welche die Rechtsordnung der Auftragsverarbeitung zugesteht.[28]

Gegenüber den betroffenen Personen ist der Auftraggeber voll dafür verantwortlich, dass die personenbezogenen Daten rechtmäßige Behandlung erfahren. Der Auftragnehmer haftet nur dann, wenn er solchen Pflichten nicht nachgekommen ist, die ihn speziell als Auftragsverarbeiter treffen, oder eine rechtmäßig erteilte Weisung nicht beachtet hat (Art. 82 Abs. 2 S. 2 DSGVO).

[28] Ob diese Privilegierungswirkung auch unter der DSGVO fortbesteht, ist nicht unumstritten. Vgl. dazu *Martini*, in: Paal/Pauli, DS-GVO Art. 28, Rn. 8a m. w. N.

2.6.2 Abgrenzung zur gemeinsamen Verantwortlichkeit und zur Funktionsübertragung

Die Weisungsbindung unterscheidet die Auftragsverarbeitung von der gemeinsamen Verantwortlichkeit (Art. 26 DSGVO) und der(jedenfalls unter dem BDSG a.F. bestehenden) Rechtsfigur der Funktionsübertragung.

2.6.2.1 Gemeinsame Verantwortlichkeit

Bei der gemeinsamen Verantwortlichkeit bestimmen zwei oder mehrere Verantwortliche *gemeinsam* über die Zwecke und Mittel der Verarbeitung (Art. 26 Abs. 1 S. 1 DSGVO).

2.6.2.2 Funktionsübertragung

Die Funktionsübertragung[29] kennzeichnet sich dadurch, dass eine andere Stelle für den Verantwortlichen tätig wird, ohne mit diesem *gemeinschaftlich* die Zwecke und Mittel der Verarbeitung zu bestimmen. Sie verfügt über eine eigenständige Entscheidungsgewalt hinsichtlich der Zwecke und Mittel der Verarbeitung. Weder das BDSG noch die DSGVO regeln die Funktionsübertragung ausdrücklich. Unter dem Regime der DSGVO lässt sie sich womöglich als rechtfertigungsbedürftige Datenübermittlung an eine andere verantwortliche Stelle einzustufen.[30]

Die Konferenz der Datenschutzbeauftragten[31] sieht diese Rechtsfigur mit Inkrafttreten der DSGVO demgegenüber überholt. Neben der gemeinsamen Verantwortlichkeit des Art. 26 DSGVO und der Auftragsverarbeitung bleibe für sie kein Raum. Insbesondere schließe die Auftragsverarbeitung nicht aus, dass dem Beauftragten Entscheidungsspielräume verbleiben.

2.6.3 Wirksamkeitsvoraussetzungen und Rechtspflichten des Auftraggebers bzw. Auftragnehmers

Ein wirksames Auftragsverhältnis setzt voraus, dass der Auftraggeber einen schriftlichen Auftrag erteilt.[32] Dieser muss insbesondere den Gegenstand, die Dauer sowie Art und Zweck der Verarbeitung und der verarbeiteten Daten bezeichnen und den Auftragsverarbeiter an die Weisungen des Verantwortlichen binden (Art. 28 Abs. 3, Art. 29 DSGVO).

Der Auftraggeber muss die geeigneten technischen und organisatorischen Maßnahmen, insbesondere zur Datensicherheit, vorgeben. Umgekehrt muss der Auftragnehmer Gewähr dafür bieten, dass er die Anforderungen der DSGVO an den Schutz personenbezogener Daten einhält (Art. 28 Abs. 1 DSGVO).

Der Auftraggeber muss sich vor Beginn der Datenverarbeitung und in der Folge regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen. Das Ergebnis dieser Überprüfung ist zu dokumentieren.

---

[29] Ausführlicher hierzu *Martini/Fritzsche*, NVwZ-Extra 21/2015, 1 (6 f.).

[30] *Martini*, in: Paal/Pauly, DS-GVO Art. 28, Rn. 7.

[31] *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Kurzpapier Nr. 13: Auftragsverarbeitung, S. 1.

[32] Was genau schriftlich zu regeln ist, legt Art. 28 Abs. 3 DSGVO detailliert fest; im Umfang des Art. 28 Abs. 6 DSGVO sind auch Standardvertragsklauseln zulässig.

Um die Übereinstimmung des Auftragsverhältnisses mit den Anforderungen der DSGVO sicherzustellen und Bürokratiekosten zu sparen sowie Rechtssicherheit herzustellen, kann es sich empfehlen, dem Auftragsverhältnis sog. Standardvertragsklauseln zugrunde zu legen. Diese beschließt die EU-Kommission bzw. die nationale Aufsichtsbehörde auf der Grundlage des Art. 28 Abs. 6–8 DSGVO (im Einklang mit dem Kohärenzverfahren gem. Art. 63 DSGVO).[33]

2.6.4 Neue Anforderungen der DSGVO an den Auftragsverarbeiter

Die DSGVO nimmt den Auftragsverarbeiter (Auftragnehmer) stärker in die Pflicht als das BDSG a. F.. Vielen datenschutzrechtlichen Verpflichtungen, die bislang lediglich den Verantwortlichen trafen, muss nunmehr auch der Auftragsverarbeiter selbst nachkommen. Dies sind insbesondere

- die Pflicht, (in den Fällen des Art. 3 Abs. 2 DSGVO) einen (unionalen) Vertreter („Repräsentanten“) in der Union zu bestellen (Art. 27 Abs. 1 DSGVO),
- die Pflicht, ein Verfahrensverzeichnis zu führen (Art. 30 Abs. 2 DSGVO),
- die Pflicht, mit der Aufsichtsbehörde zusammenzuarbeiten (Art. 31 DSGVO),
- die Pflicht, technische und organisatorische Maßnahmen der Datensicherheit zu ergreifen (Art. 32 Abs. 1 DSGVO),
- die Pflicht, eine Verletzung des Schutzes personenbezogener Daten (an den Verantwortlichen) unverzüglich zu melden (Art. 33 Abs. 2 i. V. m. Art. 4 Nr. 12 DSGVO);
- die Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 1 DSGVO) sowie
- Beschränkungen für den Datentransfer in Drittländer einzuhalten (Art. 44 DSGVO).

2.6.5 Auftragsverarbeitung bei datenverarbeitenden Tätigkeiten der Polizei- und Strafverfolgungsbehörden

Im Anwendungsbereich der RL (EU) 2016/680 – also in Fällen der Auftragsverarbeitung bei Datenverarbeitungsvorgängen der Polizei- und Strafverfolgungsbehörden – enthält § 62 BDSG dem Art. 28 DSGVO vergleichbare Regelungen.

2.7 Betroffenenrechte

Im Verhältnis zum BDSG hat die DSGVO die Betroffenenrechte weiter ausgebaut. Sie regelt diese in ihrem Kapitel III (Art. 12 ff.). Das BDSG hält in seinen §§ 32 ff. teilweise abweichende oder ergänzende Regelungen vor.

Für den Anwendungsbereich der RL (EU) 2016/680 gelten – vorbehaltlich bereichsspezifischer Regelungen (etwa u. a. im BPolG oder im BVerfSchG) – die §§ 55 ff. BDSG.

[33] Entsprechende Standardvertragsklauseln sind, sobald sie festgelegt wurden, abrufbar auf den Internetpräsenzen der Datenschutz-Aufsichtsbehörden sowie des Europäischen Datenschutzausschusses (siehe etwa https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360). Hilfreiche Dokumente und Leitfäden bietet auch die Materialiensammlung der Gesellschaft für Datenschutz und Datensicherheit e. V., vgl. https://www.gdd.de/links.

Abbildung 6: Betroffenenrechte im Geltungsbereich der DSGVO (Überblick)

Betroffene über ihre Rechte „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu unterrichten (Art. 12 Abs. 1 S. 1 DSGVO), ist der DSGVO ein besonderes Anliegen. Sie folgt damit einem Informationsmodell, das der Rechtsordnung bereits aus dem Verbraucherschutzrecht (z. B. beim Widerruf von Fernabsatzverträgen, bei Versicherungen sowie bei Finanzmarktgeschäften) vertraut ist. Die Modalitäten, in denen der Verantwortliche Betroffene auf ihre Rechte aufmerksam zu machen hat, bündelt Art. 12 DSGVO.

2.7.1 Informationspflichten (Art. 13, 14 DSGVO, §§ 32, 33 BDSG; bislang §§ 4 Abs. 3, 19a, 33 BDSG a. F.)

Nur diejenige, der darum weiß, dass seine personenbezogenen Daten Gegenstand der Verarbeitung sind, kann seine informationelle Selbstbestimmung sachgerecht ausüben. Dies sicherzustellen, ist die Mission der Informationspflichten der Art. 12 ff. DSGVO. Inhalt und Umfang dieser Verpflichtung richten sich danach, ob die Daten bei der betroffenen Person selbst (Art. 13 DSGVO) oder nicht bei dieser (Art. 14 DSGVO) erhoben wurden.

2.7.1.1 Direkterhebung (Art. 13 DSGVO)

Sofern der Verantwortliche die Daten direkt bei der betroffenen Person erhebt, sind mitzuteilen (**Art. 13 Abs. 1 DSGVO**):

- der Name und die Kontaktdaten des Verantwortlichen (und ggf. seines Vertreters) sowie ggf. die Kontaktdaten des Datenschutzbeauftragten (lit. a und b);
- die Zwecke und Rechtsgrundlagen der Datenverarbeitung (lit. c);
- die berechtigten Interessen, die der Verantwortliche bzw. Dritte verfolgt, wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO beruht[34] (lit. d);
- ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (lit. e) und
- ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie Informationen zu einem Angemessenheitsbeschluss der Kommission bzw. ein Verweis auf die geeigneten oder angemessenen Garantien (im Falle von Übermittlungen gemäß Art. 46 oder Art. 47 oder Art. 49 Abs. 1 UAbs. 2 DSGVO) und ein Hinweis darauf, wie und wo eine Kopie erhältlich ist (lit. f).

Art. 13 Abs. 2 DSGVO erlegt Verantwortlichen *zusätzliche*, konkrete Aufklärungspflichten auf. Sie sollen dem Betroffenen dazu befähigen, seine Rechte wahrnehmen zu können, und auf diese Weise eine faire und transparente Verarbeitung gewährleisten. Zu den Hinweispflichten gehören die Information über die **Speicherdauer** der Daten (lit. a) sowie über **vollständig automatisierte Entscheidungsfindung**: Der Verantwortliche muss darüber informieren, falls eine solche Form der Verarbeitung stattfindet und welcher Logik und Tragweite des Entscheidungssystem folgt (lit. f).[35]

In den Pflichtenkatalog des Art. 13 Abs. 2 DSGVO fallen darüber hinaus Informationen über das Recht auf Auskunft, auf Berichtigung oder Löschung, Datenportabilität sowie das Recht, der Verarbeitung zu widersprechen (jeweils lit. b) – ferner ggf. auf das Recht, im Falle der Art. 6 Abs. 1 UAbs. 1 lit. a oder Art. 9 Abs. 2 DSGVO die Einwilligung zu widerrufen (lit. c), das Recht, Beschwerde bei der Aufsichtsbehörde einzulegen (lit. d) sowie darüber, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist (lit. e).

Beabsichtigt der Verantwortliche die Daten zu einem **anderen als dem ursprünglichen Erhebungszweck** weiterzuverarbeiten, hat er die betroffene Person vor der Weiterverarbeitung über den neuen Zweck zu unterrichten und ihr alle maßgeblichen Informationen i. S. d. Abs. 2 mitzuteilen (Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO).

Wenn der Betroffene bereits über die Informationen verfügt, entfällt die Informationspflicht (Art. 13 Abs. 4 DSGVO).

Die Art. 12 ff. DSGVO belassen den Mitgliedstaaten nur in sehr geringem Umfang Regelungsspielraum. Art. 23 gestattet ihnen, die Betroffenenrechte aus bestimmten Gründen (lit. a-lit. j) einzuschränken, sofern dies nicht den Wesensgehalt der Grundrechte und Grundfreiheiten missachtet und sich die Maßnahme als in einer demokratischen Gesellschaft notwendig und verhältnismäßig erweist. Auf dieser Grundlage trifft das BDSG zahlreiche Regelungen, welche die Informationspflichten der DSGVO einschränken (§§ 32 f. BDSG). § 32 BDSG bezieht sich auf die Informationspflicht aus Art. 13 Abs. 3 DSGVO über eine Weiterverarbei-

[34] Siehe unter Kapitel 2.2.1.

[35] Relevant ist das z. B. für öffentliche Stellen, die Verwaltungsakte vollautomatisiert erlassen (§ 35a VwVfG); Betroffene sind hierüber gesondert zu informieren. Vgl. zum grundsätzlichen Verbot des Art. 22 DSGVO Kapitel 2.7.4.

tung zu einem anderen Zweck; § 33 BDSG regelt Ausnahmen zu Art. 14 Abs. 1, 2 und 4 DSGVO. So schränkt § 32 Abs. 1 BDSG die Pflicht zur Information über eine Zweckänderung zusätzlich zu Art. 13 Abs. 4 DSGVO ein

- in spezifischen Fällen nicht-digitaler Weiterverarbeitung (nach Interessenabwägung),
- sofern die Information die ordnungsgemäße Erfüllung einer Aufgabe im Sinne des Art. 23 Abs. 1 lit. a-e DSGVO (nach Interessenabwägung) gefährdete,
- bei Gefährdung der öffentlichen Sicherheit oder Ordnung (nach Interessenabwägung),
- soweit die Information die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche (nach Interessenabwägung) gefährdet,
- soweit die Information über die Weiterverarbeitung eine vertrauliche Übermittlung an (andere) öffentliche Stellen gefährdet.

Unterbleibt die Information aufgrund eines Ausnahmetatbestandes (§ 32 Abs. 1, § 33 Abs. 1 BDSG), so muss der Verantwortliche angemessene Ausgleichsmaßnahmen treffen. Insbesondere hat er die Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen (§ 32 Abs. 2, § 33 Abs. 2 BDSG).

2.7.1.2 Erhebung der Daten bei einer anderen als der betroffenen Person (Art. 14 DSGVO)

Sofern der Verantwortliche die Daten *nicht* direkt bei der betroffenen Person erhebt, hat er im Wesentlichen die gleichen Informationspflichten zu erfüllen, wie sie auch bei einer Direkterhebung geboten sind **(Art. 14 DSGVO)**.

Auch der Pflichtenkatalog der *zusätzlichen* Informationen (Art. 14 Abs. 2 DSGVO) orientiert sich an Art. 13 Abs. 2 DSGVO. Im Falle des Art. 14 DSGVO (falls also keine Direkterhebung beim Betroffenen erfolgt) tritt lediglich die Information über die Quelle der Daten hinzu (Art. 14 Abs. 2 lit. f DSGVO).

Die Informationspflicht entfällt nicht nur – wie im Falle der Direkterhebung – dann, wenn der Betroffene bereits über die Informationen verfügt (Art. 13 Abs. 4, Art. 14 Abs. 5 lit. a DSGVO), sondern auch wenn

- es sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, die Information zu erteilen (lit. b; Beispiele: Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke),
- unionale oder nationale Rechtsvorschriften, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich regeln, inwieweit die Informationen zu erlangen oder offenzulegen ist (lit. c) oder
- die personenbezogenen Daten kraft unionalem oder nationalem Recht dem (z. B. anwaltlichen oder ärztlichen) Berufsgeheimnis unterliegen und daher vertraulich zu behandeln sind (lit. d).

Ergänzend schränkt § 33 Abs. 1 BDSG unter Rückgriff auf die Öffnungsklausel des Art. 23 DSGVO die Pflichten des Art. 14 Abs. 1, 2 und 4 DSGVO für öffentliche Stellen ein, wenn die Information

- die nationale Sicherheit,
- die Landesverteidigung,

  - die öffentliche Sicherheit,
  - die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung,

  und damit die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben (im Sinne des Art. 23 Abs. 1 lit. a–e DSGVO), gefährden würde oder
- die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

2.7.2 Auskunftsrecht (Art. 15 DSGVO, § 34 BDSG; bislang §§ 19, 19a, 34, 35 BDSG a. F.)

2.7.2.1 Gegenstand und Inhalt des Auskunftsrechts

Betroffene (also natürliche Personen, über die Daten erhoben, verarbeitet oder genutzt werden) haben – auch losgelöst von einem konkreten Verarbeitungsvorgang – gegenüber Verantwortlichen ein Recht auf Auskunft (Art. 15 DSGVO). Sie können einen Antrag an die öffentliche Stelle richten, Auskunft zu folgenden Informationen zu erteilen:

- die Verarbeitungszwecke (lit. a),
- die Kategorien personenbezogener Daten, die verarbeitet werden (lit. b),
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen (lit. c),
- die geplante Speicherdauer der personenbezogenen Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (lit. d),
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten bzw. auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen die Verarbeitung (lit. e),
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (lit. f),
- alle verfügbaren Informationen über die Herkunft der personenbezogenen Daten, sofern diese nicht bei der betroffenen Person erhoben werden (lit. g),
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (lit. h).

Der Verantwortliche ist verpflichtet, eine Kopie der personenbezogenen Daten, welche Gegenstand der Verarbeitung sind, zur Verfügung zu stellen (Art. 15 Abs. 3 S. 1 DSGVO). Er hat hierzu ein gängiges elektronisches Format zu verwenden, wenn die betroffene Person den Antrag elektronisch stellt und sie nichts anderes angibt (Art. 15 Abs. 3 S. 3 DSGVO).

2.7.2.2 Ausnahmen (§ 34 Abs. 1 BDSG)

2.7.2.2.1. Art. 12 Abs. 5 S. 2 lit. b DSGVO

Das Auskunftsrecht besteht nicht vorbehaltlos. Verantwortliche dürfen die Auskunft bei offenkundig unbegründeten oder exzessiven Anträgen verweigern (Art. 12 Abs. 5 S. 2 lit. b DSGVO). *Offenkundig unbegründet* sind Anträge, wenn ohne Weiteres erkennbar ist, dass die Antragsvoraussetzungen nicht gegeben sind; *exzessiv* sind etwa anlasslos repetitive Anträge.[36]

Dem Verantwortlichen obliegt es einerseits, den Antragssteller korrekt zu identifizieren und dessen Identität zu überprüfen, um keine Daten an Nichtberechtigte zu übermitteln. Andererseits darf er dem Antragsteller keine so hohen Hürden in den Weg legen, dass er den Auskunftsanspruch faktisch vereitelt. Welche Anforderungen der Verantwortliche an die Glaubhaftmachung der Identität des Antragstellers stellen kann, hängt maßgeblich von der Sensibilität und Schutzbedürftigkeit der betroffenen Daten ab. So wird beispielsweise ein Online-Händler an ein Auskunftsbegehren keine höheren formellen Ansprüche stellen können als an einen Vertragsabschluss, sodass auch ein rein elektronisch gestelltes Begehren zu beauskunften wäre. Auf der anderen Seite können und müssen öffentliche Stellen, die besonders sensible Daten verarbeiten (etwa Polizei- und sonstige Gefahrenabwehrbehörden), u. U. durchaus höhere Anforderungen stellen, bspw. im Original unterschriebene Anträge oder (teilweise geschwärzte) Ausweiskopien fordern. Die Anforderungen dürfen den Auskunftsanspruch zugleich aber nicht faktisch infolge ihrer unzumutbaren Höhe aushebeln. Ein persönliches Erscheinen des Anspruchstellers darf die Behörde grundsätzlich nicht fordern.

Das Auskunftsrecht ist ein höchstpersönliches Recht der betroffenen Person. Folgerichtig ist beispielsweise ein Insolvenzverwalter nicht befugt, dem Insolvenzschuldner zustehende Auskunftsansprüche gegenüber öffentlichen Stellen geltend zu machen, um Insolvenzanfechtungsansprüche vorzubereiten. Auf der anderen Seite ist eine bloße Vertretung bei der Antragsstellung grundsätzlich zulässig, insbesondere darf die betroffene Person sich der Hilfe eines Rechtsanwaltes bedienen. Wenn Tatsachen allerdings den Verdacht rechtfertigen, dass eine Vertretungsmacht nicht besteht oder der Antragsteller sie missbräuchlich erlangt hat, bspw. wenn ausländische impressumslose Dienstleister ohne Vorlage einer Vollmacht auftreten und hochsensible Daten anfordern, kann die Auskunft direkt an die betroffene Person statt an den Vertreter erteilt werden, um das Risiko einer Datenübermittlung an Nichtberechtigte auf ein vertretbares Maß zu reduzieren.

2.7.2.2.2. § 34 Abs. 1 BDSG

Die Mitgliedsstaaten dürfen das Auskunftsrecht auf der Grundlage und innerhalb der Grenzen des Art. 23 DSGVO beschränken. Davon macht das neue BDSG in seinem § 34 Abs. 1 Gebrauch: Das Auskunftsrecht entfällt, wenn

- die betroffene Person kraft § 33 Abs. 1 Nr. 1, Nr. 2 lit. b oder Abs. 3 BDSG nicht zu informieren ist (siehe Kapitel 2.7), namentlich weil
    - die Gefahr besteht, dass die öffentliche Stelle ihre *Aufgabe dadurch nicht ordnungsgemäß erfüllen* könnte, z. B. wenn laufende polizeiliche Ermittlungen gefährdet würden (§§ 34, 33 Abs. 1 Nr. 1 lit. a BDSG i. V. m. Art. 23 Abs. 1 lit. d DSGVO),

[36] *Paal*, in: Paal/Pauly, DS-GVO Art. 12, Rn. 64 f.

- die Auskunft die *öffentliche Sicherheit oder Ordnung* gefährden würde (§§ 34, 33 Abs. 1 Nr. 1 lit. b BDSG), oder
- die Daten oder die Tatsache, dass die Stelle sie speichert, (sei es aus gesetzlichen Gründen, sei es im Geheimhaltungsinteresse eines Dritten, z. B. Adoptionsgeheimnis) *geheim gehalten werden müssen* und deswegen das Interesse des Betroffenen an der Auskunft zurücktreten muss (§ 29 Abs. 1 S. 2 BDSG), oder

- die Daten
  - nur deshalb gespeichert sind, weil es aufgrund gesetzlicher oder satzungsgemäßer *Aufbewahrungsvorschriften* unzulässig wäre, sie zu löschen, oder
  - sie ausschließlich *Zwecken der Datensicherung oder der Datenschutzkontrolle* dienen

  und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

2.7.3 Berichtigung, Löschung und Sperrung sowie Widerspruchsrecht (Art. 16, 17, 21 DSGVO, §§ 35, 36 BDSG; bislang §§ 20, 35 BDSG a. F.) unter Berücksichtigung von §§ 5 f. BArchG

2.7.3.1 Widerspruchsrecht (Art. 21 DSGVO)

2.7.3.1.1 Widerspruch gegen Verarbeitungen, die auf der Grundlage von Art. 6 Abs. 1 UAbs. lit. e oder lit. f DSGVO erfolgen (Art. 21 Abs. 1 DSGVO)

Einer rechtmäßigen Verarbeitung darf der Betroffene unter bestimmten Voraussetzungen widersprechen. So darf er gegen Verarbeitungen, die auf Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. e (Verarbeitung zur Wahrnehmung einer öffentlichen Aufgabe oder in Ausübung öffentlicher Gewalt) oder Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO (Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen bzw. eines Dritten) erfolgen, aus Gründen, die sich aus seiner besonderen Situation ergeben, Widerspruch einlegen (Art. 21 Abs. 1 DSGVO).

Dieses Widerspruchsrecht besteht nach dem Willen des deutschen Gesetzgebers jedoch nicht gegenüber einer öffentlichen Stelle, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet (§ 36 BDSG).[37]

2.7.3.1.2 Widerspruch gegen Direktwerbung (Art. 21 Abs. 2 DSGVO)

Noch weiter als das Widerspruchsrecht des Art. 21 Abs. 1 geht das Widerspruchsrecht in den Fällen, in denen Verantwortliche (oder Auftragsverarbeiter) personenbezogene Daten verarbeiten, um *Direktwerbung* zu betreiben. In diesen Fällen hat die betroffene Person das Recht, jederzeit – ohne dass sie weitere Gründe geltend machen müsste – der Verarbeitung zu widersprechen (Art. 21 Abs. 2 DSGVO).

2.7.3.1.3 Widerspruch gegen Verarbeitungen zu wissenschaftlichen, historischen oder statistischen Zwecken (Art. 21 Abs. 6 DSGVO)

[37] Zur Vereinbarkeit der Vorschrift mit dem Unionsrecht siehe *Martini*, in: Paal/Pauly, DS-GVO Art. 21, Rn. 80 ff.

Verarbeitungen, die wissenschaftlichen, historischen oder statistischen Zwecken dienen, sind den höchsten Hürden an ein Widerspruchsrecht ausgesetzt: Zulässig ist der Widerspruch in diesen Fällen nur aus Gründen, die sich aus der besonderen Situation des Betroffenen ergeben. Auch dann bleibt der Widerspruch ohne Erfolg, wenn die Verarbeitung für eine Aufgabe erforderlich ist, die im öffentlichen Interesse liegt.

2.7.3.2 Allgemeine Grundsätze zur Berichtigung und Löschung von personenbezogenen Daten

2.7.3.2.1. Art. 17 Abs. 1 DSGVO

Jede Stelle, die personenbezogene Daten verarbeitet, ist verpflichtet, unrichtige Daten zu berichtigen (Art. 16 S. 1 DSGVO).

Personenbezogene Daten muss der Verantwortliche in folgenden Fällen löschen (lassen):

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, *nicht mehr notwendig* (Art. 17 Abs. 1 lit. a DSGVO).
- Die betroffene Person *widerruft* ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung (Art. 17 Abs. 1 lit. b DSGVO).
- Die betroffene Person legt gemäß Art. 21 Abs. 1 DSGVO *Widerspruch* gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Art. 21 Abs. 2 DSGVO Widerspruch gegen die Verarbeitung ein (Art. 17 Abs. 1 lit. c DSGVO).
- Die personenbezogenen Daten wurden *unrechtmäßig verarbeitet* (Art. 17 Abs. 1 lit. d DSGVO).
- Die Löschung der personenbezogenen Daten ist erforderlich, um eine *rechtliche Verpflichtung* nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zu erfüllen, dem der Verantwortliche unterliegt, (Art. 17 Abs. 1 lit. e DSGVO).
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben, in die ein *Kind eingewilligt* hat (Art. 8 Abs. 1 i. V. m. Art. 17 Abs. 1 lit. f DSGVO).

2.7.3.2.2. Ausnahmen (Art. 17 Abs. 3 DSGVO, § 35 BDSG)

Ausnahmetatbestände halten insbesondere Art. 17 Abs. 3 DSGVO und § 35 BDSG vor. Die Pflicht zur Löschung entfällt für öffentliche Stellen daher, wenn die Datenverarbeitung erforderlich ist,

- um das *Recht auf freie Meinungsäußerung und Information* wahrzunehmen;
- um eine *rechtliche Verpflichtung* zu erfüllen, die die Verarbeitung nach dem unionalen oder nationalen Recht erfordert,[38] oder um eine Aufgabe wahrzunehmen, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

[38] Zu nennen sind hier insbesondere bereichsspezifische gesetzliche (Daten-)Aufbewahrungspflichten, etwa § 147 Abs. 3 der Abgabenordnung (AO), § 257 des Handelsgesetzbuchs (HGB) oder § 14b des Umsatzsteuergesetzes (UStG).

- aus Gründen des öffentlichen Interesses im Bereich der *öffentlichen Gesundheit* (Art. 9 Abs. 2 lit. h und i sowie Art. 9 Abs. 3 DSGVO);
- für liegende *Archivzwecke, die* im öffentlichen Interesse liegen, *wissenschaftliche oder historische Forschungszwecke* oder für *statistische Zwecke* (Art. 89 Abs. 1 DSGVO), soweit das Recht auf Löschung diese Ziele entweder unmöglich macht oder ernsthaft beeinträchtigt, oder
- um *Rechtsansprüche* geltend zu machen, auszuüben oder zu verteidigen.

Der nationale Gesetzgeber schränkt das Recht auf Löschung (zugunsten einer Einschränkung der Verarbeitung im Sinne des Art. 18 DSGVO) zusätzlich ein: Betroffene können im Falle nicht-automatisierter Datenverarbeitung keine Löschung verlangen, wenn wegen der besonderen Art der Speicherung die Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und zudem das Interesse der betroffenen Person an der Löschung als gering anzusehen ist (§ 35 Abs. 1 BDSG).

Ein Recht auf Löschung besteht ferner nicht, wenn satzungsmäßige oder vertragliche Aufbewahrungsfristen dem entgegenstehen (§ 35 Abs. 3 BDSG).

Eine Löschung ist nur für personenbezogene Daten vorgesehen, die entweder aus automatisierter Datenverarbeitung stammen oder aus einer manuellen Datei, jedoch nicht für einzelne Daten, die in nicht dateimäßig strukturierten Akten festgehalten sind.[39] Sind allerdings komplette Akten unzulässig angelegt, so sind sie ebenfalls zu vernichten. Ebenso ist im Allgemeinen mit nicht mehr erforderlichen Akten zu verfahren.

2.7.3.3 Grundsätze zur Löschung von Protokolldaten

2.7.3.3.1 Anwendungsbereich der DSGVO

Bei der automatisierten Datenverarbeitung werden häufig Protokolldaten erzeugt, gespeichert und übertragen. Beispiele hierfür sind u. a.:

- An- und Abmeldevorgänge von Nutzern,
- Zugriffe auf Dateien,
- E-Mail-Verkehr,
- Internetnutzung.

Enthalten diese Protokolldateien personenbezogene Daten oder lassen sie zumindest Rückschlüsse auf solche Daten zu, unterliegen sie den datenschutzrechtlichen Grundsätzen, insbesondere dem Gebot der Zweckbindung und der Datenminimierung (Art. 5 Abs. 1 lit. b und c DSGVO).

Auch hier findet Art. 17 Abs. 1 lit. a DSGVO Anwendung: Die personenbezogenen Daten sind daher zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle nicht mehr erforderlich ist, um ihre Aufgaben zu erfüllen.

2.7.3.3.2 Anwendungsbereich der RL (EU) 2016/680

Für den Anwendungsbereich der RL (EU) 2016/680 – also bei der Verarbeitung personenbezogener Daten (insbesondere) zu Zwecken der Gefahrenabwehr und Strafverfolgung – sieht § 76 BDSG eine gesonderte Protokollierungspflicht vor. In automatisierten Datenverarbeitungssystemen sind daher zumindest die

[39] Das ergibt sich indirekt aus dem Anwendungsbereich der DSGVO, vgl. Art. 2 Abs. 1 DSGVO und § 1 Abs. 1 BDSG. Das BDSG trifft insoweit keine abweichende Regelung.

- die Erhebung,
- die Veränderung,
- die Abfrage,
- die Offenlegung und Übermittlung,
- die Kombination sowie die
- die Löschung

zu protokollieren. Diese Protokolldaten sind am Ende des Jahres, das auf die Generierung folgt, zu löschen (§ 76 Abs. 4 BDSG), sofern nicht eine fachspezifische Sondervorschrift eine abweichende Regelung trifft.

Im Übrigen trifft das BDSG zur Erforderlichkeit von Protokollierungen keine expliziten Regelungen. Auch aus dem Gebot, ein Verzeichnis von Verarbeitungstätigkeiten zu führen (Art. 30 DSGVO) ergibt sich eine solche Protokollierungspflicht nicht. Immerhin erlegt die DSGVO Verantwortlichen aber eine allgemeine Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) sowie eine allgemeine Nachweispflicht auf (Art. 24 Abs. 1 S. 1 DSGVO: „und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt“).

2.7.3.4 Grundsätze zur Einschränkung der Verarbeitung personenbezogener Daten (Art. 18 DSGVO)

Die Verarbeitung personenbezogener Daten ist (auf Verlangen des Betroffenen) einzuschränken, wenn

- der Betroffene die Richtigkeit der personenbezogenen Daten *bestreitet.* Dieser Anspruch reicht aber zeitlich nicht unbegrenzt, sondern nur für eine Dauer, die dem Verantwortlichen die Überprüfung der Richtigkeit der personenbezogenen Daten ermöglicht (Art. 18 Abs. 1 lit. a DSGVO),
- die Verarbeitung *unrechtmäßig* ist, die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt (Art. 18 Abs. 1 lit. b DSGVO),
- der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung *nicht länger benötigt*, die betroffene Person jedoch auf die Daten angewiesen ist, um Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen (Art. 18 Abs. 1 lit. c DSGVO), oder
- die betroffene Person gegen eine auf der Grundlage des Art. 6 Abs. 1 lit. e oder lit. f DSGVO erfolgende Verarbeitung aus Gründen, die sich aus ihrer besonderen Situation ergeben, *Widerspruch* eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen (Art. 18 Abs. 1 lit. d DSGVO).

§ 35 Abs. 2 S. 1 BDSG erweitert die Möglichkeit, die Verarbeitung einzuschränken auf solche Fälle, in denen der Verantwortliche Grund zur Annahme hat, dass eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt.

2.7.3.5 Sonderregelung der Anbietungspflicht von Unterlagen

Alle „Verfassungsorgane, Behörden und Gerichte des Bundes, die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und die sonstigen Stellen des Bundes“ (vgl. § 1 Nr. 8 BArchG) sind verpflichtet, dem Bundes-, Landes- bzw. Kommunalarchiv „alle Unterlagen, die bei ihnen vorhan-

den sind, in ihr Eigentum übergegangen sind oder ihnen zur Nutzung überlassen worden sind, zur Übernahme anzubieten," wenn sie nicht mehr benötigen, um ihre öffentlichen Aufgaben – einschließlich der Wahrung der Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder – zu erfüllen, und ihnen nicht besondere Rechtsvorschriften gestatten, die Unterlagen weiterhin aufzubewahren (§ 5 Abs. 1 S. 1 BArchG). Anderenfalls sind die Unterlagen dem Bundesarchiv spätestens 30 Jahre nach ihrer Entstehung anzubieten (S. 2).

Handelt es sich um Unterlagen von bleibendem Wert im Sinne des § 1 Nr. 10 BArchG, sind sie als Archivgut des Bundes zu übergeben (§ 5 Abs. 2 S. 2 BArchG). Von der Anbietungspflicht sind solche Unterlagen ausgenommen, deren Offenbarung gegen das Brief-, Post- oder Fernmeldegeheimnis verstieße, sowie Unterlagen, die nach gesetzlichen Vorgaben zu vernichten sind und die nach diesen Vorschriften nicht ersatzweise den zuständigen öffentlichen Archiven angeboten werden dürfen (§ 6 Abs. 2 BArchG).

Demnach unterliegen auch Personaldaten[40] der Anbietungspflicht gegenüber dem Bundesarchiv. Dieses hat vom Zeitpunkt der Übernahme an u. a. die schutzwürdigen Belange der Betroffenen in gleicher Weise zu beachten wie die abgebende Stelle (§ 6 BArchG).

Entsprechend weist auch § 113 Abs. 4 BBG auf die Anbietungspflicht gegenüber dem zuständigen Archiv nach § 5 BArchG hin.

Dem Gebot einer Datenlöschung, welches für eine *personaldaten*- oder *personalaktendaten*führende öffentliche Stelle gilt, ist also auch dann Genüge getan, wenn diese Daten dem Bundesarchiv übergeben und aus den eigenen Datenhaltungssystemen entfernt wurden.

2.7.4 Verbot vollständig automatisierter Einzelentscheidungen (Art. 22 Abs. 1 DSGVO, § 54 BDSG; bislang § 6a BDSG)

Sofern gesetzlich nichts anderes bestimmt ist, darf die öffentliche Stelle niemanden einer Entscheidung unterwerfen, die ausschließlich auf einer automatisierten Datenverarbeitung beruht – also ohne jegliches menschliches Eingreifen zustande kommt – und gegenüber der Person rechtliche Wirkung oder eine damit vergleichbare Beeinträchtigung entfaltet (Art. 22 Abs. 1 DSGVO). Diese Regelung verfügt der Unionsgesetzgeber als Ausfluss des Gebots, den Einzelnen nicht zum Objekt einer rein maschinellen Entscheidung zu machen.

Art. 22 hat der Gesetzgeber zwar systematisch im Kapitel III der DSGVO (Rechte der betroffenen Person) verortet, ihm aber zusätzlich den Charakter einer objektiven Verbotsnorm beigegeben: Die Verbotswirkung ist nicht davon abhängig, dass der Betroffene sein Recht geltend macht.[41]

Entscheidungs*vorbereitende* und *-unterstützende* Maßnahmen eines Computerprogramms sowie Profiling-Maßnahmen als solche erfasst das Verbot des Art. 22 Abs. 1 DSGVO indes nicht.

Das Verbot des Art. 22 gilt nicht vorbehaltlos. Die DSGVO lässt in Art. 22 Abs. 2 vielmehr mehrere Ausnahmen zu: Vollständig automatisiert getroffene Entscheidungen sind ausnahmsweise zulässig

- im Rahmen vertraglicher Beziehungen (lit. a),

[40] Zur Definition vgl. Kapitel 2.10.

[41] Vgl. dazu *Martini*, in: Paal/Pauly, DS-GVO Art. 22, Rn. 29.

- aufgrund spezieller Rechtsvorschriften (lit. b) sowie
- mit ausdrücklicher Einwilligung (lit. c).

In diesen Fällen hat der Verantwortliche jeweils Mindestgarantien einzuhalten, um die Rechte und Freiheiten der Betroffenen angemessen zu gewährleisten.[42] Der Betroffene muss insbesondere das Recht haben, seinen eigenen Standpunkt darlegen zu können, die Entscheidung anfechten d. h. inhaltliche Neubescheidung, sowie verlangen zu können, dass eine natürliche Person in den Verarbeitungsprozess einwirkt (Art. 22 Abs. 2 lit. b und Abs. 3 DSGVO).[43] Daneben muss der Verantwortliche zumindest eine faire und transparente Verarbeitung sicherstellen (ErwGrd 71 UAbs. 2 S. 1 DSGVO).

Nicht nur die Union, sondern auch der deutsche Gesetzgeber kann weitere Ausnahmetatbestände schaffen, sofern er datenschutzrechtliche Mindeststandards wahrt, welche einen hinreichenden Schutz der Persönlichkeitsrechte sicherstellen. Beispiele sind etwa im Recht des Besteuerungsverfahrens (§ 155 Abs. 4 AO), im Sozialrecht (§ 31a SGB X) sowie im allgemeinen Verwaltungsverfahrensrecht (§ 35a VwVfG) zu finden.[44]

Für den Geltungsbereich der RL (EU) 2016/680 (vgl. Art. 11 der RL) trifft § 54 BDSG eine entsprechende Regelung.

2.8 Beauftragter für den Datenschutz (Art. 37 DSGVO, §§ 5 ff. BDSG; bislang §§ 4f, 4g BDSG a. F.)

Art. 37 Abs. 1 lit. a DSGVO und § 5 Abs. 1 BDSG verpflichten alle Stellen und Einrichtungen des Bundes, einen Beauftragten für den Datenschutz zu bestellen. Dieser muss die erforderliche Fachkunde und Zuverlässigkeit besitzen (Art. 37 Abs. 5 DSGVO und § 5 Abs. 3 BDSG). Zwar ist er als Beschäftigter der Behörde organisatorisch in diese eingebettet. Allerdings stattet ihn die DSGVO in Art. 38 Abs. 3 S. 1 und 2 mit einem Mindestmaß an Unabhängigkeit aus: Der behördliche Datenschutzbeauftragte muss zum einen keine Anweisungen befolgen, die sich auf die Erfüllung seiner Aufgaben als Datenschutzbeauftragter beziehen (S. 1). Zum anderen darf der Verantwortliche ihn nicht allein deshalb abberufen oder benachteiligen, weil er die Aufgaben erledigt, welche ihm die DSGVO zuweist (S. 2). Der Unionsgesetzgeber lässt sich bei diesen Verbürgungen von einem überzeugenden Gedanken leiten: Besäße der behördliche Datenschutzbeauftragte sie nicht, bestünde die Gefahr, dass er sein Verhalten an den (antizipierten) Vorstellungen der Behördenleitung ausrichtet und in der Folge keine wirksame Datenschutzkontrolle ausüben kann.

Der Datenschutzbeauftragte nimmt für die Behörde wichtige Kontroll- und Servicefunktionen wahr. Er ist dazu berufen, zu prüfen, ob die unionalen und nationalen Datenschutzvorschriften eingehalten wurden, und hat ggf. auf einen rechtskonformen Umgang hinzuwirken (vgl. Art. 39 Abs. 1 lit. a und b DSGVO). In dieser Funktion ergänzt er die externe Aufsicht der unabhängigen Datenschutzaufsichtsbehörden (Art. 51 ff. DSGVO; §§ 8 ff. BDSG). Er fungiert insoweit als kommunikatives Bindeglied (vgl. Art. 39 Abs. 1 lit. d und e DSGVO). Aufgrund

[42] Dazu ausführlich *Martini/Nink*, Wenn Maschinen entscheiden… – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, NVwZ-Extra 10/2017, 1 (3 ff.).

[43] Dazu bspw. *Martini*, in: Paal/Pauly, DS-GVO Art. 22, Rn. 39 ff.

[44] Daneben ermöglicht auch § 37 BDSG Ausnahmen von Art. 22 Abs. 1 DSGVO für vollautomatisierte Entscheidungen in der Versicherungsvertragswirtschaft.

seines Fachwissens und seines Sachverstands ist er aber auch innerhalb der Behörde selbst ein wichtiger Ansprechpartner und Ratgeber in datenschutzrechtlichen Fragen: Er berät die Behörde und unterrichtet die Mitarbeiter über die rechtlichen Anforderungen und etwaige Neuerungen (z. B. durch Mitarbeiterschulungen) – vgl. Art. 39 Abs. 1 lit. a und c DSGVO.

Umgekehrt unterliegt die Behörde als Verantwortliche aber auch der Pflicht, den Datenschutzbeauftragten „ordnungsgemäß und frühzeitig" einzubeziehen (vgl. Art. 38 Abs. 1 DSGVO). Denn nur dann kann dieser die Funktion, die ihm das Gesetz aufträgt, zum Wohle aller (der Behörde selbst wie auch derjenigen, deren Daten sie verarbeitet) erfüllen.

2.9 Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO; bislang §§ 4e, 4g Abs. 2 S. 2, 18 Abs. 2 BDSG a. F.)

Öffentliche Stellen sind gehalten, ein umfassendes Verzeichnis sämtlicher Datenverarbeitungstätigkeiten zu führen (Art. 30 DSGVO).[45] Diese Pflicht ist ein verbriefter Ausdruck der allgemeinen Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO: Der Verantwortliche muss nachweisen können, dass er die Datenschutzgrundsätze des Art. 5 Abs. 1 DSGVO einhält. In das Verzeichnis sind insbesondere die Zwecke der Verarbeitung (Abs. 1 lit. b), die Kategorien betroffener Personen und von Empfängern (lit. c und d), etwaige Übermittlungen in ein Drittland (lit. e) sowie („wenn möglich") eine Beschreibung der technischen und organisatorischen Maßnahmen der Datensicherheit (lit. g) aufzunehmen. Die Verpflichtung trifft den Verantwortlichen und ggf. seinen Vertreter ebenso wie den Auftragsverarbeiter und dessen Vertreter. Das Verzeichnis dient den Datenschutz-Aufsichtsbehörden als Ausgangspunkt ihrer Kontrollmaßnahmen und soll eine vorläufige Rechtmäßigkeitsprüfung ermöglichen. Es unterliegt daher keiner Veröffentlichungspflicht.

Von der Verpflichtung, ein Verfahrensverzeichnis zu führen, sind kleine und mittlere „Unternehmen und Einrichtungen" (Abs. 5) mit einer Beschäftigtenzahl unter 250 ausgenommen. Darunter fallen auch Behörden.[46] Die Privilegierung greift jedoch nur, wenn die Verarbeitung kein Risiko für die Rechte der betroffenen Personen birgt, nicht regelmäßig erfolgt und keine besonderen Datenkategorien (Art. 9 Abs. 1 bzw. Art. 10 DSGVO) zum Gegenstand hat.[47] Diese hohen Hürden schränken den Anwendungsbereich des Ausnahmetatbestandes deutlich ein.

Das Verfahrensverzeichnis dient in der Praxis als Ausgangspunkt sowohl für eine eventuelle Datenschutz-Folgenabschätzung nach Art. 35 DSGVO (vgl. Kapitel 2.5, 3.1 und 4.7.3) als auch zur Evaluation und Planung der technischen und organisatorischen Maßnahmen, die Art. 24, 25 und 32 DSGVO dem Verantwortlichen abverlangen.

[45] Das Verzeichnis nach Art. 30 DSGVO ersetzt namentlich das sog. Verfahrensverzeichnis für jedermann bzw. öffentliches Verfahrensverzeichnis nach §§ 4e, 4g Abs. 2 S. 2 BDSG a. F..

[46] Vgl. *Martini*, in: Paal/Pauly, DS-GVO Art. 30, Rn. 27.

[47] Vgl. *Martini*, in: Paal/Pauly, DS-GVO Art. 30, Rn. 30 f.

2.10 Besonderheiten bei Personaldaten und Personalaktendaten (Art. 88 DSGVO, § 26 BDSG, §§ 106 ff. BBG, § 29 SG; bislang §§ 12 Abs. 4, 32, 34 BDSG a. F., §§ 106 ff. BBG, § 29 SG)

Personaldaten und Personalaktendaten unterliegen – gerade mit Blick auf ihre besondere Sensibilität – jeweils einem speziellen datenschutzrechtlichen Regime. Die DSGVO nimmt insoweit ihren unionsweiten Geltungsanspruch normativen Geltungsanspruch spürbar zurück. Art. 88 DSGVO eröffnet den Mitgliedstaaten durch eine Öffnungsklausel weitgehende Regelungsspielräume. Von dieser Option macht der deutsche Gesetzgeber für den Bereich der Personal- bzw. Beschäftigtendaten in § 26 BDSG Gebrauch. Er erlaubt personenbezogene Daten eines Beschäftigten zu erheben, zu verarbeiten oder zu nutzen, wenn dies erforderlich ist, um ein Beschäftigungsverhältnis zu begründen, durchzuführen oder zu beenden[48] – aber nicht nur das: Der Gesetzgeber lässt daneben explizit auch zu, Beschäftigtendaten auf der Grundlage einer Einwilligung des Betroffenen zu verarbeiten (§ 26 Abs. 2 S. 1 BDSG).

Zu den allgemeinen Vorschriften des BDSG treten die §§ 106 ff. BBG als bereichsspezifisches Datenschutzrecht für Personalakten(daten) hinzu. Sie regeln die Besonderheiten bei der Führung von Personalakten.[49]

Für die Tarifbeschäftigten des Bundes findet sich in § 3 Abs. 5 TVöD-AT lediglich das Recht auf Einsicht in die Personalakte. Die Vorschriften aus §§ 106-115 BBG finden jedoch sinngemäß ergänzende Anwendung. Als **bereichsspezifisches Recht** genießen diese Regelungen auch **Vorrang vor § 26 BDSG**.

2.10.1 Elektronische Aktenführung

Einer (gänzlich) elektronisch geführten Personalakte setzt die Rechtsordnung keine unüberwindbaren Hindernisse entgegen. § 106 Abs. 1 S. 3 BBG gestattet vielmehr ausdrücklich die vollständig „automatisierte“ Personalaktenführung. Hinsichtlich des Schriftformerfordernisses bestimmter Dokumententypen, die sich regelmäßig in einer Personalakte finden, wie z. B. ein Arbeitsvertrag oder die Kündigung eines Arbeitsverhältnisses (§ 2 Nachweisgesetz, § 623 BGB), führt – zumindest im Rahmen der öffentlichen Verwaltung – eine rein digital geführte Personalakte nicht zu einer Minderung des Beweiswerts (vom Urkunds- zum Augenscheinsbeweis). Denn die Zivilprozessordnung (ZPO) misst öffentlichen, elektronischen Dokumenten unter bestimmten Maßgaben eine uneingeschränkte urkundliche Qualität zu (§ 437 i. V. m. § 416a i. V. m. § 371a ZPO).

2.10.2 Teilakten

§ 106 Abs. 2 BBG erlaubt den zuständigen Behörden, Teilakten zu führen. Eine Untergliederung in Teilakten erleichtert die technische und organisatorische Umsetzung eines stark reglementierten Zugriffs im Rahmen des Rollen- und Berechtigungskonzepts.

---

[48] § 26 BDSG gilt gleichermaßen für Beamte, Richter, Soldaten, Arbeitnehmer, Auszubildende und sonstige bei den öffentlichen Stellen beschäftigte Personen (Abs. 8). Die Vorschrift gilt auch für die nicht-automatisierte Verarbeitung der Daten bzw. Daten, die nicht in einem Dateisystem gespeichert sind oder werden sollen (§ 26 Abs. 7 BDSG).

[49] „Zur Personalakte gehören alle Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit ihrem oder seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten).“ (§ 106 Abs. 1 S. 4 BBG). Kein Bestandteil der Personalakte sind demgegenüber „Unterlagen, die besonderen, von der Person und dem Dienstverhältnis sachlich zu trennenden Zwecken dienen, insbesondere Prüfungs-, Sicherheits- und Kindergeldakten. Kindergeldakten können mit Besoldungs- und Versorgungsakten verbunden geführt werden, wenn diese von der übrigen Personalakte getrennt sind und von einer von der Personalverwaltung getrennten Organisationseinheit bearbeitet werden“ (§ 106 Abs. 1 S. 6 und 7 BBG).

Typische Beispiele für Teilakten zur Personalakte sind:

- Verwendungs- und Laufbahnvorgänge,
- Beurteilungen,
- Urlaub, Arbeits- und Dienstbefreiung,
- Aus- und Fortbildung,
- Krankheit / Gesundheit,
- Besoldung und Versorgung,
- Disziplinarvorgänge,
- Beihilfe / Heilfürsorge,
- Nebentätigkeiten,
- Dienstunfälle.

2.10.3 Nebenakten

Nebenakten, also „Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden“ (§ 106 Abs. 2 S. 3 BBG) dürfen demgegenüber nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für den Beamten zuständig sind; sie dürfen nur solche Unterlagen enthalten, deren Kenntnis erforderlich ist, um die Aufgaben rechtmäßig zu erledigen. Das soll in erster Linie vermeiden, dass im weiteren Dokumentenlebenszyklus nur noch schwer zu steuernde Duplikate schutzwürdiger Unterlagen entstehen. Der Gesetzgeber gibt den Personalakten führenden Behörden zudem auf, „in die Grundakte […] ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen“ *(*§ 106 Abs. 2 BBG*)*. „Wird die Personalakte nicht vollständig in Schriftform oder vollständig automatisiert geführt, legt die personalverwaltende Stelle jeweils schriftlich oder elektronisch fest, welche Teile in welcher Form geführt werden und nimmt dies in das Verzeichnis […] auf“ (§ 106 Abs. 2 S. 5 BBG). Das soll sicherstellen, dass in der Grundakte alle Duplikate nachgewiesen sind.

2.10.4 Akteneinsichts- und Auskunftsrecht

Beamte haben ebenso wie Tarifbeschäftigte nach § 3 Abs. 5 TVöD und Soldaten nach § 29 SG das Recht, nicht nur ihre Personalakte selbst einzusehen oder durch Bevollmächtigte einsehen zu lassen. Sie können auch in andere Unterlagen, die für ihr Dienstverhältnis verwendet werden, Einsicht erhalten, sofern diese sie betreffende personenbezogene Daten erhalten. Dies gilt jedoch nur, sofern dies nicht schutzwürdige Belange Dritter berührt (§ 110 BBG).

Unter bestimmten Bedingungen dürfen Personalakten auch Dritten vorgelegt werden bzw. dürfen Dritte Auskünfte aus Personalakten erhalten (§ 111 BBG).

Unter welchen Voraussetzungen Inhalte aus Personalakten abweichend vom Grundsatz der Unversehrtheit und Vollständigkeit zu entfernen sind, regelt § 112 BBG.

Die Sondervorschriften, die dem Schutz der Personaldaten von Beamten, Tarifbeschäftigten und Soldaten dienen, gehen im Grundsatz den allgemeinen Regelungen des BDSG vor (vgl. auch Kapitel 2.1.3, 2.13.9).

2.11 Schutzziele und Schutzbedarf

2.11.1 Schutzziele

Personenbezogene Daten sind kraft ihrer Ausstrahlung auf das informationelle Selbstbestimmungsrecht in besonderer Weise schutzbedürftig (vgl. Art. 1 DSGVO): Der Einzelne ist davor zu schützen, dass ein rechtswidriger Umgang mit seinen Daten ihn in seinem Persönlichkeitsrecht beeinträchtigt.

Die Schutzziele der technisch-organisatorischen Maßnahmen zum Datenschutz (vgl. Kapitel 3) entstammen dem sog. Standard-Datenschutzmodell.[50] Sie lassen sich aus den datenschutzrechtlichen Grundsätzen (Art. 5 Abs. 1 DSGVO, Kapitel 2.1) und denjenigen Einzelvorschriften der DSGVO ableiten, welche diese Grundsätze konkretisieren – insbesondere Art. 32 DSGVO.[51] Zu diesen Schutzzielen gehören:

- **Vertraulichkeit** (Art. 5 Abs. 1 lit. f, 32 Abs. 1 lit. b DSGVO): Unbefugte dürfen keinen Zugriff auf Verfahren und Daten erlangen.
- **Integrität** (Art. 5 Abs. 1 lit. f, 32 Abs. 1 lit. b DSGVO): Daten aus Verfahren sollten unversehrt, zurechenbar und vollständig bleiben.
- **Verfügbarkeit** (Art. 32 Abs. 1 lit. b DSGVO): Verfahren und Daten sollten zeitgerecht zur Verfügung stehen und eine ordnungsgemäße Anwendung erfahren.
- **Belastbarkeit** (Art. 32 Abs. 1 lit. b DSGVO)[52]: Datenverarbeitungssysteme müssen so widerstandsfähig sein, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung oder bei Angriffen von außen gewährleistet ist. Dies erfasst Maßnahmen, die das jeweilige System vor solchen externen Angriffen schützt.
- **Transparenz** (Art. 5 Abs. 1 lit. a DSGVO): Es muss sich mit zumutbarem Aufwand nachvollziehen, überprüfen und bewerten lassen, wie ein Systemen personenbezogene Daten erhebt, verarbeitet und nutzt.
- **Unverkettbarkeit** (Art. 5 Abs. 1 lit. b und c DSGVO): Verfahren sind so einzurichten, dass deren Daten sich nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erheben, verarbeiten und nutzen lassen (*technisch-organisatorische Gewährleistung der Zweckbindung*).
- **Intervenierbarkeit** (vgl. insbesondere Art. 5 Abs. 1 lit. d, 16, 17 DSGVO): Verfahren sind so zu gestalten, dass sie dem Betroffenen die Ausübung der Rechte ermöglichen, die ihm zustehen.

Die Schutzziele **Vertraulichkeit, Integrität, Verfügbarkeit (und Belastbarkeit)** sind Grundwerte der Informationssicherheit. Sie haben den technischen und or-

[50] BSI-Standard 200-2 „IT-Grundschutz-Vorgehensweise“, abrufbar unter https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.0.pdf.

[51] Eine vollständige Übersicht zu dem Verhältnis zwischen den Maßgaben der DSGVO und den Schutzzielen nach dem Standard-Datenschutzmodell findet sich bei *Bock/Ernestus/ et al.*, Das Standard-Datenschutzmodell, S. 27 ff., https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.0.pdf..

[52] Die Belastbarkeit, die Art. 32 Abs. 1 lit. b DSGVO fordert, ist allerdings kein klassisches Ziel der IT-Sicherheit – auch der IT-Grundschutzkatalog des BSI greift sie nicht als Schutzziel auf. Es handelt sich vielmehr um eine funktionale (und generelle) Anforderung an IT-Systeme, vgl. Jandt, in: Kühling/Buchner, DS-GVO, Art. 32, Rn. 26. In der Sache geht es um die Fähigkeit eines Systems, mit Veränderungen – etwa durch Risikoeintritte – umgehen zu können, also um die Toleranz und die Ausgleichsfähigkeit eines Systems gegenüber Störungen.

ganisatorischen Schutz der Informationsverarbeitung im Fokus und gewährleisten somit mittelbar auch den Schutz der verarbeiteten personenbezogenen Daten.

Die drei weiteren Schutzziele **Transparenz, Unverkettbarkeit und Intervenierbarkeit** erwachsen hingegen unmittelbar aus den datenschutzrechtlichen Grundsätzen. Erst wenn der Verantwortliche diese Schutzziele in praxi umsetzt, ist die Datenverarbeitung zulässig.

Verfolgt der Verantwortliche alle Schutzziele, kann es zu **Konflikten** zwischen den Ansprüchen des Datenschutzes einerseits und der Informationssicherheit andererseits kommen. Dies kann sich bspw. dann ereignen, wenn aus Sicherheitsgründen erhobene Protokollinformationen technischer Systeme Daten von Beschäftigten enthalten, die diese Systeme nutzen.

Den Schutzzielen und der Vorbeugung von möglichen Verstößen gegen die datenschutzrechtlichen Grundsätze ist beim Einsatz der elektronischen Aktenführung und der elektronischen Vorgangsbearbeitung schon im Rahmen der Konzeption und beim Systemdesign Rechnung zu tragen. Das entspricht auch dem datenschutzrechtlichen Prinzip „Privacy by Design“, dass Art. 25 Abs. 1 DSGVO als Verarbeitungsprinzip festschreibt. Im Besonderen ist zu vermeiden, dass

- (personenbezogene) Daten unzulässig in der E-Akte *gespeichert* werden oder bleiben,
- Personen auf Daten der E Akte unberechtigt zugreifen können,
- sich Daten manipulieren lassen und
- ein Zugriff auf Protokolldaten der Beschäftigten zum Zweck der Leistungs- und Verhaltenskontrolle erfolgt.

2.11.2 Schutzbedarf

Die Schutzziele der technisch-organisatorischen Maßnahmen beziehen sich auf jegliche Arten der Verarbeitung personenbezogener Daten in informationstechnischen Systemen. Allerdings sind nicht alle Daten (bzw. im Falle der E-Akte nicht alle Dokumente) gleichermaßen schutzbedürftig. So kennt auch das Datenschutzrecht besondere Kategorien personenbezogener Daten, die besonderen Schutzbedarf[53] auslösen (Art. 9 DSGVO). Für sie formuliert die DSGVO ein verschärftes Verarbeitungsverbot.

Der Schutzbedarf bezieht sich primär auf die Schwere der potenziellen Einschränkung des Persönlichkeitsrechts des Betroffenen. Er steigt mit dem denkbaren Schaden, den der Einzelne erleiden würde, wenn seine Daten missbraucht würden. Die technischen und organisatorischen Schutzmaßnahmen müssen also mit dem datenschutzrechtlichen **Risiko** – als Produkt aus Eintrittswahrscheinlichkeit und Schadensschwere für substanzielle Freiheitsrechte natürlicher Personen[54] – korrelieren.

Dabei sollte stets der Bezug zu den Schutzzielen (Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Transparenz, Unverkettbarkeit und Intervenierbarkeit) hergestellt werden. Sie bilden die Zielmarken, um zu bewerten, ob und in welcher

[53] Der Begriff „Schutzbedarf“ bezeichnet Kriterien, die in der Lage sind, die Zweckmäßigkeit und Notwendigkeit von Maßnahmen zu bewerten und zu begründen.

[54] Vgl. *Martini*, in: Paal/Pauly, DS-GVO Art. 35, Rn. 14 f.

Schwere ihre Verletzung zu Beeinträchtigungen der Persönlichkeitsrechte des Betroffenen führen kann.

Verletzungen der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit können in vielfältiger Weise Folgen zeitigen. Das illustrieren die folgenden drei Beispiele:

- Wer die **Vertraulichkeit** verletzt, indem er medizinische Informationen über eine Person offenlegt, kann diese in ihrem Recht auf freie Berufswahl einschränken oder zu anderweitigen Diskriminierungen führen.
- Wer die I**ntegrität** verletzt, indem er Einkommens- und Steuerdaten einer Person verfällt, kann sich strafrechtlicher Verfolgung aussetzen.
- Geht die **Verfügbarkeit** von Sozialdaten durch Löschen verloren, kann das im Extremfall bedeuten, dass die betroffene Person keine Ansprüche auf Sozialleistungen geltend machen kann.

Denkbar sind physische, materielle oder auch immaterielle Schäden. Der Erw-Grd 75 DSGVO nennt paradigmatisch

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- Finanzieller Verlust,
- Rufschädigung.

Der Schutzbedarf lässt sich hinsichtlich der Höhe und der Relevanz der Schadensfolgen skalieren, die ein Verstoß gegen eines der elementaren Schutzziele nach sich ziehen würde. Dafür hat die Rechtspraxis verschiedene Ansätze entwickelt.

Die **IT-Grundschutzvorgehensweise** des BSI (BSI-Standard 200-2[55]) unterscheidet **drei Schutzbedarfskategorien**:

- *Normal* – Die Schadensauswirkungen sind begrenzt und überschaubar.
- *Hoch* – Die Schadensauswirkungen können beträchtlich sein.
- *Sehr hoch* – Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Der Schutzbedarf lässt sich sowohl hinsichtlich eines einzelnen Betroffenen (Intensität der Verletzung) als auch hinsichtlich der datenverarbeitenden Institution (Anzahl der Betroffenen) skalieren.

Die Norm **DIN 66399**[56] zur Datenträgervernichtung definiert drei Schutzklassen:

- *Schutzklasse 1* – normaler Bedarf für interne Daten

  Der Schutz personenbezogener Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, den Betroffenen in seiner Stellung und seinen wirtschaftlichen Verhältnissen zu beeinträchtigen.

  Beispiele:

  - Besoldung/Entgeltzahlungen,

[55] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.html;jsessionid=5C6A652D740F4061111E4A85BBB4DE4B.1_cid360.

[56] DIN 66399-1 „Büro- und Datentechnik – Vernichten von Datenträgern – Teil 1: Grundlagen und Begriffe“, DIN 66399-2 „Büro- und Datentechnik – Vernichten von Datenträgern – Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern“, DIN 66399-3 „Büro- und Datentechnik – Vernichten von Datenträgern – Teil 3: Prozess der Datenträgervernichtung“.

- Abrechnungsdaten,
- Abfertigungsdaten, Steuerbescheide,
- Personenbezogene Firmendaten,
- Ordnungswidrigkeitenverfahren,
- Dienstliche Beurteilungen und Leistungseinschätzungen.

- *Schutzklasse 2* – hoher Bedarf für vertrauliche Daten

  Hier besteht die Gefahr, dass der Betroffene bei unzureichendem Schutz seiner Daten in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.

  Beispiele:

  - Führungszeugnisse, Strafverfahren, Disziplinarverfahren,
  - psychologisch-medizinische Untersuchungsergebnisse,
  - Pfändungen, Insolvenzen.

- *Schutzklasse 3* – sehr hoher Bedarf für besonders geheime Daten

  Der Schutz personenbezogener Daten muss hier unbedingt gewährleistet sein. Andernfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen.

  Beispiele:

  - Zeugenschutzprogramme,
  - Informationen aller Geheimhaltungsgrade des Bundes und der Länder,
  - Geheime bzw. streng geheime Unterlagen aus Forschung und Entwicklung.

Die niedersächsische Landesbeauftragte für Datenschutz (LfD) empfiehlt ein differenziertes Schutzstufenkonzept, welches zwischen fünf Schutzstufen personenbezogener Daten unterscheidet.[57]

Personenbezogene Informationen mit unterschiedlichem Schutzbedarf können grundsätzlich in allen Aktentypen (Generalakten, Fallakten und Personalakten) vorkommen. Sie sind hinsichtlich ihres notwendigen Schutzgrades jeweils auf Dokumentenebene zu bewerten.

Die Personalakte repräsentiert einen Sonderfall, den ergänzend Kapitel 4 exemplarisch behandelt.

2.12 Arten von Informationen zu elektronischen Akten, Vorgängen und Dokumenten

Die elektronischen Schriftgutobjekte „Akte“, „Vorgang“ und „Dokument“ bestehen aus verschiedenen Arten elektronischer Daten. Diese können auch jeweils per-

[57] Siehe https://www.lfd.niedersachsen.de/technik_und_organisation/schutzstufen/schutzstufen-56140.html (Stand: Oktober 2018), weitere Schutzstufenkonzepte werden vom Datenschutzzentrum d. Saarlandes (https://datenschutz.saarland.de/fileadmin/themen/Schutzstufen.pdf) sowie im Standard-Datenschutzmodell (https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html) angeboten.

sonenbezogene oder personenbeziehbare Informationen enthalten: Neben den Primärdaten sind dies Meta- und die Protokolldaten.[58]

2.12.1 Primärdaten

Primärdaten bezeichnen die in den elektronischen Dokumenten enthaltenen Informationen. Dabei kann es sich um Inhalte binär kodierter Dateien, wie bspw. Dateien aus Textverarbeitungsprogrammen, PDF-Dateien, Bilddateien, oder um Inhalte von Textdateien handeln.

Damit der Anwender über das E-Akte-System auch Suchen in den Primärdaten durchführen kann, wird für binär-kodierte Dokumente häufig ein Volltextindex extrahiert.[59] Dieser ermöglicht es, in elektronischen Dokumenten – je nach Benutzerberechtigung – über mehrere Vorgänge und Aktenbereiche hinweg zu suchen.

Die personenbezogenen Informationen, die in den Primärdaten elektronischer Dokumente enthalten sein können, unterscheiden sich je nach Aufgabe der Verwaltung. Die Analyse des eingehenden und ausgehenden Schriftguts und seines jeweiligen Schutzbedarfs ist für jede Behörde einzeln und auf Dokumentenebene vorzunehmen.[60]

Insbesondere die Volltextsuche über verschiedene Datenbestände (und Zuständigkeiten) hinweg birgt substanzielle datenschutzrechtliche Herausforderungen. Hier kann es unter dem Gesichtspunkt des Zweckbindungsgrundsatzes des Art. 5 Abs. 1 lit. b DSGVO erforderlich sein, dass Unterlagen, für die der Suchende nicht mindestens über eine Leseberechtigung verfügt, auch nicht recherchierbar sind – mit der Folge, dass diese in der Trefferliste einer Suchanfrage nicht erscheinen (siehe auch Kapitel 2.13.8). Welche Funktionen bei welchen Daten möglich sein sollen, muss der Verantwortliche auch unter organisatorischen Gesichtspunkten prüfen und in einem Rollen- und Berechtigungskonzept festlegen.

Die prinzipiellen Möglichkeiten eines technischen Administrators, übergreifende Sichten auf einen oder mehrere Datenbestände zu erzeugen, bedürfen datenschutzrechtlich ebenso besonderer Rechtfertigung. Entsprechende Risiken lassen sich durch eine klar definierte Einschränkung dieser Möglichkeiten auf das unbedingt Erforderliche und/oder mithilfe der Etablierung des Vier-Augen-Prinzips bzw. eines Zwei-Schlüssel-Prinzips bei der Erzeugung bestimmter Abfragen begrenzen.

2.12.2 Metadaten

Metadaten sind strukturierte Daten über (Merkmale anderer) Daten. Sie bilden eine wesentliche Komponente der Schriftgutverwaltung.

---

[58] Zu den Begriffen vgl. ergänzend das Glossar des Organisationskonzepts „Elektronische Verwaltungsarbeit“; http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/glossar_e_verwaltung.pdf.

[59] Der Volltextindex wird bspw. beim Scannen von Schriftgut über eine OCR-Erkennung aus dem Papierdokument extrahiert oder bei der Erstellung, Bearbeitung oder dem Import elektronischer Dokumente über einen Konverter erzeugt und zusammen mit dem Binärdokument im System geführt. Die Volltextobjekte sind dabei für den Benutzer nicht als eigene Objekte im E-Akte-System sichtbar.

[60] Detaillierte Informationen hierzu stellen die Kapitel 3.2 „Analyse des Prozessablaufs und der Prozessbeteiligten“ und Kapitel 3.3 „Schutzbedarfs- und Gefährdungsanalyse“ bereit.

Metadaten dienen dazu, Informationsobjekte[61] zu beschreiben, zuordnen, zu indizieren und klassifizieren. Sie bergen beschreibende Informationen und treffen somit Aussagen über die Eigenschaften der elektronischen Schriftgutobjekte sowie deren Struktur und inhaltliche Zusammenhänge.

Durch ihren informativen Charakter helfen Metadaten einerseits dabei, redundante Datenerfassungen zu vermeiden und andererseits, vorhandene Lücken in den Datenbeständen aufzudecken (Ermittlung fehlender Angaben). Neben ihrer Bedeutung für die Qualitätssicherung, ermöglichen sie Vergleiche zwischen alternativen Datenbeständen und tragen erheblich zur Transparenz des Datenbestandes bei. Metadaten können in ihrer Nutzung umso sinnvoller sein, je eher sie standardisierte Begriffe und Informationen verwenden.

Metadaten beschreiben nicht nur Informationsobjekte. Sie steuern auch automatisierbare Datenverwaltungsprozesse, wie z. B. die Gestaltung von Workflows, die Steuerung der Datenpflege (z. B. Versionierung) sowie die Aussonderung und Löschung von Daten.

Bestehende Normen und Standards zu Metadaten im Rahmen der Schriftgutverwaltung finden sich in der:

- DIN ISO 15489-1 Schriftgutverwaltung
- DIN ISO 23081-1 Information und Dokumentation - Metadaten für Verfahren der Schriftgutverwaltung
- MoReq2010 (Modular Requirements for Records Systems)[62].

Einzelne Metadatenfelder können unmittelbar datenschutzrechtlichen Schutzbedarf im Hinblick auf die Informationen auslösen, die sie enthalten. So können bspw. Angaben zu Betreff und Unterbetreff, zum Absender oder auch die Beschreibung des Inhalts eines Dokuments durch den Sachbearbeiter oder den Mitarbeiter der Post- und Scan-Stelle Datenmaterial enthalten, das personenbezogen und damit datenschutzrechtlich relevant ist.

Eine Beschreibung des Vorgehens bei der Bewertung des Schutzbedarfs findet sich in Kapitel 3.3.

2.12.3 Protokolldaten

Protokolldaten sind Daten zum Geschäftsgang bzw. zur allgemeinen Nutzung und Bearbeitung der elektronischen Schriftgutobjekte. Die Protokollierung weist automatisiert Handlungen der Anwender eines E-Akte-Systems an den Schriftgutobjekten nach, die im Rahmen des elektronischen Geschäftsgangs (wie bspw. Erstellen, Ändern oder Löschen[63]) erfolgen. Sie bezieht sich üblicherweise auf alle Arten von Schriftgutobjekten – auf Dokumente und ihre Metadaten sowie auf die Vorgänge und Akten.

---

[61] Informationsobjekte können dabei elektronische Dokumente als kleinste logische Einheiten des Schriftguts im elektronischen Geschäftsgang sowie der Vorgänge und Akten sein.

[62] Es handelt sich um den europäischen De-facto-Standard für das elektronische Records-Management. Die Richtlinie wurde im Rahmen des IDA-Programmes der Europäischen Kommission entwickelt und vom DLM-Forum veröffentlicht. Inzwischen hat sich MoReq als Grundlage für verschiedene Standards der elektronischen Dokumenten-, Archiv- und Schriftgutverwaltung etabliert.

[63] Aus Gründen der datenschutzrechtlichen Revisionsfähigkeit kann es geboten sein, auch lesende Zugriffe zu protokollieren, um bspw. die Zulässigkeit dieser Zugriffe im E-Akte-System nachvollziehbar zu halten (bspw. Zugriffe der Fachadministration auf sensible Bereiche des Aktenbestands). Vgl. dazu auch die Orientierungshilfe Protokollierung der AG „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 2009, http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_Protokollierung.pdf?__blob=publicationFile&v=4.

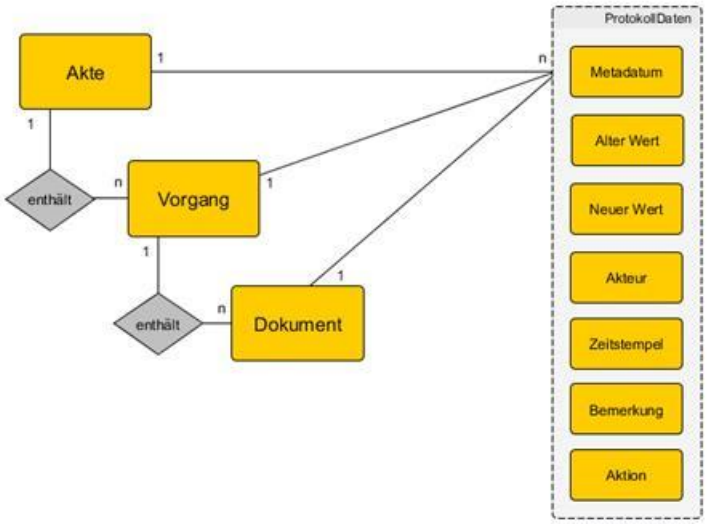

Abbildung 7: Relation von Protokolldaten zu elektronischen Schriftgutobjekten

Die Protokolldaten halten fest, wer (Sozialebene) wann (Zeitebene) was und wie (Sachebene) verändert hat. Typischerweise sieht ein Protokolleintrag über bspw. die Löschung eines Dokumentes folgendermaßen aus:

<Zeitstempel> <Objekt (GZ /Dokument-Nr.)> <Aktivität (Löschen)> <Bearbeiter>

Häufig werden Protokollinformationen zu den einzelnen Hierarchieebenen „Akte“, „Vorgang“, „Dokument“ jeweils auf der nächsthöheren Ebene zur Verfügung gestellt, um insbesondere die Nachvollziehbarkeit des elektronischen Geschäftsganges zu gewährleisten. So würde der im Falle der Löschung eines Dokuments erzeugte Protokolleintrag sinnvollerweise auch in dem betreffenden Vorgang sichtbar. Ebenso erfolgt die Bereitstellung der Protokolldaten über die zdA-Verfügung eines Vorgangs auch in der enthaltenden Akte.

Das Gebot der behördlichen Aktenführung fordert, Protokollinformationen durch das E-Akte-System zu erfassen.[64] Aus datenschutzrechtlicher Sicht sind die Betroffenen stets die Anwender, d. h. im Falle des elektronischen Geschäftsganges: die Bediensteten. Denn jeder Protokolleintrag erfasst diese auf der Sozialebene eindeutig, meist namentlich.

Die so erzeugten personen-, zeit- und aktivitätsbezogenen Informationen eröffnen grundsätzlich die Möglichkeit, das Datenmaterial aus dem E-Akte-System zum Zwecke der Leistungskontrolle zusammenzuführen und auszuwerten. Dies gefährdet die Persönlichkeitsrechte der Betroffenen und kann mit dem Grundsatz der Zweckbindung i. S. d. Art. 5 Abs. 1 lit. b DSGVO kollidieren.

Die Beschäftigten haben jedoch auch im Arbeitsverhältnis ein Recht darauf, dass der Arbeitgeber bzw. Dienstherr ihr informationelle Selbstbestimmungsrecht achtet und ihre personenbezogenen Daten angemessen schützt (vgl § 26 Abs. 1 S. 1 BDSG).[65]

[64] Siehe zur Anforderung der Nachweisbarkeit von Geschäftsgangvermerken, Zeichnungen, Kenntnisnahmen, etc. im elektronischen Geschäftsgang § 6 Abs. 4 RegR.

[65] Keine Erörterung findet an dieser Stelle die Protokollierung auf anderen Ebenen – sog. Betriebsprotokolle, die bspw. Zugriffe oder Login-Versuche einzelner Benutzer auf Komponentenebene (Firewall, Applikationsserver, Datenbankserver etc.) dokumentieren. Diese Art der Protokollierung kann bspw. als Sicherheitsmaßnahme umgesetzt sein. Auch hier haben die Betroffenen grundsätzlich ein Recht auf Einsichtnahme.

Die Anforderungen an die Protokollierung in einem E-Akte-System sind bei Einführungsprojekten im Zuge der Soll-Konzeption detailliert zu definieren.[66] Die Beteiligung des (behördlichen) Datenschutzbeauftragten ist dringend zu empfehlen (vgl. insbesondere § 7 Abs. 1 S. 1 Nr. 1 und Nr. 2 BDSG).

2.13 Besonderheiten im Lebenszyklus elektronischer Dokumente

Der Lebenszyklus elektronischer Dokumente (bspw. deren Erstellung, Bearbeitung und Aussonderung; die Einnahme von Stellvertretungen im elektronischen Geschäftsgang; externe Schnittstellen) liefert wichtige Ansatzpunkte, um bei der Umsetzung des Datenschutzes (wie in Kapitel 3 beschrieben) Gefährdungen entsprechend zu gruppieren und geeignete Maßnahmen ableiten zu können.

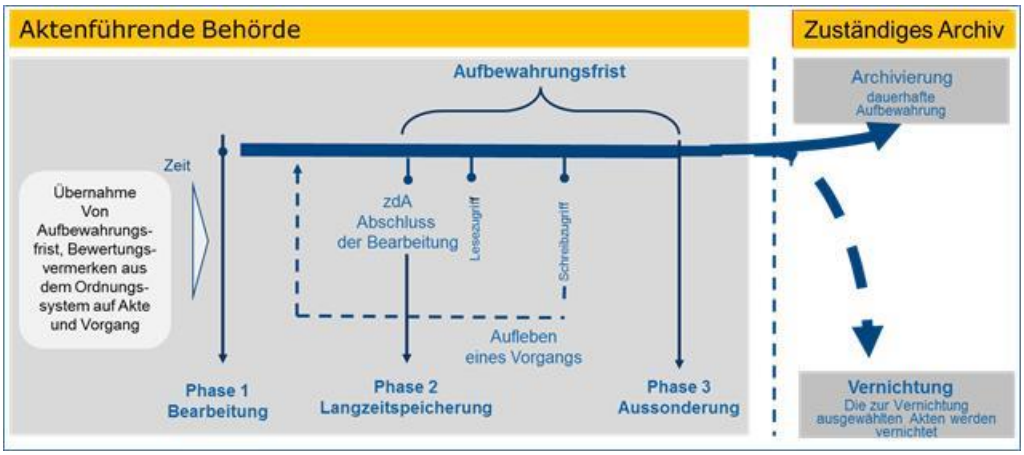

Abbildung 8: Lebenszyklus elektronischer Schriftgutobjekte

Die speziellen Maßnahmen des Datenschutzes in den einzelnen Bearbeitungsphasen sind je nach Art der Gefährdung (siehe Kapitel 3.3.4) als organisatorische Maßnahmen und/oder als technische Maßnahmen umzusetzen. Die Umsetzung organisatorischer Maßnahmen erfordert wiederum entsprechende Regelungen (per Dienstanweisung oder Geschäfts- bzw. Hausanordnung).

2.13.1 Eingangsbehandlung

Die Digitalisierung der Posteingänge[67] und die systematische elektronische Verteilung durch eine zentrale Post- und Scanstelle bergen einerseits in Behörden ein hohes Potenzial, um die Effizienz im elektronischen Geschäftsgang zu steigern. Für diejenigen Beschäftigten, die mit der Ersterfassung betraut sind, stellen die in ihrer Art sehr unterschiedlichen Posteingänge jedoch häufig eine Herausforderung dar.[68]

Hinsichtlich des Datenschutzes, der Datensicherheit und der Datenqualität sind u. a. folgende Risiken zu berücksichtigen:

[66] Vgl. zum Verfahrensverzeichnis im Sinne des Art. 30 DSGVO Kapitel 2.9.

[67] Dies beinhaltet ggf. auch die OCR-Wandlung des Schriftgutes in ein Textformat (CI-Dokument), um im E-Akte-System eine Volltextrecherche über die Primärinformationen des Dokuments zu ermöglichen.

[68] Die Bausteine „E-Poststelle“ und „Scanprozess“ des Organisationskonzeptes E-Verwaltung behandeln diese allgemeinen rechtlichen, fachlichen und funktionalen Anforderungen an die Digitalisierung des Posteingangs sowie die Prozesse der elektronischen Posteingangs- und -ausgangsbearbeitung.

- Verfälschung der digitalisierten Dokumente durch fehlerhafte bzw. unvollständige OCR-Erkennung.[69]
- Bei der Ersterfassung ist die Vergabe inhaltsbeschreibender Metadaten möglich, die personenbezogene Informationen mit Schutzbedarf enthalten.[70]
- Dem ersetzenden Scannen[71] und der damit verbundenen Vernichtung des Papieroriginals stehen die gesetzlichen Anforderungen der Beweiswerterhaltung sowie des Rechts, das Original zurückzuerhalten, gegenüber. Beim automatisierten Scannen besteht die Gefahr, dass das Schriftgut falsch klassifiziert und dadurch falsch zugeteilt wird (Verlust von Vertraulichkeit).[72]
- Bei der Zuleitung der digitalisierten Posteingänge in Postmappen an die jeweils zuständige Abteilung kann es zu Fehlleitungen aufgrund von Fehleinschätzungen hinsichtlich der fachlichen Zuständigkeit oder aufgrund von Fehlbedienungen kommen. Dies kann für Posteingänge mit personenbezogenen Informationen von hohem Schutzbedarf den Vertraulichkeitsgrundsatz verletzen.
- Bei elektronischen Eingängen, die als E-Mail nicht an zentrale Postfächer, sondern direkt an den Sachbearbeiter adressiert sind, ist das Schriftgut frühzeitig in der Akte zu registrieren.

Für elektronische Eingänge aus E-Mail-, Fax- und Formularsystemen gelten grundsätzlich die gleichen Bearbeitungsregeln wie für konventionelle, papiergebundene Posteingänge. Auch bei E-Mails ist es in der Regel technisch möglich, den Betreff und den Absender einer E-Mail automatisiert auf die entsprechenden Metadatenfelder des elektronischen Dokuments zu übernehmen.[73]

Aus datenschutzrechtlicher Sicht ist im Vorfeld zu ermitteln, für welche elektronischen Schriftgutobjekte die Eingangsbehandlung zentralisiert erfolgen sollte und wo eine funktionsbezogene, dezentrale Behandlung der Posteingänge (bspw. zur Wahrung der Vertraulichkeit) geboten ist. Zudem ist zu prüfen, inwieweit sich bei der Vergabe von Metadaten für das Schriftgut der jeweiligen Behörde Automatismen verwenden lassen. Ggf. sind ergänzend organisatorische Regelungen zu treffen.

2.13.2 Inhaltliche Ersterfassung und Registrierung

Auf die Eingangsbehandlung in der Poststelle folgen die inhaltliche Ersterfassung und das Registrieren des Posteingangs im E-Akte-System. Diese Aufgabe übernimmt gemeinhin die Registratur oder eine andere dafür zuständige Stelle[74], die

[69] Optical Character Recognition (Optische Zeichenerkennung); siehe dazu im Baustein „Scanprozess“, Kapitel 2.4.5. (verfälscht wäre hier der zur binären Scan-Ausgabedatei hinterlegte Volltext des Posteingangs, was in der späteren Bearbeitung dazu führen kann, dass das Schriftgutobjekt bei der Recherche nicht zu finden ist).

[70] Dies kann mittels moderner OCR-Technologien (Capturing) auch automatisiert durch die Extraktion von Bereichsinhalten wie bspw. den Betreff oder den Absender eines Schreibens erfolgen.

[71] Siehe dazu Organisationskonzept „E-Verwaltung“, Baustein „Scanprozess“ sowie die Technische Richtlinie RESISCAN 03138 des Bundesamts für Sicherheit in der Informationstechnik.

[72] Fragen zur Beweiswerterhaltung des gescannten Originals behandelt der Baustein „Scanprozess“ des Organisationskonzeptes „Elektronische Verwaltungsarbeit“, Kapitel 2.2.10.

[73] Vgl. dazu Organisationskonzept „Elektronische Verwaltungsarbeit“ – Baustein „E-Vorgangsbearbeitung“, S. 16.

[74] Es besteht auch die Möglichkeit der Zusammenführung der Registratur mit der Poststelle zu einer zentralen Service-Einheit, die Eingangsbehandlung, Ersterfassung, Registrierung und Ausgangsbehandlung des Schriftguts für die gesamte Behörde übernimmt (siehe dazu Baustein „E-Akte“, Kapitel 2.3.6.1 ff. bzw. Baustein „E-Poststelle“, Kapitel 3 „Umsetzungsszenarien“).

den Eingang einer Zuständigkeitsprüfung unterzieht, weitere Metadaten zum Dokument erfasst und es einem Aktenzeichen und Vorgang zuordnet.

Aus datenschutzrechtlicher Perspektive sind in dieser Phase Maßnahmen bzw. Regelungen u. a. zu den folgenden Punkten zu treffen:

- Schriftgut mit schutzwürdigen, personenbezogenen Informationen darf nicht aufgrund fälschlicher Zuordnung zu einer anderen Akte oder einem anderen Vorgang an den falschen Personenkreis innerhalb der Behörde adressiert werden bzw. mit den falschen Zugriffsrechten versehen werden.
- In den Metadaten sollen keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO[75] zur Beschreibung des elektronischen Dokuments erscheinen. Denn Ihnen kommt besonders hoher Schutzbedarf zu.
- Bei der Festlegung von Schlagworten im Rahmen der Registrierung von Schriftgut ist darauf zu achten, dass die elektronischen Dokumente nicht in einem bestimmten Kontext recherchierbar bleiben, aus dem sich indirekt Rückschlüsse auf schutzwürdige personenbezogene (oder personenbeziehbare) Informationen ziehen lassen.

Die o. g. Gefahren können aufgrund von Fehleinschätzungen der Zuständigkeiten, einer fehlerhaften Klassifizierung in Unkenntnis der datenschutzrechtlichen Vorgaben oder durch Fehlbedienung bei der Zuordnung der elektronischen Dokumente zu Akten und Vorgängen entstehen. Diese datenschutzrechtlichen Risiken lassen sich aber durch entsprechende Regelungen bzw. organisatorische Maßnahmen begrenzen.

Den Registratoren und den Mitarbeitern der Poststelle kommt bei der Einhaltung solcher Vorgaben eine besondere Bedeutung zu. Die Beschäftigten sind daher entsprechend zu schulen und zu sensibilisieren.[76]

2.13.3 Entwurfserstellung und Bearbeitung

Im Allgemeinen hat die sachbearbeitende Stelle nach der Registrierung Zugriff auf das elektronische Dokument, das einer Akte und einem Vorgang mit Berechtigung für ihre Organisationseinheit bzw. für ihre Funktion zugeordnet wurde.

Aus datenschutzrechtlicher Perspektive sind im Zuge der Erstellung und Bearbeitung von Dokumenten bzw. Schriftgutobjekten folgende Aspekte von besonderer Bedeutung:

- Sämtliche Bearbeitungsschritte und Änderungen von Primär- sowie Metadaten sind im E-Akte-System nachvollziehbar zu halten und müssen eindeutig der jeweiligen sachbearbeitenden Person zuordenbar sein.[77]
- Als Anlagen sind nur solche Dokumente in den Geschäftsgang zu geben, die personenbezogene Daten in dem Umfang enthalten, wie sie für die aktuelle Bearbeitung nötig sind. Das ist Ausdruck des Gebots der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO). Hierfür kann es ggf. erforderlich

[75] Siehe dazu oben S. 14.

[76] Siehe dazu im Baustein „E-Poststelle“, Kapitel 4.5.

[77] Dies gilt insbesondere dann, wenn im Geschäftsgang personenbezogene Daten erfasst oder bearbeitet werden. Siehe dazu auch § 22 Abs. 2 S. 2 Nr. 2 BDSG (bislang „Eingabekontrolle“ nach S. 2 Nr. 5 der Anlage zu § 9 BDSG a. F.).

sein, eine Kopie des ursprünglichen Dokuments erstellen zu können, in der die für den konkreten Vorgang überflüssigen, personenbezogenen Informationen geschwärzt sind.[78]

- Wo es möglich ist, sind (insbesondere im Interesse des Gebots der Datenminimierung – Art. 5 Abs. 1 lit. c DSGVO) – im elektronischen Geschäftsgang Kopien zum Verbleib zu vermeiden. Stattdessen bieten sich Verweise an. Durch diese verbleiben die referenzierten Dokumente in ihrem ursprünglichen Kontext mit den ursprünglichen Berechtigungen.
- Kopien zum Verbleib sollten generell nur mit den entsprechend notwendigen Bearbeitungsrechten versehen sein und sind ggf. in einem unveränderbaren Format (PDF) zu übermitteln.

Grundsätzlich obliegt es der Stelle, die federführend sachbearbeitend innerhalb eines Vorgangs arbeitet, die inhaltlichen Zusammenhänge und die Erforderlichkeit der Beteiligung oder der Information anderer Organisationseinheiten zu beurteilen. Bei der entsprechenden Umsetzung im elektronischen Geschäftsgang muss wiederum auch innerhalb einer Behörde das Prinzip der Datenminimierung stets Berücksichtigung finden.[79]

2.13.4 Mitzeichnung und Schlusszeichnung

Im Mitzeichnungsverfahren übernehmen die mitzeichnenden Stellen entsprechend ihrer Kompetenz einen Teil der Gesamtverantwortung für eine Entscheidungsvorlage. Dazu hat jede zuständige, mitzeichnende Stelle die Möglichkeit, den Entwurf zu ergänzen, zu überarbeiten oder zu ihm Stellung zu nehmen. Ebenso wie im Falle der federführend sachbearbeitenden Stelle liegt hier die Verantwortung für den Umgang mit personenbezogenen Daten bei der jeweiligen mitzeichnenden Stelle.

- Die *zeichnende Person* muss eindeutig identifizierbar sein – entsprechend den erforderlichen Schutzmaßnahmen des jeweiligen Verfahrens kann dabei eine einfache, fortgeschrittene oder auch qualifizierte Signatur zum Einsatz kommen.[80]
- Die angezeigten Dokumentversionen und die zugehörigen Zeichnungsdaten sind im elektronischen Geschäftsgang *nachvollziehbar* und *konsistent darzustellen* sowie im E-Akte-System bereitzustellen (*Integrität und Authentizität*).
- Es muss sichergestellt sein, dass die der zeichnenden Person im E-Akte-System angezeigte Version des elektronischen Dokuments auch die Version ist, mit der ihre Zeichnungsinformationen verknüpft werden.
- Ändert eine sachbearbeitende Stelle gezeichnete Dokumente einer anderen Stelle, muss das System automatisch eine neue Version des Dokuments erzeugen, um einen im Sinne der Vollständigkeit und Nachvollziehbarkeit revisionssicheren elektronischen Geschäftsgang zu ermöglichen.

[78] Schwärzen von elektronischen Dokumenten kann auf verschiedene Arten (bspw. das Ersetzen der relevanten Stellen durch beliebige Zeichenfolgen) erfolgen und bedeutet in diesem Zusammenhang das dauerhafte Löschen der personenbezogenen Informationen in der Kopie des Primärdokuments sowie im zugehörigen Volltextindex.

[79] Vgl. dazu auch das Organisationskonzept „Elektronische Verwaltungsarbeit“, Baustein „E-Akte“, S. 33-35.

[80] Zu den verschiedenen Arten der elektronischen Signatur siehe im Baustein „E-Poststelle“, Anlage 2.

- Zeichnungen (im Sinne zusammengesetzter Informationsobjekte wie in Abbildung 9 dargestellt) sind im System *manipulationssicher* bereitzustellen. Abhängig vom Schutzbedarf und nach Bewertung der Risiken sind dafür geeignete Maßnahmen zu ergreifen. Hierzu zählen etwa auch Vorgänge auf Ebene der Fach- und Datenbankadministration. Dies gilt sowohl für die Zeichnungsdaten selbst als auch für das gezeichnete Primärdokument. Letzteres wäre bspw. mit der Schlusszeichnung automatisch in ein unveränderbares Format (bspw. PDF/A) übertragbar.

Zeichnungen im elektronischen Geschäftsgang sind analog zur Papierform nach dem Grundsatz der Authentizität jederzeit nachvollziehbar im E-Akte-System umzusetzen. Der logische Zusammenhang zwischen den Informationsobjekten „Dokument“ und „Zeichnungsdaten“ ist in der nachfolgenden Abbildung dargestellt.[81]

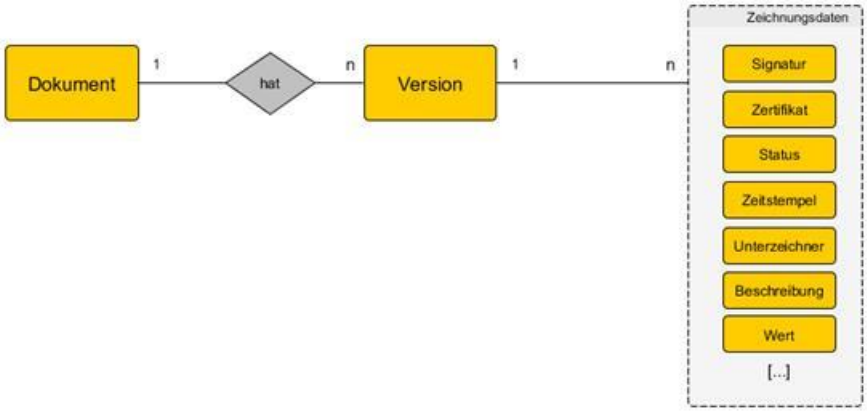

Abbildung 9: Relation von Dokument, Version und Zeichnungsdaten

2.13.5 Postausgang

Die meisten E-Akte-Systeme unterstützen mittels benutzerfreundlicher Funktionalitäten die sachadäquate Postausgangsbehandlung im Kontext des jeweiligen Schriftgutobjekts und ggf. des jeweiligen Prozessschrittes. Im Rahmen des elektronischen Geschäftsgangs besteht einerseits die Möglichkeit des dezentralen Versands durch die federführende bzw. aktuell sachbearbeitende Stelle. Andererseits kann der Versand durch eine zentrale Poststelle erfolgen.[82]

- Die sachbearbeitende Stelle oder eine zentrale Poststelle sollte für den elektronischen Versand als Absenderadresse möglichst ein funktionsbezogenes Postfach und nicht die persönliche E-Mail-Adresse nutzen. Regelmäßig erfolgt die Beantwortung elektronischer Ausgänge direkt an den Absender. Verwendet der Nutzer eine persönliche E-Mail-Adresse als Absenderadresse, würde daher eine zentrale Stelle zur Erfassung/Registrierung der elektronischen Eingänge umgangen. Damit erhöhte sich gleichzeitig das Risiko der Unvollständigkeit der elektronischen

[81] Die Frage, wie die Gültigkeit elektronischer Signaturen während der Langzeitspeicherung und Archivierung dauerhaft sicherzustellen ist, behandelt der Baustein „E-Langzeitspeicherung“[81] des Organisationskonzepts „Elektronische Verwaltungsarbeit“ ebenso wie die Aspekte der Signaturerneuerung oder Übersignierung.

[82] Vgl. dazu im Baustein „E-Poststelle“ das Kapitel 4.5 „Elektronischer Postausgang“ und im „Baustein“ E-Akte, S. 36 ff.

Akte.[83] Bei einem zwischenzeitlichen Funktionswechsel eine Nachricht womöglich vollständig ins Leere.

- Um die Nichtabstreitbarkeit des elektronischen Postausgangs zu gewährleisten, ist ein geeigneter Nachrichtenübermittlungs- und Zustelldienst (elektronisches Gerichts- und Verwaltungspostfach (EGVP) oder De-Mail), der unter Verwendung elektronischer Signaturen eine rechtsverbindliche Empfangsbestätigung erzeugt, zu verwenden.
- Der Einsatz qualifizierter elektronischer Signaturen kann helfen, den Beweiswert von elektronisch versendeten Informationen zu erhalten, sowie dem Risiko eines Identitätsmissbrauchs entgegenwirken.[84]
- Bei der Ausgangsbehandlung von Dokumenten mit hohem Schutzbedarf sind folgende Schutzmaßnahmen möglich:
  - Der Versand darf nur verschlüsselt erfolgen (Kryptografie) und/oder
  - der Versand darf nur an definierte Empfängeradressen erfolgen oder
  - das System unterbindet den Versand solcher Dokumente.
- Jeder elektronische Versand ist durch das E-Akte-System zu dokumentieren (inkl. Adressat und Absendevermerken).

Hinweise

1. An Beteiligte mit Zugriff auf das E-Akte-System sind möglichst nur die internen Links auf die abgelegten Dokumente und Vorgänge zu versenden. Dadurch bleibt das zugrunde liegende Rechtekonzept für die Schriftgutobjekte gewahrt und die Auswirkungen im Falle einer Fehladressierung halten sich in Grenzen. Damit dies möglich ist, müssen die Beteiligten jedoch über die entsprechenden Zugriffsberechtigungen verfügen. Wie diese ausgestaltet sein sollten, ist in diesem Fall ebenfalls in einem Rollen- und Berechtigungskonzept zu definieren.

2. Für den elektronischen Versand über die E-Mail-Schnittstelle des E-Akte-Systems kann sich auch die Hinterlegung einer Positivliste der in Frage kommenden Empfänger anbieten. Dadurch lassen sich mögliche Fehladressierungen (bspw. an verwaltungsexterne Adressen) ausschließen.

2.13.6 Anbieten, Aussondern und Archivieren der Inhalte einer E-Akte

Die Aufbewahrungsfrist beginnt bei der E-Akte mit der zdA-Verfügung. Diese schließt die Akte oder den Vorgang ab und kennzeichnet diese als abschließend bearbeitet. Die betreffenden Akten und Vorgänge dürfen aus Gründen der Rechts- und Beweissicherheit nicht mehr verändert oder gelöscht werden. Sie können aber innerhalb der sog. Transferfrist[85] erneut in Bearbeitung genommen

[83] Welche Implikationen und Risiken mit dem Versand von personenbezogenen Informationen unter der Absenderadresse eines Organisationspostfachs hinsichtlich einer Verletzung des Vertraulichkeitsgrundsatzes bestehen, ist im Einzelfall zu bewerten. Weitere Informationen finden sich im Baustein „E-Poststelle“, Kapitel 3.1 „Organisatorische Umsetzungsszenarien“.

[84] Siehe dazu auch https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html.

[85] Die Transferfrist legt fest, für welchen Zeitraum zdA-verfügte Akten und Vorgänge im aktiven Aktenbestand des DMS vorzuhalten sind, und beträgt in der Regel ein Jahr. Siehe dazu im Baustein „E-Langzeitspeicherung“ das Kapitel 4 „Lebenszyklus der elektronischen Akte“.

werden. Die zdA-Verfügung ist nur nach Abschluss aller offenen Geschäftsgangvermerke und Verfügungen anzubringen.

Wenn die Akten innerhalb der Transferfrist – in der Regel ein Jahr – reaktiviert, d. h. einer erneuten Bearbeitung zugeführt werden, beginnt die Transfer- und Aufbewahrungsfrist erneut.

Für die Dauer der Aufbewahrungsfrist verbleiben die Unterlagen in der Zuständigkeit der aktenführenden Behörde bzw. im Zwischenarchiv des Bundesarchivs (falls entsprechende Vereinbarungen existieren). Dort werden sie unter denselben Schutzbestimmungen wie die aktiven Unterlagen den Anforderungen entsprechend gespeichert.

Mit Ablauf der Aufbewahrungsfrist beginnt das vierstufige Anbiete- und Übernahmeverfahren im Zusammenwirken mit dem zuständigen Archiv (§ 5 BArchG). Alle als archivwürdig bewerteten Unterlagen – einschließlich aller Unterlagen, die dem Datenschutz, dem Geheimschutz oder anderen Schutzbestimmungen unterliegen – sind in nicht-anonymisierter Form an das Archiv abzugeben. Elektronisch verschlüsselte Dokumente sind für die Übergabe an die Archivbehörde unter Angabe des Verfassers und des Datums im Klartext lesbar zu speichern. Elektronische Signaturen sind aufzulösen. Das Abgabeverfahren endet mit dem endgültigen Löschen der weitergeleiteten Daten aus dem E-Akte-System der aktenführenden Behörde.

Die finale Abgabe ist in geeigneter Form zu protokollieren. Nach der Benachrichtigung über den erfolgreichen Import ins Archivsystem ist daraufhin auch eine Löschung des mit „A“ gekennzeichneten Schriftguts möglich.

Auch für die Archivierung gelten Regelungen zur Sicherung gegen Missbrauch personenbezogener Daten. Insbesondere sind zu beachten die Schutzfristen für die Nutzung des Archivguts, die Pflicht zur ordnungsgemäßen und sicheren Aufbewahrung und die Schutzrechte der Betroffenen (§§ 5 Abs. 5, 6, 10 Abs. 2, 11-13, 16 Abs. 2 Nr. 1 BArchG).

Für die Aussonderung und das Löschen von Schriftgut sind besondere Berechtigungen zu vergeben.

2.13.7 Löschung

Die Löschung von Akten oder deren Bestandteilen, die nicht als Ergebnis eines regulären Anbieteverfahrens bzw. aufgrund einer Kassationsgenehmigung des zuständigen Archivs erfolgt oder aber den besonderen gesetzlichen Vorschriften entspricht, ist grundsätzlich nicht zulässig. Vielmehr sind hierfür besondere Berechtigungen erforderlich.

Art. 17 DSGVO kann für personenbezogene Daten Löschpflichten auslösen, z. B. wenn der Betroffene die Richtigkeit der Daten bestreitet.[86] Für Personalakten trifft § 113 BBG eine bereichsspezifische Aufbewahrungsfrist: Sie beträgt in der Regel fünf Jahre. Fünf Jahre nach Abschluss der Personalakte sind daher die Akten – vorbehaltlich ihrer Übernahme in ein Archiv (§§ 5 bis 7 BArchG) – zu vernichten.

In entsprechenden Fach- bzw. Rollen- und Berechtigungskonzepten ist zu definieren, ob die vorgenommenen Löschungen nachzuweisen bzw. zu protokollieren sind und wenn ja, wie. Dabei ist darauf zu achten, dass derartige Protokolle

[86] Siehe hierzu Kapitel 2.7.3.2.

nicht zugleich die Angaben weiterhin mitführen, die den zu löschenden Inhalten zugeordnet waren.

Bedient sich die öffentliche Verwaltung eines Auftragsverarbeiters, so muss der Vertrag (bzw. das äquivalente Rechtsinstrument) den Auftragsverarbeiter verpflichten, die Daten nach Beendigung des Verarbeitungsvorgangs zu löschen oder zurückzugeben (vgl. Art. 28 Abs. 3 S. 2 lit. g DSGVO).

Zum Löschen vorgesehene oder schon gelöschte Schriftgutobjekte dürfen für nicht speziell berechtigte Anwender weder abrufbar sein noch bspw. in einer Trefferliste erscheinen.

Unterlagen, die das zuständige Archiv als archivwürdig bewertet hat, sind diesem vollständig und ohne jede Rückbehalte zu übergeben. Die als nicht archivwürdig eingestuften Unterlagen sind vollständig zu löschen; das Archiv bewahrt als Nachweis eine Kassationsliste auf.

2.13.8 Recherche

Das Schriftgut muss nach den erfassten formalen wie auch inhaltlichen Kriterien im elektronischen Geschäftsgang durch die Berechtigten recherchierbar sein. Dabei soll sowohl die Möglichkeit der Volltextrecherche in den Primärdaten als auch der Suche in Metadatenfeldern sowie ggf. von Kombinationen aus beiden gegeben sein.[87]

E-Akte-Systeme eröffnen üblicherweise die Möglichkeit einer Schnellsuche, die sowohl die Primärinformationen – sofern diese in einem Volltextindex vorliegen – als auch die Metadaten der erfassten Schriftgutobjekte einbezieht. Darüber hinaus gehören meist auch erweiterte, strukturierte Suchen in Metadatenfeldern, Volltexten und Wiedervorlageinformationen zum Funktionsumfang.

Unter datenschutzrechtlichen Gesichtspunkten ist einerseits die Gültigkeit der Zugriffsrechte, die für die einzelnen Schriftgutobjekte vergeben wurden, entscheidend. Fehlt einem Bearbeiter ein Suchrecht, läuft eine Suche dann leer. Andererseits kann es Konstellationen geben, in denen Schriftgutobjekte, für die der angemeldete Benutzer kein Leserecht hat, in einer Trefferliste erscheinen sollen (bspw. in Bereichen der Fachadministration oder Registratur).

Hinweis

Im Falle von Schriftgutobjekten mit vertraulichen, personenbezogenen Inhalten (bspw. Personalakten) ist bereits zu unterbinden, dass Suchanfragen Treffer erzeugen. Denn allein der Umstand, dass Vorgänge zu bestimmten Suchbegriffen vorhanden sind, kann schon die Anforderungen des Datenschutzes verletzen (bspw. das Vorhandensein von Abmahnungen in einer Personalakte).

Systeme zur Unterstützung der elektronischen Verwaltungsarbeit bieten den berechtigten Benutzern häufig die Möglichkeit, Standardauswertungen zu definieren. Personen- bzw. bearbeiterbezogene Auswertungen der Protokollinformationen des elektronischen Geschäftsgangs verletzen jedoch dann den datenschutzrechtlichen Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO), wenn zur Leistungskontrolle zweckentfremdet werden.

[87] Vgl. dazu Baustein „Scanprozess“, Kapitel 3.3.1 „Metadatenvergabe/Indexierung/Volltextrecherche“.

2.13.9 Einsichtnahme

Betroffene haben ein Recht auf Auskunft über die zu ihrer Person gespeicherten Daten, deren Herkunft und Weitergabe, den Zweck der Speicherung, das Bestehen etwaiger Rechte auf Berichtigung oder Löschung, das Bestehen eines Beschwerderechts sowie die Tatsache einer automatisierten Entscheidungsfindung einschließlich Profiling (Art. 15 DSGVO). Auf personenbezogene Daten Dritter bezieht sich der Auskunftsanspruch nicht. Ggf. sind dabei daher Daten Dritter zu schwärzen.

Die Auskunft kann auch über einen technischen Zugang zum aktenführenden System erfolgen. In diesem Falle sind die Berechtigungen allerdings stark einzuschränken, um nicht Persönlichkeitsrechte Dritter zu verletzen.

Verantwortliche sollten das Recht auf Einsichtnahme entweder als technische Funktionalität (Konfiguration eines entsprechenden Berechtigungsprofils) des E-Akte-Systems oder als organisatorische Regelung[88] im Rahmen eines Standardprozesses bereits in der Planungsphase eines Einführungsprojekts berücksichtigen (vgl. Art. 25 Abs. 2 DSGVO).

Für den Bereich der Personalakten ergibt sich eine Besonderheit dadurch, dass dem Beamten (§ 110 BBG), dem Tarifbeschäftigten (§ 3 Abs. 5 TVöD) und dem Soldaten (§ 29 SG) Einsicht in die Personalakte zu gewähren ist – gleich ob diese in Papierform oder elektronisch geführt wird.

Diese Regelungen unterwandern den unmittelbaren Geltungsanspruch der DSGVO nicht. Denn diese räumt den Mitgliedstaaten in Art. 88 Abs. 1 selbst eine Öffnungsklausel ein. Die mitgliedstaatliche Spezifizierung verdrängt daher insoweit Art. 15 DSGVO.

Inwieweit es zulässig ist, **Dritten** Auskünfte über den Inhalt einer Personalakte zu erteilen, richtet sich grundsätzlich nach § 111 Abs. 3 BBG. Im Regelfall ist die Einwilligung des Betroffenen erforderlich. Daneben besteht jedoch auch der allgemeine Informationszugangsanspruch aus § 1 Abs. 1 des Informationsfreiheitsgesetzes des Bundes (IFG); die Rechtsprechung sieht ihn nicht durch die Vorgaben des BBG als verdrängt an.[89] Der IFG-Anspruch ist jedoch seinerseits engen Schranken unterworfen: Das Informationsinteresse des Dritten tritt bei sensiblen Personal- und Personalaktendaten grundsätzlich hinter das Schutzinteresse des Beschäftigten zurück (§ 5 Abs. 2 IFG).

2.13.10 Verfügen

Auch im elektronischen Geschäftsgang übernimmt die federführende sachbearbeitende Stelle die Verantwortung dafür, die Entscheidungsvorlage abzustimmen. Der Laufweg und die Bearbeitung von Dokumenten und Vorgängen lassen sich durch Verfügungen (z. B. „zur Mitzeichnung“, „zur Schlusszeichnung“, „zur Kenntnis“) steuern. Die Laufwege definiert die zuständige Sachbearbeitung in der Regel ad hoc.

Datenschutzrechtlich sind beim Verfügen von Dokumenten und Vorgängen die folgenden Aspekte zu beachten:

---

[88] Mit Bezug auf § 1 Abs. 2 IFG hat die aktenführende Stelle die Möglichkeit, die Art des Zugangs vorzugeben: *„[...] Begehrt der Antragsteller eine bestimmte Art des Informationszugangs, so darf dieser nur aus wichtigem Grund auf andere Art gewährt werden. Als wichtiger Grund gilt insbesondere ein deutlich höherer Verwaltungsaufwand. [...]“. Dies gilt, wenn unterstellt werden kann, dass die technische Konfiguration eines entsprechend eingeschränkten Zugriffs auf die Informationen des E-Akte-Systems einen deutlich höheren Aufwand darstellt.*

[89] BVerwG, NVwZ 2017, 1862 (1862 ff.).

- Der Versand von Objektkopien zum Verbleib sollte nur in unveränderlichen Formaten erfolgen (dabei ist insbesondere PDF/A zu empfehlen[90]). Mit Blick auf das Gebot der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) ist jeweils zu prüfen, ob es überhaupt eines Duplikats zum Verbleib bedarf.
- Bei der Verfügung von Container-Objekten (wie Mappen, Vorgängen oder Akten) werden ggf. untergeordnete Dokumente mitverfügt. Zeichnungsmappen (für Zeichnungsverfahren) bzw. Versandmappen (für den Versand von Kopien zum Verbleib) zu verwenden, schafft hier Abhilfe, da sie den zu verfügenden Schriftgutobjekten explizit zugeordnet werden müssen.
- Fehladressierungen lassen sich leichter identifizieren, wenn die Bearbeitungsreihenfolge und die Adressaten (oder die Stellenkennzeichen) in den Informationen zum elektronischen Geschäftsgang vermerkt werden.
- Fehladressierungen durch Verwechslungen lassen sich leichter vermeiden, wenn der Benutzer in den Dialogen zur Suche und Auswahl von Mitarbeitern und Organisationseinheiten zusätzlich zum Namen des Bearbeiters auch dessen Organisationseinheit- oder Stellenkennzeichen sieht.
- Die Geschäftsgangvermerke sind grundsätzlich aktenrelevant. Es darf daher grundsätzlich nicht möglich sein, sie im weiteren Verlauf zu verändern oder zu löschen.

2.13.11 Stellvertretung

Stellvertretungen sind in der Regel für definierte Zeiträume und Vertretungen im E-Akte-System aktiviert. Sie bewirken, dass die Vertretung den erforderlichen Zugang zu den Daten sowie die erforderlichen Bearbeitungsrechte erhält.

Datenschutzrechtlich ist wesentlich,

- die Stellvertretung auf den erforderlichen Zeitraum sowie explizit zu wählende Benutzer zu beschränken,
- die Stellvertretung als solche sowie alle im Rahmen des elektronischen Geschäftsgangs an Schriftgutobjekten in Stellvertretung vorgenommenen Änderungen zu protokollieren.

Eine mögliche Form der Protokollierung im Falle der Löschung eines Dokumentes in Stellvertretung wäre demnach:

<Zeitstempel> <Objekt (GZ/Dokument-Nr.) <Aktivität (Löschen)> “In Stellvertretung: “<Bearbeiter>

Für Dokumente, Vorgänge und Aktenbereiche mit hohem Schutzbedarf ist zu prüfen, ob diese nicht generell oder in bestimmten Fallkonstellationen von der Stellvertretung ausgenommen sein sollten (bspw. durch die Vergabe eines Vertraulichkeitskennzeichens). Hinsichtlich der Stellvertretung empfiehlt es sich, unterschiedliche Rollen- und Berechtigungsprofile nicht in einem Benutzer-Account zu vereinen, sondern vielmehr klar voneinander zu trennen.

Beispiel:

[90] Siehe den Baustein „E-Langzeitspeicherung“ des Organisationskonzeptes „Elektronische Verwaltungsarbeit“, http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/e_langzeitspeicherung.pdf?__blob=publicationFile&v=3.

Ein Sachbearbeiter eines Referates ist neben seiner regulären Tätigkeit im Personalrat tätig. Beide Bereiche – Referat und Personalvertretung – haben einen eigenen Aktenbereich, welcher der entsprechenden Organisationseinheit zugeordnet ist. Im Falle einer Stellvertretung sollte der Sachbearbeiter entweder nicht mit ein und demselben Benutzer-Account Zugang zu beiden Aktenbeständen haben (er sollte also vielmehr für seine Tätigkeit als Personalvertreter eine eigene zusätzliche Kennung haben). Oder aber es sollte für den Aktenbestand der Personalvertretung gar keine generelle Stellvertretung möglich sein.

Nur wenn eine der beiden o. g. Maßnahmen umgesetzt ist, kann eine Stellvertretung ohne Verletzung des Vertraulichkeitsgrundsatzes erfolgen.

2.13.12 Zugriffsrechte und Rollenprofile

Die Verwaltung der Zugriffsrechte und Berechtigungsprofile muss im Rahmen der Fachadministration zentral erfolgen. Dies ermöglicht, die Vergabe von Berechtigungen im E-Akte-System nach einem mandantenweit einheitlichen Prozess zu gewährleisten.

- Die Protokollierung einer Änderung von Berechtigungsprofilen, der Zuordnung von Benutzern zu Berechtigungsprofilen und der Anmeldung von Benutzern mit fachadministrativen Rechten ermöglicht eine Kontrolle der Rechtevergabe.
- Authentisierungsinformationen (Zuordnung der Nutzer zu Organisationseinheiten sowie Rollen- und Berechtigungsprofilen) sind möglichst aus Verzeichnisdiensten zu übernehmen bzw. in Verzeichnisdiensten zu verwalten. Dies stellt sicher, dass die vergebenen Berechtigungen bzw. der Entzug von Berechtigungen im verwendeten E-Akte-System synchron umgesetzt werden (Zugangs- und Zugriffskontrolle).
- Berechtigungen müssen für Schriftgutobjekte differenziert nach Erstellen, Lesen, Suchen, Ändern und Löschen zu vergeben sein können.
- Das System sollte die Möglichkeit bieten, bestimmte Aktenplanbereiche mit den entsprechenden (bspw. Organisationseinheit-bezogenen) Berechtigungen vorbelegen zu können.
- Es muss möglich sein, Sonderberechtigungen wie den Export, den Versand / die Weiterleitung an externe Stellen und die Nutzung von Schnittstellen zu anderen Verfahren als in Berechtigungsprofilen gebündelte Benutzerrechte zu verwalten.
- Bestimmte Funktionalitäten (wie bspw. Stellvertretung, E-Mail-Versand) sollten für bestimmte Aktenbereiche und die in ihnen enthaltenen Schriftgutobjekte gesperrt werden können. Das E-Akte-System muss in der Lage sein, Benutzer- und Objektrechte entsprechend zu kombinieren.
- Auf Ebene der Schriftgutobjekte sollte möglich sein, die Vergabe von Zugriffsrechten an benutzerspezifische Sicherheitsfreigaben zu binden, die wiederum mit entsprechenden Vertraulichkeitsstufen für Systemobjekte verknüpft sind (wie bspw. VS-NfD).
- Für den Zugriff auf Metadaten muss es möglich sein, bis auf Feldebene zu differenzieren, ob die jeweilige Information für den aktuellen Bearbeiter sichtbar, lesbar oder änderbar ist.

2.13.13 Mobile Vorgangsbearbeitung

Die Möglichkeit ortsunabhängigen Arbeitens nehmen auch die Beschäftigten der öffentlichen Verwaltung (in der Projektarbeit wie auch in den Führungspositionen) zunehmend wahr. Technisch ist das nur möglich, wenn ihnen der dezentrale Zugriff auf die Daten und IT-Verfahren offensteht, die sie benötigen, um ihre Aufgaben zu erfüllen.

Aus datenschutzrechtlichem Blickwinkel ist das Szenario des mobilen Arbeitens mit einer Reihe von Anforderungen an das E-Akte-System verknüpft.

- Das System muss es ermöglichen, eine lokale Kopie eines Schriftgutobjektes auf dem mobilen Endgerät i. V. m. der Sperrung des Originals (Check-out) zu erstellen und die anschließende Synchronisierung bei erneuter Verbindung (Check-in) zu unterstützen.
- Ob und welche Schriftgutobjekte und Aktenplanbereiche aufgrund von Datenschutzaspekten von der Verwendung der Funktionen zum mobilen Arbeiten (im Sinne von Sonderberechtigungen, s. o.) auszunehmen sind, sollte vorab geklärt werden.
- Es muss technisch möglich sein, konkrete Schriftgutobjekte auf dem jeweiligen Endgerät verschlüsselt zu bearbeiten.
- Kommunikationsverbindungen müssen eine Ende-zu-Ende-Verschlüsselung zwischen mobilem Client und dem zentralen Verfahren unterstützen.
- Der Nutzer des mobilen Systems muss geeignete Vorkehrungen dafür treffen, dass unberechtigte Dritte auf die geschützten Daten keinen Zugriff nehmen können.

Bestimmte Schriftgutobjekte – wie bspw. Personalakten, Beihilfeakten – sollten prinzipiell nur innerbehördlich und zentral bearbeitet werden, um die (technischen und) organisatorischen Maßnahmen tatsächlich umsetzen zu können, die Art. 32 DSGVO gebietet. Die Maßnahmen, welche bereits nach § 9 BDSG a. F. i. V. m. der Anlage zu § 9 S. 1 BDSG a. F. formulierte – etwa Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Verfügbarkeitskontrolle – können insoweit als Orientierungsmaßstab dienen.

2.13.14 Hybridaktenführung

Bei der hybriden Aktenführung bestehen die Akten sowohl aus *papierbasiertem* Schriftgut als auch aus *elektronischen* Dokumenten. Hybridakten zu führen, kann bei der Einführung der elektronischen Verwaltungsarbeit und Aktenführung für eine Übergangszeit sinnvoll bzw. notwendig sein (vgl. Kapitel 4.5). In diesem Fall ist diese Überbrückungsperiode mit einzuplanen. Der Verbleib von Papierschriftgut (Dokument, Mappe, Band, Teilakte, Akte etc.) ist auch hier im E-Akte-System mit Angaben zum Ort des Verbleibs (Organisationseinheit, Benutzer u. Ä.), dem Datum der Ausleihe und etwaigen Bemerkungen nachzuweisen.

- Es ist schwierig, den Bearbeitungskontext der elektronischen wie auch der analogen Dokumente vollständig zu halten. Denn eine gemeinsame Sicht auf die in der Akte enthaltenen Dokumente lässt sich nur schwierig herstellen. Dadurch ist das Prinzip der Verfügbarkeit aller relevanten Informationen gefährdet (bspw. bei der Suche nach Schlagworten).
- Lediglich der elektronische Teil der in der Akte enthaltenen Schriftgutobjekte lässt sich automatisiert steuern. Beide Teile sind daher nur unter er-

schwerten Bedingungen synchron zu halten (bspw. bei der Aussonderung oder Abgabe oder im Falle spezifischer Sicherheitsfreigaben).

2.13.15 Umstrukturierung des Aktenbestands (Umprotokollierung)

Die Neuordnung der Aufbauorganisation (z. B. die Umbenennung, Neubildung oder Auflösung von Organisationseinheiten mit Aufgabenübertragung bzw. der Wechsel der übergeordneten Organisationseinheit sowie ggf. der Wechsel des Ressorts durch einer Behörde) erfordert in der Regel auch entsprechende Umstrukturierungen des Aktenbestands.

Um die Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit und Transparenz nicht zu gefährden, muss das System Umstrukturierungen des Aktenbestands funktional unterstützen. Insbesondere hat es alle Änderungen an den elektronischen Schriftgutobjekten durchgängig zu protokollieren. Eine Umschreibung kann sich dabei auf existierende Geschäfts- und Aktenzeichen beziehen, auf die vergebenen, organisationseinheitsbezogenen Objektrechte oder – im Falle von Ressortumbildungen – auf den Export ganzer Aktenplanbereiche und der enthaltenen Objekte (inkl. ihrer Primär-, Meta-, Bearbeitungs- und Protokollinformationen).

2.13.16 Langzeitspeicherung

Langzeitspeicherung ist die Aufbewahrung elektronischer Dokumente innerhalb der Aufbewahrungsfrist in Verantwortung der aktenführenden Verwaltung, bevor sie an das zuständige Archiv abgegeben wird (siehe auch Kapitel 2.13.6).

Die Umwandlung der elektronischen Dokumente in ein unveränderliches, archivwürdiges Format (wie bspw. PDF/A) erfolgt nach Ablauf der Transferfrist. Aus datenschutzrechtlicher Sicht ist bei der entsprechenden Formatwandlung sicherzustellen, dass die Anforderungen an die Verfügbarkeit und Integrität erfüllt werden. Dies gilt für die Primärdaten wie auch für Meta-, Protokoll- und Signaturdaten.[91]

Elektronische Personalakten enthalten personenbezogene Informationen mit ggf. hohem Schutzbedarf.[92] Zudem sind sie unter Umständen von besonderer Bedeutung, damit Betroffene ihre Rechte wahrnehmen können (z. B. Pensions-, Renten- und Versorgungsansprüche). Daher sind bei der Langzeitspeicherung die Anforderungen an die Verfügbarkeit, die Integrität sowie an den Beweiswerterhalt im Sinne der Prozessordnungen zwingend zu berücksichtigen.

[91] Zu den Anforderungen an die Langzeitspeicherung vgl. Baustein „E-Langzeitspeicherung“ des Organisationskonzeptes „E-Verwaltung“, Kapitel 3.4 ff.

[92] Dazu auch Kapitel 4.

3 Allgemeines Vorgehen bei der Planung und Umsetzung von Maßnahmen zum Datenschutz

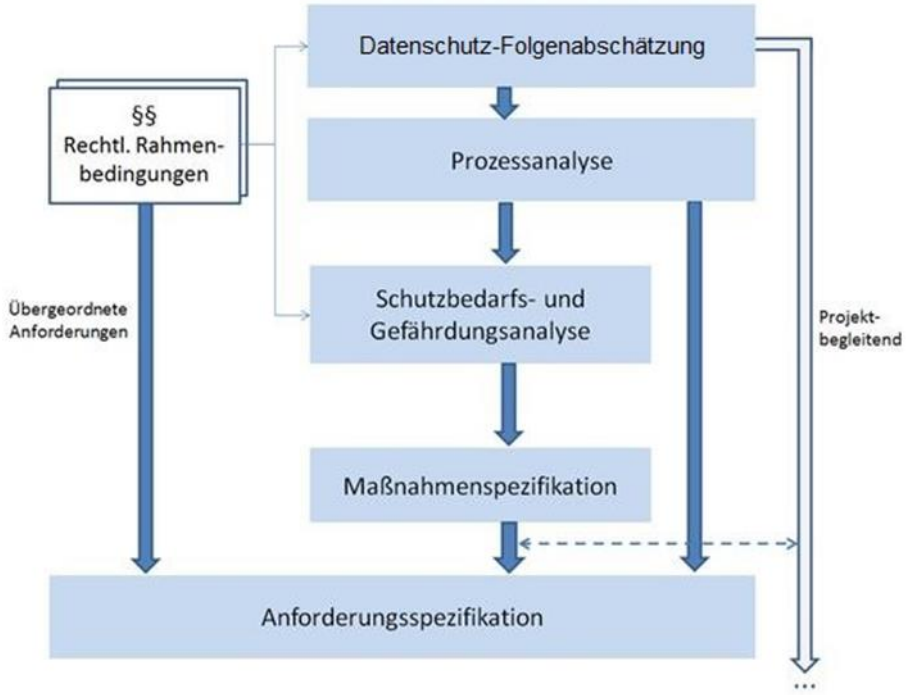

Abbildung 10: Prozessablauf - Planung und Umsetzung von Maßnahmen zum Datenschutz

In Einführungsprojekten zur elektronischen Verwaltungsarbeit ist für alle Arten personenbezogener Daten, die im jeweiligen Arbeitsbereich anfallen, zu prüfen, ob sich die datenschutzrechtlichen Ziele im Sinne der DSGVO und des BDSG in dem geplanten elektronischen Verfahren verbindlich umsetzen lassen.

Sowohl die Posteingänge und der (Papier-)Aktenbestand der Behörde als auch die Erfassung der Bearbeitungsprozesse der jeweiligen Schriftgutobjekte sind im elektronischen Geschäftsgang zu dokumentieren und aus Sicht der geltenden Datenschutzanforderungen zu bewerten.

In diesem Zusammenhang empfiehlt es sich grundsätzlich, den Datenschutzbeauftragten, den IT-Sicherheitsbeauftragten und die Personalvertretung (Letztere insbesondere zum Thema Protokollierung) frühzeitig einzubinden.

Die Systematik des IT-Grundschutzes (Schutzbedarf ermitteln, Maßnahmen definieren, Gefährdungen und Risiken analysieren) zeichnet i. V. m. den entsprechenden Gefährdungs- und Maßnahmenkatalogen (siehe Kapitel 2.11.2, 3.3 und 4.7.4) die relevanten Schritte vor.

3.1 Grundlegende Bewertung des Risikos für die Rechte und Freiheiten der Betroffenen (Datenschutz-Folgenabschätzung)

Unter dem Datenschutzregime der DSGVO löst die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) die Vorabkontrolle (§ 4d Abs. 5 und 6 BDSG a. F.) ab. Das Instrument der Folgenabschätzung ist jedoch nicht für jede neue Datenverarbeitung obligatorisch. Der Gesetzgeber verlangt sie dem Ver-

antwortlichen nur dann ab, wenn *voraussichtlich ein hohes datenschutzrechtliches Risiko* besteht.[93]

Die Datenschutz-Folgenabschätzung soll die Konsequenzen sensibler Verarbeitungsvorgänge für die Rechte Betroffener antizipieren. Sie soll helfen, Risiken vorab rechtzeitig zu erkennen, und – hieran anknüpfend – geeignete technische und organisatorische Gegenmaßnahmen zu ergreifen.

Die Datenschutz-Folgenabschätzung enthält als Instrument zur Risikoerkennung und -bewertung zumindest:

- eine systematische *Beschreibung* der geplanten Verarbeitungsvorgänge und -zwecke, gegebenenfalls einschließlich der berechtigten Interessen, die der Verantwortliche verfolgt;
- eine *Bewertung* der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;[94]
- eine *Einschätzung* der Risiken für die Rechte und Freiheiten der Betroffenen sowie
- die *Abhilfemaßnahmen*, die der Verantwortliche plant, um auftretende Risiken zu bewältigen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, die den Schutz personenbezogener Daten sicherstellen und den Nachweis, dass der Verantwortliche DSGVO-Vorgaben einhält.

Hält der Verantwortliche genehmigte Verhaltensregeln i. S. d. Art. 40 DSGVO ein, ist dies bei der Beurteilung der Auswirkungen der Verarbeitungsvorgänge gebührend zu berücksichtigen (Art. 35 Abs. 8 DSGVO).

Für die Datenschutz-Folgenabschätzung holt der Verantwortliche nicht nur den Rat des Datenschutzbeauftragten ein, sondern auch den Standpunkt der betroffenen Person oder ihrer Vertreter und setzt sich inhaltlich hiermit auseinander (Art. 35 Abs. 2, Abs. 9 DSGVO).

Die praktische Ausgestaltung einer Datenschutz-Folgenabschätzung lässt sich in folgende Phasen gliedern:

[93] Vgl. dazu oben Kapitel 2.5.1 sowie insbesondere die „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt'" der Art.-29-Datenschutzgruppe bzw. des Europäischen Datenschutzausschusses, abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

[94] Zum Zweckbindungsgrundsatz siehe Kapitel 2.3.

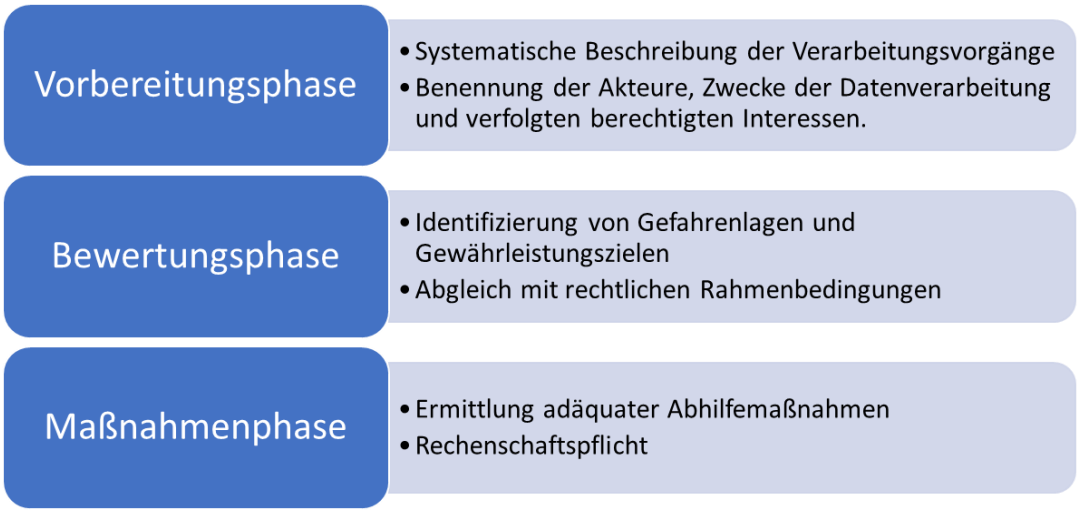

Abbildung 11: Überblick Datenschutz-Folgenabschätzung

- Vorbereitungsphase

  Die Vorbereitungsphase richtet die Ziele und organisatorische Abwicklung der Datenschutz-Folgenabschätzung aus. Sie beschreibt die geplanten Verarbeitungsvorgänge samt Technologie und beteiligten Akteure sowie der Verarbeitungszwecke, ggf. einschließlich der verfolgten berechtigten Interessen. Dabei sind typischerweise angezeigt:

  - die Ermittlung der einschlägigen rechtlichen Vorgaben,
  - die Erstellung eines Verzeichnisses (systematische Beschreibung) der geplanten und umgesetzten Verarbeitung personenbezogener Daten, insbesondere der Art, des Umfangs und der Dauer, der näheren Umstände der Datenverarbeitung sowie der hierfür eingesetzten Technik samt Schnittstellen, Prozessabläufen und Funktionsrollen;
  - die Bestimmung der betroffenen Datenkategorien;
  - die Benennung der daraus erwachsenden Risiken;
  - die Prüfung, ob eine Weitergabe der Daten vorgesehen ist bzw. an wen und zu welchem Zweck;
  - die Ermittlung, wer Zugriff auf die Daten hat sowie zu welchem Zweck und in welchem Umfang;
  - die Veranschlagung der geplanten Aufbewahrungsfrist;
  - die Prüfung, ob die Verarbeitung der Daten wirklich erforderlich ist, und
  - die Prüfung, wie transparent die Bearbeitung gegenüber Betroffenen erfolgt.

- Bewertungsphase

  Im Rahmen der Bewertungsphase gleicht der Verantwortliche die geplanten tatsächlichen Verarbeitungsvorgänge sowie -zwecke, insbesondere die Risiken für die Rechte und Freiheiten Betroffener, mit den einschlägigen rechtlichen Vorgaben ab. Dazu identifiziert er Gefahrenlagen (normales, hohes oder sehr hohes Risiko; siehe die Schutzbedarfskategorien unter Kapitel 2.11.2) sowie Gewährleistungsziele (entsprechend den Schutzzielen unter Kapitel 2.11.1) als Prüfungsmaßstab und bricht die sich daraus ergebenden

Konsequenzen auf die konkreten Verarbeitungsvorgänge herunter. Ziel ist, zu einem angemessenen Ausgleich der kollidierenden Interessen zu gelangen.

- Maßnahmenphase (Risikobehandlungsplan)[95]

  Die Ergebnisse der Vorbereitungs- und Bewertungsphase sind in der Maßnahmenphase im Rahmen der Entscheidung über geeignete Abhilfemaßnahmen zum Schutz der Rechte und Freiheiten der Betroffenen zu berücksichtigen. Das Risiko der Verarbeitung hat der Verantwortliche durch technische und organisatorische Maßnahmen auf ein vertretbares Maß abzusenken. Dies muss der Verantwortliche durch eine Dokumentation nachweisen (Art. 35 Abs. 7 lit. d, Art. 5 Abs. 2 DSGVO).

  Das Ergebnis der Analyse (Datenschutz-Folgenabschätzungs-Bericht) ist als Teil der allgemeinen Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) den zuständigen Aufsichtsbehörden auf Anforderung zur Verfügung zu stellen.

Reichen die getroffenen Maßnahmen nicht aus, um mit vertretbaren Mitteln ein hohes Risiko hinreichend sicher auf ein hinnehmbares Niveau abzusenken, verbleibt also ein (hohes oder mittleres) Restrisiko, ist vor Durchführung der Verarbeitung die Aufsichtsbehörde zu konsultieren (Art. 36 Abs. 1 DSGVO). Besteht demgegenüber kein hohes Restrisiko, bedarf es keiner Konsultation der Aufsichtsbehörde; die Datenverarbeitung darauf verfolgen.

Eine einmal vorgenommene Datenschutz-Folgenabschätzung entbindet den Verantwortlichen indessen nicht von der Prüfung, ob ihre Prämissen fortbestehen und ob sich die Verarbeitung in Übereinstimmung mit den Hypothesen der Datenschutz-Folgenabschätzung vollzieht. „Erforderlichenfalls“ hat der Verantwortliche daher zu ermitteln, ob die Verarbeitung auch tatsächlich nach den Vorgaben der Datenschutz-Folgenabschätzung erfolgt und ob die umgesetzten technischen und organisatorischen Maßnahmen ausreichen (Art. 35 Abs. 11 DSGVO).

Gerade bei Entwicklungs- und Einführungsprojekten lässt sich die Datenschutz-Folgenabschätzung nicht als einmalige, dem Projekt vorangestellte Aktivität konzipieren. Sie stellt sich vielmehr als komplexer, *projektbegleitender* Prozess dar. Insbesondere die Einführung von IT-Verfahren ist häufig mit Änderungen der ursprünglichen Konzeptionen und Planungen verbunden. Dann ist auch die datenschutzrechtliche Bewertung der technischen und organisatorischen Maßnahmen entsprechend zu aktualisieren. Geboten ist dies jedenfalls dann, wenn das tatsächliche von dem kalkulierten Verarbeitungsrisiko abweicht.

Ein beispielhaftes Vorgehen für die Datenschutz-Folgenabschätzung bei Einführung der elektronischen Personalakte findet sich im Anhang 5.1. Ergänzend bieten auch der Leitfaden des BITKOM zur Risikoanalyse und zur Durchführung einer Datenschutz-Folgenabschätzung[96], das Standard-Datenschutzmodell (SDM)[97], das „PIA-Tool“ der französischen Datenschutzaufsichtsbehörde CNIL[98] sowie die Leitlinien der ISO-Norm ISO/IEC 29134:2017[99] erste Orientierung.

---

[95] Ausführungen zur Planung und Umsetzung der einzuleitenden Abhilfemaßnahmen finden sich unter Kapitel 3.4.

[96] Bitkom, Leitfaden Risk Assessment & Datenschutz-Folgenabschätzung, abrufbar unter https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Datenschutz-Folgenabschaetzung.html.

[97] In der Version V.I.1. (Erprobungsfassung aus April 2018) abrufbar unter https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf.

Auch das „Whitepaper Datenschutz-Folgenabschätzung“ des *Forums Privatheit* (https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf) setzt in den Maßnahmenbestimmungen auf das SDM.

3.2 Analyse des Prozessablaufs und der Prozessbeteiligten

Die Analyse des Prozessablaufs hat zum Ziel, alle aus fachlicher Sicht beteiligten Personen, Anwendungen, Informationsobjekte und Bearbeitungsschritte in ihrer Gesamtheit und in ihren gegenseitigen Beziehungen zu erfassen. Das Ergebnis liefert alle für die später in der IT-Sicherheitskonzeption durchzuführende Strukturanalyse[100] benötigten Informationen.

Sinnvollerweise erfasst die Analyse des Prozessablaufs zunächst die bestehenden Arbeitsprozesse des ggf. papiergebundenen Verwaltungshandelns einer Behörde als Grundlage in einem Ist-Stand. Sodann modelliert sie diese im Rahmen der Sollkonzeption eines IT-gestützten, elektronischen Geschäftsgangs.

Hinweis

Das Phasenmodell zur Einführung der elektronischen Verwaltungsarbeit (Baustein „Projektleitfaden“, Kapitel 4)[101] sieht die Ist-Analyse und die Soll-Konzeption in den Phasen Vor- und Hauptuntersuchung vor. Dies ist mit den datenschutzrechtlichen Vorgaben (Folgenabschätzung und Planung von Maßnahmen) vereinbar. Ist-Analyse und Soll-Konzeption sowie die entsprechende Modellierung sind also als übergreifende Projektaufgaben zu verstehen, innerhalb derer der Datenschutz als ein grundlegender Aspekt zu berücksichtigen ist.

Eine mögliche Notation zur Erfassung der Ist- und Soll-Prozesse ist die BPMN 2.0[102]. Mit ihrer Hilfe lassen sich die verschiedenen Ebenen (fachliche Prozesse, Daten-Input und -Output, Akteure, Systeme, manuelle und automatisierte Aktivitäten) in einem Prozessmodell darstellen.

Die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen, firmiert auch unter dem Begriff „Informationsverbund“. Er definiert den Geltungsbereich des zu erstellenden Sicherheitskonzepts.

Die Modellierung der behördenspezifischen Abläufe ermöglicht im nächsten Schritt, Risiken und Maßnahmen abzuleiten (siehe dazu die Kapitel 3.3.4 und 3.4).

3.2.1 Behördeninterne Abläufe

Die Prozessanalyse sollte möglichst alle behördeninternen Bearbeitungsabläufe umfassen, welche die Einführung des E-Akte-Systems tangiert. Dabei sollte sie die spezifischen datenschutzrechtlichen Fragestellungen berücksichtigen.

Ziel der Modellierung ist es, die datenschutzrechtlichen Anforderungen an den elektronischen Geschäftsgang zu spezifizieren, Risiken zu identifizieren sowie

98 Die Software zur Durchführung einer Datenschutz-Folgenabschätzung (engl.: Privacy Impact Assessment, PIA) ist abrufbar unter https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

99 ISO, Informationstechnologie – Sicherheitsverfahren – Datenschutz-Folgenabschätzung – Leitfaden, abrufbar unter https://www.iso.org/standard/62289.html.

100 Die einzelnen Schritte der Strukturanalyse beschreibt im Detail Kapitel (7.4 und) 8.1 der IT-Grundschutz-Vorgehensweise (BSI-Standard 200-2) in Form einer Handlungsanweisung. Das Ergebnis der Strukturanalyse ist der vollständig modellierte Informationsverbund, auf den Maßnahmen zugeschnitten werden.

101 http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/projektleitfaden.pdf.

102 Business Process Model and Notation der OMG (Object Management Group), http://www.omg.org/spec/BPMN/2.0/.

technische und organisatorische Maßnahmen im Prozess zu verorten. Beispielhaft stellen sich folgende Fragen:

- Welche Informationen und Dokumenttypen (bspw. Verträge, rechtsbildende Dokumente) soll die Behörde elektronisch erfassen und bearbeiten?
- Welche Metadaten erfordern die einzelnen Dokumenttypen?
- Wie soll die Posteingangsbehandlung und Digitalisierung (zentrale Post- und Scan-Stelle, Abteilungs-Scanstelle) erfolgen?
- Welche Standardlaufwege innerhalb der Behörde gibt es?
- Wie viele verschiedene Stellen bzw. welche Akteure sind innerhalb der Behörde am Geschäftsgang von der Ersterfassung bis zum Versand und der zdA-Verfügung des Schriftguts beteiligt?
- Welche automatisierten Bearbeitungsschritte gibt es?
- Handelt es sich um strukturierte, semistrukturierte oder Ad-hoc-Prozesse?
- Welche Informationen sollen zu den einzelnen Bearbeitungsschritten automatisiert erfasst werden?
- Welche Informationen sollen in den einzelnen Arbeitsschritten zur Verfügung stehen oder ausgewertet werden dürfen?
- Welche Recherchemöglichkeiten sollen bestehen?

Es empfiehlt sich, bei der Modellierung der Geschäftsprozesse ein Prinzip anzuwenden, das der IT-Grundschutz[103] als „Komplexitätsreduktion durch Gruppenbildung“ bezeichnet. In BPMN 2.0 hat es in der Verwendung von Subprozessen seine Entsprechung hat.[104]

3.2.2 Beteiligung externer Stellen

Hinsichtlich der nachgelagerten Prozesse und der Beteiligung externer Stellen hat die einführende Behörde datenschutzrechtlich insbesondere die Übergabepunkte in den Fokus zu nehmen.

Zur Analyse des Prozessablaufs und der Feststellung der externen Beteiligten sind die folgenden Fragestellungen relevant:

- Was sind die nachgelagerten Prozesse? An welchen Stellen und zwischen welchen Beteiligten finden Übergänge statt?
- Welche Szenarien für den Austausch oder die Abgabe von Daten an andere Verfahren und Behörden bestehen?
- In welchen Formaten sind Daten ggf. zu übergeben?
- Welche Personen/Stellen sind ggf. zu beteiligen?
- Welche Personen/Stellen haben ein Recht auf Einsichtnahme?

[103] BSI-Standard 200-2, abrufbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html.

[104] Siehe dazu Kapitel 5.6. Im Anhang zu Kapitel 5.6 findet sich insbesondere ein Beispiel für die Definition eines Sollprozesses der elektronischen Verwaltungsarbeit und der aus dem Prozessmodell abzuleitenden datenschutzrechtlichen Fragestellungen.

- Auf welche Informationen bezieht sich ein Recht auf Einsichtnahme?
- Wie erfolgen Anbietung, Archivierung und Aussonderung?

Auch für die Beteiligung externer Stellen bietet sich das Prozessmodell aus Kapitel 5.6 an. Es enthält zwei Schnittstellen zu zwei externen Prozessteilnehmern, dem zuständigen Archiv und einer anderen Behörde.

Für größere, datenschutzrechtlich sensible Projekte der Bundesverwaltung – wie etwa die Einführung der eP-Akte – ist es unbedingt ratsam, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit frühzeitig einzubinden. Für die Datenschutz-Folgenabschätzung etabliert Art. 35 Abs. 2 DSGVO eine Beteiligungspflicht für den internen (bzw. den behördlichen) Datenschutzbeauftragten; nach Abs. 9 ist ggf. zusätzlich der Standpunkt der betroffenen Personen einzuholen.

3.2.3 Prozessbeteiligte und Betroffene

Die Prozessanalyse soll die beteiligten Organisationen, Personengruppen und Stellen (analog zu den o. g. internen und externen Prozessbeteiligten) erfassen und hinsichtlich ihrer Rolle und/oder Betroffenheit datenschutzrechtlich einordnen. Einzelne Subprozesse sind zu diesem Zwecke weiter zu detaillieren, wie bspw. der Subprozess „Anbietung und Abgabe“ (vgl. Kapitel 2.13.6) zur Feststellung der beteiligten Akteure und Rollen.

Betroffene Personengruppen sind:

- natürliche Personen/Bürger, zu denen personenbezogene Daten in Primärinformationen erfasst und verarbeitet werden (und die damit auch das Recht zur Einsichtnahme haben);
- Sachbearbeiter im elektronischen Geschäftsgang, deren personenbezogene Daten in Protokollinformationen liegen und die in IT-Systemen potenziell auswertbar sind (Leistungskontrolle);
- Bedienstete, deren personenbezogene Daten in elektronischen Personalakten erscheinen.

3.3 Schutzbedarfs- und Gefährdungsanalyse

Grundlage der Schutzbedarfsanalyse und der anschließenden Analyse der Gefährdungen ist die vollständige Erfassung der im geplanten E-Akte-System zu verarbeitenden elektronischen Dokumente und Informationen im Zuge der oben beschriebenen Prozessanalyse.

3.3.1 Zweck der Schutzbedarfsanalyse

Die Schutzbedarfsanalyse elektronischer Dokumente und auch sonstiger im E-Akte-System erhobener, erzeugter und verarbeiteter personenbezogener Daten zielt darauf, festzustellen, welche negativen Folgen Betroffenen entstehen können, wenn die Daten offengelegt, verfälscht oder verloren werden, inwiefern also insbesondere deren informationelles Selbstbestimmungsrecht beeinträchtigt würde.[105]

[105] Vgl. dazu auch bereits Kapitel 2.11.2.

Für jeden der drei Datentypen Primärdaten, Metadaten und Protokolldaten[106] ist der Schutzbedarf separat zu bestimmen. Bei den Primärdaten ist es ggf. sinnvoll, weitere Subtypen zu definieren, wenn bspw. Teilakten oder einzelne Dokumente besondere Arten personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO bzw. § 22 BDSG enthalten können. Dabei finden auch die bereichsspezifischen Regelungen, wie z. B. des Sozial-, Arbeits- oder Personalrechts, besondere Berücksichtigung.

Im Regelfall ermöglicht erst die Schutzbedarfsanalyse, begründete Aussagen über Risiken der elektronischen Aktenführung zu treffen sowie darauf aufbauend Schutzmaßnahmen festzulegen und umzusetzen. Ihre Ergebnisse legen somit den Grundstein, um die datenschutzrechtlichen Anforderungen an das E-Akte-System, seine Betriebsumgebung sowie weitere organisatorische und personelle Nutzungsbedingungen zu erheben. Sie liefern darüber hinaus die Rechtfertigung für etwaige, zusätzlich anfallende Kosten für technische oder organisatorische Maßnahmen.

3.3.2 Schadensszenarien und Skalierung

Der Schutzbedarf personenbezogener Daten[107] lässt sich je nach eingenommener Perspektive unterschiedlich skalieren.

Die DIN 66399 fokussiert den Verlust von Vertraulichkeit als Schadenszenario, der sich aus der Vernichtung von Datenträgern ergibt. Die in der Norm definierten Schutzklassen 1, 2 und 3 nehmen ausschließlich Bezug auf Schäden durch Offenlegung und nachfolgenden Missbrauch der Daten.

Auch das Schutzstufenkonzept des LfD Niedersachsen konzentriert sich auf die Offenlegung und den Missbrauch personenbezogener Daten und deren Folgen für den Betroffenen. Es unterscheidet fünf Schutzstufen. Dadurch ist es etwas granularer als der DIN-Ansatz, erfasst damit aber ebenfalls noch nicht alle Aspekte der Schutzbedürftigkeit personenbezogener Daten.[108]

Der BSI-Standard 200-2 hat 2017 den Standard 100-2 abgelöst.[109] Wie sein Vorgänger übernimmt er in seiner (weiter gefassten) Szenarienbetrachtung den Begriff des informationellen Selbstbestimmungsrechts. Dieser umfasst deutlich mehr als den Vertraulichkeits- und Missbrauchsschutz.[110] Er entspricht damit eher den Anforderungen des technisch-organisatorischen Datenschutzes (vgl. Kapitel 2.4).

Der Charme des weiten Begriffs besteht einerseits darin, dass das Schadensszenario „Beeinträchtigung des informationellen Selbstbestimmungsrechts*“* auf die Schutzziele *Belastbarkeit, Vertraulichkeit, Integrität und Verfügbarkeit* Anwendung findet. Andererseits bringt ein solches Begriffsverständnis klar zum Ausdruck, dass die Verletzung eines dieser Schutzziele bei der elektronischen Aktenführung negative Auswirkungen auf das informationelle Selbstbestimmungsrecht des Betroffenen haben kann.

---

[106] Siehe dazu Kapitel 2.12.

[107] Siehe Kapitel 2.11.2 Schutzbedarf.

[108] http://www.lfd.niedersachsen.de/download/52033/Schutzstufenkonzept_LfD_Niedersachsen_.pdf

[109] Zur Versionshistorie vgl. BSI, IT-Grundschutz-Methodik Standard 200-2, S. 7, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.html.

[110] Vgl. BSI, IT-Grundschutz-Methodik Standard 200-2, S. 105 ff., https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.html..

Je nachdem, welche Konsequenzen eine Offenlegung, Kompromittierung oder ein Missbrauch der entsprechenden personenbezogenen Daten hat, lassen sich folgende Schutzbedarfskategorien unterscheiden:[111]

- Schutzbedarfskategorie *normal*:

  Der Betroffene kann in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden.

- Schutzbedarfskategorie *hoch*:

  Eine Verletzung kann den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen.

- Schutzbedarfskategorie *sehr hoch*:

  Es droht eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen.

Als methodisches Instrument der Schutzbedarfsanalyse empfiehlt sich der BSI-Standards 200-2, d. h.: Die Analyse sollte für die einzelnen Datentypen bzw. Subtypen einschätzen, ob und in welcher Größenordnung der Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit der Daten das informationelle Selbstbestimmungsrecht der Betroffenen beeinträchtigen kann. Dabei sind stets **auch die mittelbaren Folgen** einer Kompromittierung der Daten in Rechnung zu stellen.

3.3.3 Form der Schutzbedarfsanalyse

Eine Schutzbedarfsanalyse lässt sich am besten in tabellarischer Form dokumentieren. Sie könnte bspw. wie folgt aussehen:

Datentyp	Schutzziel	Schutzbedarf	Begründung
Primärdaten	Vertraulichkeit	Hoch	Es werden Steuer- und Sozialdaten verarbeitet, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte.
	Integrität	Hoch	Es werden Steuer- und Sozialdaten verarbeitet, deren Verfälschung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte.
	Verfügbarkeit	Normal	Die Primärdaten werden parallel in Papierform vorgehalten. Die Betroffenenrechte auf Auskunft lassen sich nur mit Zusatzaufwand gewährleisten.

[111] Siehe BSI, IT-Grundschutz-Methodik Standard 200-2, S. 104 ff., https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.html.

Metadaten	Vertraulichkeit	Normal	Die Metadaten enthalten typischerweise keine Informationen, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen nennenswert beeinträchtigt.
	Integrität	Hoch	Eine Verfälschung der Metadaten könnte zum Verlust von Primärdaten führen. Außerdem könnten unberechtigte Zugriffe auf zugehörige Primärdaten unbemerkt bleiben, sodass ein erheblicher Schaden droht.
	Verfügbarkeit	Hoch	Der Verlust der Metadaten könnte zum Verlust von Primärdaten führen. Außerdem könnten unberechtigte Zugriffe auf zugehörige Primärdaten unbemerkt bleiben, sodass ein erheblicher Schaden entstehen könnte.
Protokolldaten	Vertraulichkeit	Normal	Die Protokolldaten enthalten keine Informationen, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen nennenswert beeinträchtigen würde.
	Integrität	Hoch	Eine Verfälschung der Protokolldaten könnte dazu führen, dass unberechtigte Zugriffe auf Primärdaten unbemerkt bleiben, sodass ein erheblicher Schaden droht.
	Verfügbarkeit	Hoch	Der Verlust der Protokolldaten könnte dazu führen, dass unberechtigte Zugriffe auf Primärdaten unbemerkt bleiben, sodass ein erheblicher Schaden droht.

Tabelle 1: Beispiel für eine Schutzbedarfsanalyse von Datenarten

3.3.4 Gefährdungsanalyse

Die Gefährdungsanalyse erfasst die Gefahrenquellen für den Schutz der Primär-, Meta- und Protokolldaten unter Berücksichtigung des jeweiligen Schutzbedarfs möglichst vollständig.

Unmittelbare Gefährdungen entstehen, wenn die datenschutzrechtlichen Grundsätze der DSGVO (siehe Kapitel 2.1) nicht oder nur ungenügend eingehalten werden. Folgende unmittelbare Risiken lassen sich typisierend unterscheiden:

Gefährdung	Gefährdete Schutzziele[112]	Kapitel
Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten	Unverkettbarkeit; Vertraulichkeit	2.2
Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten	Unverkettbarkeit; Vertraulichkeit	2.3
Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten	Unverkettbarkeit	2.1.1
Fehlende oder unzureichende Datenminimierung bei der Verarbeitung personenbezogener Daten	Unverkettbarkeit	2.1.1
Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten	Vertraulichkeit	2.2.3
Fehlende oder nicht ausreichende Datenschutz-Folgenabschätzung	Alle	2.5
Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten	Intervenierbarkeit, ggf. Unverkettbarkeit und Transparenz	2.7
Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten	Alle	2.4

Tabelle 2: Unmittelbare datenschutzrechtliche Gefährdungslagen

Mittelbare Gefährdungen des informationellen Selbstbestimmungsrechts können sich ergeben, wenn bei der Realisierung, beim Betrieb oder bei der Nutzung des E-Akte-Systems keine oder nur unzureichende technisch-organisatorische Maßnahmen erfolgen, um die Schutzziele entsprechend dem Schutzbedarf der Daten zu erreichen.

Anhaltspunkte für solche indirekten Gefahrenquellen bietet das Verzeichnis der Elementargefährdungen aus den IT-Grundschutzkatalogen des BSI. Typische (indirekte) Gefährdungen[113] können bspw. sein:

Gefährdung	Gefährdete Schutzziele	Kapitel
Verlust gespeicherter Daten	Verfügbarkeit, Transparenz, Intervenierbarkeit	2.4, 2.7
Überlastung von Informationssystemen	Integrität, Verfügbarkeit, Belastbarkeit	2.4
Fehlfunktion von Geräten oder Systemen	Alle	2.4, 2.7
Software-Konzeptionsfehler	Alle	2.2, 2.3

[112] Zu den einzelnen Schutzzielen s. Kapitel 2.11.1

[113] Vgl. die IT-Grundschutz-Kataloge des BSI zu den Elementargefährdungen („G 0 – Elementare Gefährdungen"), abrufbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g00/g00.html. Hierunter fallen bspw. Gefährdungen durch Feuer, Wasser, Verschmutzung usw.

Gefährdung	Gefährdete Schutzziele	Kapitel
Software-Schwachstellen oder -Fehler	Alle	2.2, 2.3, 2.4
Ausspähen von Informationen / Spionage	Vertraulichkeit	2.2.3, 2.6
Abhören	Vertraulichkeit	2.2.3, 2.6
Sorglosigkeit im Umgang mit Informationen	Vertraulichkeit, Intervenierbarkeit	2.2.3
Missbrauch von Berechtigungen	Alle	2.2.4, 2.3, 2.6

Tabelle 3: Beispiele indirekter Gefährdungen für den Datenschutz

3.4 Planung und Umsetzung von Maßnahmen

Die technischen und organisatorischen Maßnahmen, welche das informationelle Selbstbestimmungsrecht schützen, sind in einem **Datenschutz- und Datensicherheitskonzept** (inkl. Rollen-, Rechte- und Protokollierungskonzept) zu definieren, das auf das geplante elektronische Verfahren abgestimmt ist.

Es behandelt die spezifischen Gefährdungen und Maßnahmen für die Anwendung zur elektronischen Vorgangsbearbeitung und Aktenhaltung im Rahmen der definierten Soll-Prozesse (bei der Betrachtung bleiben bspw. Maßnahmen in den Bereichen Netzwerksicherheit, Virenschutz etc. außen vor).

In diesem Zusammenhang sind u. a. Regelungen zu folgenden Punkten zu treffen:

- Authentisierung,
- Speicherung und Archivierung,
- Erfassung und Nutzung von Protokolldaten,
- Signaturen, Verschlüsselung und ggf. Nachsignierung,
- Virtuelle Poststelle,
- Organisationspostfächer,
- Dienstanweisungen.

3.4.1 Standardmaßnahmen

Im Rahmen des elektronischen Geschäftsgangs hat der Verantwortliche eine Vielzahl von Schutzmaßnahmen in den Blick zu nehmen und bei Bedarf vorzunehmen. Exemplarisch die Anwendung relevanter Schutzmaßnahmen. Der IT-Grundschutzbaustein B 1.5 „Datenschutz“[114] fasst insoweit wichtige Empfehlungen zusammen.

3.4.1.1 Prüfung rechtlicher Rahmenbedingungen und Datenschutz-Folgenabschätzung bei der Verarbeitung personenbezogener Daten

Bei der Analyse der rechtlichen Rahmenbedingungen der Datenverarbeitung sind von besonderer Bedeutung:

[114] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01005.html.

- handelt es sich bei verarbeiteten Daten um personenbezogene Daten?;
- Besteht eine Einwilligung oder eine gesetzliche Verarbeitungserlaubnis?;
- Ist die Verarbeitung personenbezogener Daten erforderlich?;
- Steht die Datenverwendung im Einklang mit dem Zweckbindungsgrundsatz?;[115]
- Ist eine Datenschutz-Folgenabschätzung aufgrund voraussichtlich hohen Risikos für die Rechte und Freiheiten natürlicher Personen erforderlich und durchgeführt worden?[116] Es empfiehlt sich, die Folgenabschätzung auf der Grundlage eines IT-Sicherheitskonzeptes nach IT-Grundschutz vorzunehmen, in dem die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen für das E-Akte-System dokumentiert ist.

Hinweis

Der IT-Grundschutz sowie die Datenschutzgesetze einiger Länder fordern zusätzlich eine schriftliche datenschutzrechtliche Freigabe beim erstmaligen Einsatz von IT-Verfahren, die personenbezogene Daten verarbeiten.

3.4.1.2 Festlegung technisch-organisatorischer Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

Bei der Planung und Durchführung der technischen und organisatorischen Maßnahmen, die Art. 24, 25 und 32 DSGVO[117] dem Verantwortlichen abverlangen, ist entscheidend, sie als ein zusammenwirkendes Schutzsystem zu verstehen. Dann erst ein solches gewährleistet einerseits rechtlich erforderlichen Datenschutz und andererseits aber auch einen ordentlichen Betriebsablauf, der sicherstellt, dass die Behörde ihre Aufgaben ordnungsgemäß wahrnehmen kann. Deshalb ist es wichtig, das Datenschutzkonzept jeweils in Abstimmung mit den Fachkonzepten der betreffenden Organisationseinheiten und den sonstigen Sicherheitskonzepten, z. B. dem Informationssicherheitskonzept, zu entwickeln und anzuwenden.

Der Aufwand, der sich mit den notwendigen Maßnahmen verknüpft, sollte in einem angemessenen Verhältnis zum angestrebten Schutzzweck und zum ermittelten Schutzbedarf stehen. Der Unionsgesetzgeber fordert von dem Verantwortlichen keine über das Ziel hinausschießenden Maßnahmen, sondern ein „angemessenes Schutzniveau“ (Art. 32 Abs. 1 DSGVO), das eine „Verarbeitung gemäß [der DSGVO]“ (Art. 24 Abs. 1 S. 1 DSGVO; vgl. auch Art. 25 Abs. 1 DSGVO) sicherstellt.

[115] Überschreitet die anvisierte (Weiter-)Verarbeitung die ursprüngliche Zwecksetzung (Art. 6 Abs. 4 DSGVO), bedarf die neue Verarbeitung einer Einwilligung oder einer gesetzlichen Gestattung der Verarbeitung, welche die Auflösung der Zweckbindung rechtfertigt. Art. 6 Abs. 4 formuliert an gesetzliche Erlaubnisse zweckändernder Verarbeitung hohe Anforderungen: Sie müssen insbesondere dem Prinzip der Verhältnismäßigkeit genügen und sich unter die Zweckbestimmungen des Art. 23 DSGVO rubrizieren lassen (siehe dazu Kapitel 2.3).

[116] Im Rahmen der Datenschutz-Folgenabschätzung ist vor dem erstmaligen Einsatz automatisierter Verfahren zur Bearbeitung personenbezogener Daten zu prüfen, welche Gefahren hierdurch für das informationelle Selbstbestimmungsrecht erwachsen können (siehe Kapitel 0.844126.0.0.).

[117] Siehe dazu Kapitel 2.4.

3.4.1.3 Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten

Diejenigen Personen, die mit personenbezogenen Daten in Berührung kommen, sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten[118] bzw. darüber zu unterrichten. Die Verpflichtung, das Dienstgeheimnis zu wahren, besteht auch nach Beendigung der Tätigkeit fort. Die Verpflichtung/Unterrichtung muss in geeigneter Weise durchgeführt werden; die Durchführung ist zu dokumentieren und bei Bedarf zu wiederholen.

3.4.1.4 Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten

Die Betroffenenrechte, welche die DSGVO formuliert, namentlich das Recht auf Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18) und auf Widerspruch (Art. 21),[119] muss jede Behörde einlösen (können). Sie hat technisch-organisatorische Verfahren zu entwickeln, welche die Durchsetzung der Rechte sicherstellen. Dazu gehören auch Informationen über die Betroffenenrechte „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ (Art. 12 Abs. 1 S. 1 DSGVO). Der Unionsgesetzgeber gibt dem Verantwortlichen insbesondere auf, „der betroffenen Person die Ausübung ihrer Rechte“ zu erleichtern (Art. 12 Abs. 2 S. 1 DSGVO) sowie Informationen über Mitteilungen und Maßnahmen unentgeltlich zur Verfügung zu stellen (Art. 12 Abs. 5 S. 1 DSGVO). Diese Verfahren müssen so beschaffen sein, dass die Rechte der Betroffenen schnell und zweckmäßig umsetzbar sind.

3.4.1.5 Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten

Soweit ein externer Dienstleister das E-Akte-System betreibt, ist der Tatbestand der Auftragsdatenverarbeitung erfüllt (siehe Art. 28 DSGVO, Kapitel 2.6). Die Auftragsverarbeitung als solche entbindet den Auftraggeber aber nicht davon, die Einhaltung der datenschutzrechtlichen Normen sicherzustellen. Er hat den Auftragnehmer insbesondere sorgfältig auszuwählen (Art. 28 Abs. 1 DSGVO).

Abhängig davon, wie schutzbedürftig die personenbezogenen Daten sind, die im Auftrag verarbeitet werden sollen, sind die Anforderungen an den Vertrag mit dem Auftragnehmer an die jeweilige Situation anzupassen. Je schutzwürdiger sie sind, desto enger und präziser muss der Auftrag formuliert werden. Die Vorgaben an den Vertrag (bzw. das andere Rechtsinstrument, welches das Auftragsverhältnis regelt) beschreibt Art. 28 Abs. 3 DSGVO en détail.[120] Bei besonders sensiblen Verarbeitungen kann sich eine Vergabe an Außenstehende gänzlich verbieten (z. B. Fahndungsdaten).

---

[118] Diese Pflicht ergibt sich (auch wenn weder die DSGVO noch das BDSG n. F. eine dem § 5 BDSG a. F. entsprechende Regelung kennen), aus Art. 5 Abs. 2, 24 Abs. 1 S. 1 DSGVO. Auch in die Verarbeitung eingeschaltete Auftragsverarbeiter müssen gewährleisten, „dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen“ (Art. 29 Abs. 3 lit. b).

[119] Siehe dazu oben Kapitel 2.7.

[120] Dazu *Martini*, in: Paal/Pauly, DS-GVO Art. 28, Rn. 27 ff.

3.4.1.6 Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten

Bei datenbankbasierten IT-Anwendungen besteht aufgrund ihrer Systemarchitektur die grundsätzliche Möglichkeit, mittels nicht unmittelbar in dem Programm vorgesehener Werkzeuge (z. B. Script-Sprachen, SQL-Editoren) auf Datenbankinhalte zuzugreifen. Damit lassen sich Informationen abfragen und aggregieren sowie Auswertungen vornehmen, die in der Software so nicht vorgesehen und ggf. datenschutzrechtlich unzulässig sind.

Die Daten, auf die solche Werkzeuge zugreifen sollen, und die zu eröffnenden Abfragearten sind einer Vorab-Prüfung zu unterziehen.

Keine datenschutzrechtlichen Bedenken bestehen gegen den Einsatz solcher Abfragewerkzeuge dann, wenn die Auswertung nur zu anonymisierten Ergebnissen führt, d. h. Rückschlüsse auf einzelne Personen nicht möglich sind. Denn die DSGVO findet nur auf die Verarbeitung personenbezogener Daten Anwendung (Art. 2 Abs. 1 DSGVO). Datensätze sind allerdings nicht bereits dadurch anonymisiert, dass sie selbst keinen Rückschluss auf einzelne Personen zulassen. Solange sich durch durch eine Verknüpfung mit anderen Daten (insb. einer anderen Datenbank), auf die der Verantwortliche ebenfalls zugreifen kann, der Personenbezug wieder herstellen lässt, sind die Daten nicht anonymisiert, sondern allenfalls pseudonymisiert – mit der Folge, dass sie nach wie vor den Regelungen der DSGVO unterliegen.

3.4.1.7 Datenschutzaspekte bei der Protokollierung

Protokollierung beim Betrieb von IT-Systemen ist ein Instrument, um mit Hilfe manueller oder automatisierter Aufzeichnungen Verarbeitungsvorgänge auch Ex post nachvollziehbar zu machen, etwa um zu ermitteln:: „Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: „Wer hatte von wann bis wann welche Zugriffsrechte?"

Die DSGVO trägt dem Verantwortlichen zwar auf, ein Verfahrensverzeichnis zu führen (Art. 30 Abs. 1 DSGVO). Eine umfassende, *allgemeine* Protokollierungspflicht ergibt sich daraus aber noch nicht, beschränkt sich der Gesetzgeber in Art. 30 Abs. 1 S. 2, Abs. 2 DSGVO doch auf allgemeine Grundlagendaten.[121] Art. 5 Abs. 2 DSGVO gibt dem Verantwortlichen allerdings auf, die Einhaltung der datenschutzrechtlichen Grundsätze stets „nachweisen [zu] können“. Es ist daher – auch für den Haftungsfall – jedenfalls empfehlenswert, automatisierte Verarbeitungsprozesse zu protokollieren (vgl. auch Art. 24 Abs. 1 S. 1 DSGVO [„Nachweis dafür erbringen zu können, dass …“]).

Bei der Verarbeitung personenbezogener Daten sind in Abhängigkeit von der Sensibilität der Verfahren und der Daten vollständig bzw. selektiv folgende Benutzeraktivitäten zu protokollieren:

Benutzeraktivität	**Anforderungen an die Protokollierung**
Eingabe von Daten	Die sog. Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z. B. Protokollierung in Akten, soweit vorhanden / Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden).

[121] Eine allgemeine Protokollierungspflicht ergibt sich mangels ausdrücklicher Nennung auch nicht aus Art. 24 Abs. 1 DSGVO, der Art. 5 DSGVO konkretisiert, oder aus Art. 32 DSGVO. Die Protokollierungspflichten der DSGVO (Art. 28 Abs. 3 S. 2 lit. a; Art. 30; Art. 33 Abs. 5 S. 1; Art. 49 Abs. 6 i. V. m. Art. 30 Abs. 1 lit. e bzw. Abs. 2 lit. c), dass der Unionsgesetzgeber den (sanktionsbewehrten) Protokollierungspflichtenkatalog nicht implizit, sondern stets explizit in die Normen integriert hat.

	Auch wenn man davon ausgeht, dass Befugnisüberschreitungen anderweitig protokolliert werden, ist eine vollständige Protokollierung von Dateneingaben als Regelfall anzusehen.
Datenübermittlungen	Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, ist eine selektive Protokollierung ausreichend.
Benutzung von automatisierten Abrufverfahren	In der Regel ist eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich, um unbefugte Kenntnisnahme im Rahmen der grundsätzlich eingeräumten Zugriffsrechte aufdecken zu können.
Löschung von Daten	Die Durchführung der Löschung ist zu protokollieren.
Aufruf von Programmen	Eine Protokollierung des Programmaufrufs kann bei besonders „sensiblen" Programmen, deren Nutzung z. B. nur zu bestimmten Zeiten oder Anlässen zulässig ist, erforderlich sein. Deshalb ist jedenfalls in diesen Fällen eine vollständige Protokollierung angezeigt. Diese entlastet auch die befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

Tabelle 4: Anforderungen an die Protokollierung aus Sicht des Datenschutzes

Wie effektiv die Protokollierung und ihre Auswertung im Rahmen von Kontrollen ist, hängt im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang sollten folgende Aspekte Berücksichtigung finden:

- Empfehlenswert ist es, ein Konzept zu erstellen, das den Zweck der Protokolle und deren Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert.
- Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muss ebenso gewährleistet sein wie die Manipulationssicherheit der Einträge in Protokolldateien. Gleichzeitig stellt die DSGVO keine technisch unmöglichen Forderungen auf: Da es bei vielen Systemen technisch bedingt (mindestens) einen Administrator mit vollem Zugriff auf die Systeme gibt, dem insbesondere die (technische) Berechtigung zum Löschen von Protokolldateien zukommt, steht diese Ausgestaltung dem Erfordernis der Zwangsläufigkeit und Vollständigkeit der Protokolle nicht per se entgegen. Den aus dieser Berechtigung resultierenden Risiken hat der Verantwortliche vielmehr mit den anderen hier aufgeführten Mitteln zu begegnen, etwa durch Etablierung von 4-Augen-Prinzipien, Durchführung von Routinekontrollen und ähnlichem.
- Entsprechend der Zweckbindung der Datenbestände sind wirksame Zugriffsbeschränkungen zu realisieren.
- Die Protokolle müssen so gestaltet sein, dass eine effektive Überprüfung möglich ist. Dazu gehört auch eine IT-Unterstützung der Auswertung.
- Die Auswertungsmöglichkeiten sollten vorab abgestimmt und festgelegt sein.
- Kontrollen sind so zeitnah vorzunehmen, dass es möglich bleibt, bei aufgedeckten Verstößen noch Schäden abzuwenden sowie etwaige Konsequenzen zu ziehen. Kontrollen müssen insbesondere auch rechtzeitig vor dem Ablauf der relevanten Löschungsfristen stattfinden. Im Falle einer Verletzung der IT-Sicherheit, die in eine Vernichtung, den Verlust oder die Veränderung bzw. unbefugte Offenlegung personenbezogener Daten mündet (Art. 4 Nr. 12 DSGVO), sieht die DSGVO strikte, zeitgebundene

Meldepflichten für Behörden ebenso wie für nicht-öffentliche Stellen vor (Kapitel 2.4.2.2). Art. 33 Abs. 1 S. 1 und Art. 34 Abs. 1 fordern insoweit vom Verantwortlichen, die Verletzung „unverzüglich“ sowohl der nationalen Datenschutz-Aufsichtsbehörde (Art. 33 Abs. 1 S. 1 DSGVO) als auch dem Betroffenen (Art. 34 Abs. 1 DSGVO) kundzutun.

- Kontrollen sollten nach dem Vier-Augen-Prinzip erfolgen.
- Die Mitarbeiter sollten darüber informiert sein, dass Überprüfungen (ggf. auch unangekündigt) erfolgen.
- Personalräte sollten bei der Erarbeitung des Protokollierungskonzeptes und bei der Festlegung der Auswertungsmöglichkeiten der Protokolle beteiligt werden.

3.4.1.8 Verschlüsselung

3.4.1.8.1. Allgemeines

Art. 32 Abs. 1 lit. a DSGVO nennt die Verschlüsselung explizit als konkrete und effektive Maßnahme, um die Vertraulichkeit der Datenverarbeitung sicherzustellen. Art. 4 DSGVO hält jedoch keine Definition hierfür bereit. Einen greifbaren Anhaltspunkt, um sich dem Topos anzunähern, liefert der Rückgriff auf die Beschreibung im IT-Grundschutzkatalog des BSI.[122]

Die Methodik der Verschlüsselung (symmetrisch oder asymmetrisch), die Schlüssellänge sowie die Organisation der ordnungsgemäßen Schlüsselgenerierung und -verwaltung müssen nach Art. 32 Abs. 1 DSGVO dem Stand der Technik entsprechen.[123]

3.4.1.8.2. Transportverschlüsselung (TLS/SSL)

Die technischen und organisatorischen Datenschutz- und Datensicherheits-Maßnahmen sind so zu wählen und zu implementieren, dass sie „ein dem Risiko angemessenes Schutzniveau gewährleisten“ (Art. 32 Abs. 1 DSGVO). Der Umfang der Verpflichtung ist also prinzipiell durch das Risiko der Verarbeitung bestimmt. Die Transportverschlüsselung ist aber mittlerweile Stand der Technik und so ist es üblich, dass sie als Maßnahme stets und nicht mehr nur bei erhöhtem Schutzbedarf einzuplanen ist.

E-Akte-Systeme verwenden zur Datenkommunikation zumeist standardisierte Internetprotokolle wie HTTP (Webserver), SMTP (Mail), WebDAV (Dateiservice) oder LDAP (Verzeichnisdienst).

Eine Verschlüsselung der Datenkommunikationsverbindungen sollte – dem konkreten Risiko entsprechend – mittels des Sicherheitsprotokolls SSL (Secure Socket Layer) bzw. dessen Weiterentwicklung TLS (Transport Layer Security) erfolgen.

---

[122] „Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die ‚Schlüssel‘ genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt“, vgl. IT-Grundschutz-Katalog des BSI, Glossar, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.

[123] Vgl. *Schläger*, in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, 2018, Teil G, Rn. 51 f. (S. 489), sowie *von Rahden*, a.a.O., Teil I, Rn. 108 ff. (S. 546 ff.).

Das BSI hat insoweit einen „Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden nach § 8 Abs. 1 Satz 1 BSIG“[124] veröffentlicht, der einzuhalten ist. Der parallel veröffentlichte Migrationsleitfaden „Migration auf TLS 1.2 – Handlungsleitfaden“[125] vermittelt, welche Systeme bis wann auf TLS umzustellen sind.

3.4.1.9 Datenschutz im laufenden Betrieb

Die interne Datenschutzkontrolle obliegt der Leitung der verantwortlichen Stelle. Sie kann und sollte aber auch den Datenschutzbeauftragten hinzuziehen (vgl. Kapitel 2.8). Zu den Prüfaspekten im laufenden Betrieb gehören:

- die Überprüfung der Verfahren darauf, dass sie sich auf eine ausreichende Verarbeitungsgrundlage stützen können und nicht gegen das Gebot der Zweckbindung verstoßen,
- die Sicherstellung der Rechte betroffener Personen auf Auskunft, Berichtigung, Sperrung, Löschung (Art. 12 ff. DSGVO),[126]
- die Unterrichtung über bzw. die Verpflichtung der Mitarbeiter auf den Datenschutz,
- die Sicherstellung der erforderlichen Meldung und Benachrichtigung über Verletzungen des Schutzes personenbezogener Daten (Art. 33 f. i. V. m. Art. 4 Nr. 12 DSGVO)[127],
- ggf. das Führen von Geräteverzeichnissen und
- die Untersuchung der aus den gesetzlichen Vorschriften abgeleiteten technisch-organisatorischen Maßnahmen, welche zur Kontrolle von Zutritt, Zugang, Zugriff, Weitergabe, Eingabe, Auftrag, Verfügbarkeit und „getrennter Verarbeitung gemäß der Zweckbestimmung" implementiert wurden.

Für das Verfahrensverzeichnis[128] ist die öffentliche Stelle verantwortlich, nicht allein der Datenschutzbeauftragte (Art. 30 Abs. 1 DSGVO); sie kann die interne Aufgabenverteilung aber entsprechend regeln.

3.4.1.10 Datenschutzgerechte Löschung/Vernichtung

Beim Löschen sensibler oder vertraulicher Daten auf magnetischen Datenträgern ist zu gewährleisten, dass die Daten sicher, d. h. vollständig und unumkehrbar, gelöscht werden. Dies ist sowohl aus der Sicht des Datenschutzes als auch der Informationssicherheit geboten. Der Zustand, in dem die Unterlagen als vernichtet gelten können, ist zudem festzulegen. Nur dann ist dem Zweck einer gesetzlichen Löschungspflicht (Art. 17 Abs. 1 DSGVO) hinreichend Rechnung getragen.

Eine Orientierung bietet die Norm DIN 66399 (Vernichten von Datenträgern) . Hiernach reicht es aus, die Informationsträger so zu vernichten, dass die Repro-

[124] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile

[125] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Migrationsleitfaden_Mindeststandard_BSI_TLS_1_2_Version_1_2.pdf?__blob=publicationFile&v=4

[126] Siehe dazu Kapitel 2.7.

[127] Siehe dazu Kapitel 2.4.2.2.

[128] Siehe dazu Kapitel 2.9.

duktion der auf ihnen wiedergegebenen Informationen nur unter erheblichem Aufwand an Personen, Hilfsmitteln oder Zeit möglich ist (Schutzstufe 3).

3.4.2 Empfohlene technische Maßnahmen bei erhöhtem Schutzbedarf

Ein erhöhter Schutzbedarf besteht immer dann, wenn die BSI-Methodik einen hohen oder sehr hohen Schutzbedarf ergeben hat oder entsprechend DIN 66399 eine Verarbeitung von Daten der Schutzklassen 2 oder 3 vorliegt.

Verarbeitet das System besondere personenbezogene Daten i. S. d. Art. 9 Abs. 1 DSGVO bzw. § 22 BDSG provoziert das automatisch einen erhöhten Schutzbedarf.

3.4.2.1 Datenbank-Verschlüsselung

Werden personenbezogene Daten mit hohem Schutzbedarf (etwa der Schutzklasse 3 im Sinne von DIN 66399) verarbeitet, kann es notwendig sein, diese Daten in der Datenbank zu verschlüsseln.[129]

Dabei lässt sich zwischen einer Online- und einer Offline-Verschlüsselung unterscheiden:

- Die *Online-Verschlüsselung* ver- und entschlüsselt die Daten während des laufenden Betriebs, ohne dass die betroffenen Benutzer davon etwas merken. Dafür können Tools Verwendung finden, die entweder auf Betriebssystemebene die gesamte Festplatte verschlüsseln, oder solche, die nur die Anwendungsdaten der Datenbank verschlüsseln.
- Eine *Offline-Verschlüsselung* verschlüsselt die Daten hingegen erst nach ihrer Bearbeitung und entschlüsselt sie vor ihrer Weiterverarbeitung wieder. Dies erfolgt im Allgemeinen mit Tools, die nicht in das Datenbanksystem integriert sind. Das kann insbesondere für Datensicherungen oder Datenübertragungen sinnvoll sein. Auf der Festplatte muss jeweils genügend Platz für das Original und die verschlüsselte Version der Datenbank vorhanden sein. Nur dann lässt sich die Ver- bzw. Entschlüsselung erfolgreich ausführen.

Darüber hinaus besteht die Möglichkeit, Daten zwar weiterhin im Klartext in der Datenbank abzuspeichern, beim Zugriff über ein Netz jedoch eine verschlüsselte Datenübertragung zu realisieren (je nach praktischer Ausgestaltung bspw. via TLS/SSL oder Ende-zu-Ende-Verschlüsselung).

Welche Daten mit welchem Verfahren zu verschlüsseln sind, ist im Idealfall bereits bei der Auswahl der Software festzustellen.

Falls keine am Markt verfügbare Datenbank-Standardsoftware den Anforderungen entspricht, ist der Einsatz von Zusatzprodukten zu prüfen, um die entsprechende Sicherheitslücke zu schließen.

3.4.2.2 Pseudonymisierung

Neben der Verschlüsselung personenbezogener Daten verlangt der Unionsgesetzgeber Verantwortlichen im Regelfall auch die Pseudonymisierung als Schutzmaßnahme ab (Art. 32 Abs. 1 lit. a DSGVO; vgl. auch Art. 25 Abs. 1, Art. 6 Abs. 4 lit. e, ErwGrd 28 ff. DSGVO). Eine Pseudonymisierung zeichnet sich

[129] Eine Datenbank-Verschlüsselung ist allerdings nicht mehr nur höheren Schutzbedarfen „vorbehalten", sondern auch in anderen Fällen empfehlenswert.

dadurch aus, dass sie eine Person nur unter Zuhilfenahme eines besonderen, getrennt aufbewahrten Schlüssels identifizierbar macht (Art. 4 Nr. 5 DSGVO). Zur Pseudonymisierung stehen dem Verantwortlichen verschiedene Verfahren bereit, von denen er je nach Gefahrenlage ein geeignetes und angemessenes auswählen kann.[130] In jedem Fall sollte er darauf achten, dass er nicht ein und denselben Identifikationsschlüssel für mehrere Datenbanken verwendet. Anderenfalls könnte bereits die Kompromittierung eines Schlüssels die Pseudonymisierung in mehreren Datenbanken unwirksam machen.

3.4.2.3 Back-up-Vorsorge

Sicherheitskopien zu erstellen, trägt dazu bei, Daten, die einen hohen Schutzbedarf haben, hinreichend sicher verfügbar zu machen. Solche Back-up-Dateien sind grundsätzlich örtlich getrennt von den Originaldaten aufzubewahren, um eine gleichzeitige physische Zerstörung beider Datenbestände zu verhindern. Die Kopien zu verarbeiten, ist grundsätzlich nur zulässig, wenn die Integrität der Originaldaten beschädigt ist oder diese nicht mehr verfügbar sind.

Der Einsatz von RAID-Systemen (ab RAID 1) kann vor physischen Ausfällen der Festplatten schützen. Diese Systeme speichern Daten zeitgleich auf zwei verschiedenen Festplatten. Fällt eine der Festplatten aus, liest das System die Daten von der anderen Festplatte aus. Weil das System die Daten immer zeitgleich an zwei Orten speichert, schützt der isolierte Einsatz von RAID-Systemen nicht vor Viren und Programmfehlern. Ist die Datei also fehlerhaft, so halten die eingesetzten Festplatten dieselbe defekte Datei zweimal vor. Daten sind zudem stets nach dem Großvater-Vater-Sohn-Prinzip zu speichern, so dass **immer mehrere Generationen** einer Sicherheitskopie bestehen. Der Abstand, in dem eine neue Generation einer Sicherungskopie in Form einer Vollsicherung anzulegen ist, ist an der Wichtigkeit der Daten zu bemessen. Es bietet sich ferner an, Vollsicherungen durch regelmäßige Differenzsicherungen zu flankieren. Diese erfassen nur etwaige Veränderungen der Daten.

Gesamte Back-up-Systeme bereitzustellen, die zerstörte Verarbeitungssysteme ohne (größere) zeitliche Verzögerungen substituieren können, erscheint hingegen in Anbetracht der Kosten, die typischerweise mit der Vorhaltung solcher Systeme einhergehen, auch bei Daten mit einem hohen Schutzbedarf nicht erforderlich. Nur bei Daten mit sehr hoher Schutzbedarfskategorie, etwa bei Gesundheits- und Personaldaten, ist es erforderlich und angemessen, gesamte Back-up-Systeme vorzuhalten.

3.4.2.4 Elektronische Signaturen und Eingabekontrollen

Der Einsatz elektronischer Signaturen, die mit einer doppelten Verschlüsselung arbeiten, schützt die Integrität der vorgehaltenen Daten. Solche elektronischen Signaturen bestehen aus einem Signaturschlüssel, der die Signatur erzeugt, und einem Signaturprüfschlüssel, der die Signatur überprüft. So ist klar identifizierbar, wer Daten signiert und ob sie unverfälscht sind.

Eingabekontrollen machen rückverfolgbar, wer Daten eingegeben, verändert oder entfernt hat. Hierzu werten die Eingabekontrollen angelegte Protokolldaten aus. Damit dies nicht zu einer rechtswidrigen Überwachung der Mitarbeiter führt, sind solche Kontrollen nur im Bedarfsfall angebracht – z. B. wenn nach dem Ein-

[130] Instruktiv hierzu *Art.-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, S. 24 ff., abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf.

satz von Signaturschlüsseln feststeht, dass Daten verfälscht wurden. Selbst dann ist regelmäßig die Mitwirkung des Datenschutzbeauftragten und/oder eines Vertreters der Personalvertretung erforderlich, entsprechende Regelungen können beispielsweise in der einschlägigen IuK-Dienst- bzw. Betriebsvereinbarung enthalten sein.

3.5 Anforderungsspezifikation

Verarbeitungssysteme müssen einer Vielzahl von Anforderungen gerecht werden.[131] Ihre Vorgaben sind entsprechend der jeweiligen Sollkonzeption des einzuführenden Systems auszuformen, zu bewerten und zu priorisieren.

Nr.	Bezeichnung	Beschreibung	Schutzziele
FA-001	Anzeige der Organisationseinheit und Stellen (Kürzel)	Das System muss die Anzeige der Organisationseinheit und des Stellenkürzels zu den Benutzernamen in Zu- und Weiterleitungsdialogen unterstützen, um so Fehladressierungen vorzubeugen.	Vertraulichkeit
FA-002	Anzeige von Metadaten bei der Registrierung	Das System muss die Anzeige von Metadaten (wie etwa Aktenbetreff, Aktenplaneintrag, Organisationseinheit, Anzahl, Vorgänge) unterstützen, um so fehlerhaften Zuordnungen elektronischer Dokumente zu Akten und Vorgängen vorzubeugen.	Vertraulichkeit
FA-003	Keine Auswahlmöglichkeit zdA-verfügter Vorgänge	Das System darf zdA-verfügte Vorgänge in Dialogen zur Registrierung von Posteingängen nicht anzeigen, um fehlerhafte Zuordnungen elektronischer Dokumente zu Akten und Vorgängen zu vermeiden.	Integrität
FA-004	Protokollierung von Änderungen	Alle Änderungen von Primär- und Metadaten von Schriftgutobjekten hat das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Integrität, Transparenz
FA-005	Protokollierung lesender Zugriffe	Lesende Zugriffe auf Primärdaten hat das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Transparenz
FA-006	Protokollierung von Zu- und Weiterleitungen	Alle im Rahmen des elektronischen Geschäftsgangs vorgenommenen Zu- und Weiterleitungen von Schriftgutobjekten (im Original und als elektronische Kopie) hat das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Vertraulichkeit, Integrität, Transparenz
FA-007	Protokollierung von Löschungen	Löschungen elektronischer Schriftgutobjekte hat das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Integrität, Verfügbarkeit, Transparenz

[131] Sie verstehen sich als Ergänzung des im Baustein „Projektleitfaden“ genannten Anforderungskatalogs in Kapitel 7.2.3.

Nr.	Bezeichnung	Beschreibung	Schutzziele
FA-008	Protokollierung der Registrierung	Alle Zuordnungen elektronischer Posteingänge zu Vorgängen und Akten sowie Änderungen in der Zuordnung elektronischer Schriftgutobjekte zu elektronischen Akten hat das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Vertraulichkeit, Integrität, Transparenz
FA-009	Protokollierung von Zeichnungen und Geschäftsgangvermerken	Alle im Rahmen des elektronischen Geschäftsgangs vorgenommenen Zeichnungen und Geschäftsgangvermerke von/zu Schriftgutobjekten hat das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Vertraulichkeit, Integrität, Transparenz
FA-010	Protokollierung der Vergabe von Vertraulichkeitsstufen	Die Vergabe von Vertraulichkeitsstufen für Schriftgutobjekte ist durch das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Vertraulichkeit, Integrität, Transparenz
FA-011	Protokollierung der Stellvertretung	Stellvertretungen und die in Stellvertretung vorgenommenen Änderungen hat das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Vertraulichkeit, Integrität, Transparenz
FA-012	Verfügbarkeit der Protokollinformationen in hierarchisch übergeordneten Objekten	Die Protokollinformationen über bestimmte, an Schriftgutobjekten vorgenommene Änderungen (wie Löschung, Änderung der Zugriffsrechte, Änderung der Zuordnung zu Vorgängen und Akten, zdA-Verfügung) sind in den jeweils übergeordneten Objekten verfügbar zu halten.	Integrität, Transparenz
FA-013	Versionierung nach Wechsel des Bearbeitungsrechts	Das System muss bei Änderungen des Primärdokuments nach Wechsel des Bearbeiters eine neue Version des Primärdokuments erzeugen.	Integrität, Transparenz
FA-014	Versionierung nach Zeichnung	Das System muss bei Änderungen eines mit- oder schlussgezeichneten, elektronischen Dokuments eine neue Version des Primärdokuments erzeugen.	Integrität, Transparenz
FA-015	Zeichnen/Signieren	Mit- und Schlusszeichnungen müssen im System auf verschiedene Arten erfolgen können (ohne Passwort, mit Login-Passwort, mit separatem Zeichnungspasswort, mittels persönlichem, digitalen Signaturschlüssels). (Je nach Erfordernis des elektronischen Geschäftsgangs und des bearbeiteten Schriftguts kann ein unterschiedlich starker Beleg der Authentizität der Zeichnung durch das System bzw. angebundene Komponenten erforderlich sein.)	Integrität, Transparenz
FA-016	Formatwandlung	Dokumente müssen mit der Schlusszeichnung durch das System automatisch in ein unveränderbares Format (bspw. PDF/A) übertragbar sein. (Das diesbezügliche Verhalten sollte systemweit konfigurierbar sein.)	Integrität

Nr.	Bezeichnung	Beschreibung	Schutzziele
FA-017	VPS	Das System muss die Verwendung eines geeigneten Nachrichtenübermittlungs- und Zustelldienstes (VPS, EGVP oder De-Mail) zur rechtsverbindlichen Kommunikation mit Externen unterstützen.	Vertraulichkeit, Integrität, Transparenz
FA-018	Links auf Dokumente	Das System muss die Anlage und den Versand von Links auf elektronische Schriftgutobjekte unterstützen. (Dies kann die Auswirkungen von Fehlleitungen minimieren, da vergebene Objektrechte auf diese Weise wirksam bleiben.)	Vertraulichkeit
FA-019	Fristengesteuerte Workflows	Das System muss die Möglichkeit fristgesteuerter Workflows bieten (bspw. für Transfer- und Aufbewahrungsfristen). (Die Funktionalität kann entscheidend dazu beitragen, dass Schriftgutobjekte mit personenbezogenen Informationen nicht länger als erforderlich im System gespeichert bleiben.)	Verfügbarkeit
FA-020	Verschlüsselung	Das System muss die verschlüsselte Speicherung vertraulicher Dokumente unterstützen, um diese vor unberechtigtem Zugriff zu schützen.	Vertraulichkeit
FA-021	Abgabe an das Archiv	Das System muss gewährleisten, dass die elektronisch verschlüsselten Dokumente mit Angabe des Verfassers und des Datums im Klartext lesbar an die Archivbehörde übergeben werden können.	Verfügbarkeit
FA-022	Berechtigungen für Aussonderung und Löschung	Um Schriftgut auszusondern und löschen zu können, muss es möglich sein, Benutzer- bzw. Rollenberechtigungen explizit zu vergeben	Integrität
FA-023	Berechtigung für (übergreifende) Suche	Die Berechtigung für Suchen über Aktenbestände muss als Benutzer- bzw. Rollenberechtigung explizit vergeben werden können.	Vertraulichkeit, Unverkettbarkeit
FA-024	Objektrechte	Die Vergabe von Berechtigungen im Sinne von Objektrechten muss für Schriftgutobjekte differenziert nach Erstellen, Lesen, Suchen, Ändern und Löschen möglich sein.	Vertraulichkeit, Unverkettbarkeit
FA-025	Vorbelegung von Objektrechten und Metadaten im Aktenplan	Es muss möglich sein, für einzelne Bereiche des Aktenplans Standard-Objektrechte und Werte für Metadatenfelder (insbesondere Aufbewahrungsfrist, Bewertung des Archivs etc.) vorzubelegen.	Vertraulichkeit
FA-026	Sicherheitsfreigaben auf Objektebene	Das System muss die Vergabe von Vertraulichkeitsstufen für Schriftgutobjekte durch den Bearbeiter im elektronischen Geschäftsgang unterstützen. (Vertraulichkeitsstufen regeln die Berechtigung für den Zugriff auf elektronisches Schriftgut auf Objektebene.)	Vertraulichkeit

Nr.	Bezeichnung	Beschreibung	Schutzziele
FA-027	Stellvertretung	Das System muss die Möglichkeit der Stellvertretung für definierte Vertreter und Zeiträume unterstützen. Dabei muss der Vertreter Zugang zu den Daten des zu Vertretenden sowie dessen Bearbeitungsrechte erhalten. Aktivitäten in Stellvertretung sind entsprechend zu protokollieren (siehe FA-11).	Integrität, Verfügbarkeit
FA-028	Unveränderbarkeit von Protokoll- und Zeichnungsinformationen	Zeichnungsinformationen (wie Zeichnungsart, Mitzeichnungs- und Schlusszeichnungsvermerke, Zeichnungsdatum) müssen im System unveränderbar mit genau derjenigen Version des Primärdokuments verknüpft sein, die Gegenstand der Zeichnung war. Protokollinformationen müssen im System unveränderbar mit den entsprechenden Schriftgutobjekten verknüpft sein.	Integrität, Verfügbarkeit
FA-029	Protokollierung fachadministrativer Änderungen	Das System muss Änderungen der Berechtigungsprofile, der Zuordnung von Benutzern zu Berechtigungsprofilen und der Anmeldung von Benutzern mit fachadministrativen Rechten protokollieren.	Vertraulichkeit, Integrität
FA-030	Authentisierung	Das System muss die Anbindung an Verzeichnisdienste und eine zentrale Verwaltung von Benutzern, Rollen und Berechtigungsprofilen unterstützen (Zugangs- und Zugriffskontrolle).	Integrität
FA-031	Zugriff auf Metadaten	Das System muss eine Rechtevergabe für den lesenden bzw. schreibenden Zugriff auf einzelne Metadatenfelder auf Feldebene ermöglichen.	Vertraulichkeit, Verfügbarkeit
FA-032	Schwärzen/ Unkenntlichmachen	Das Schwärzen (Unkenntlichmachen)[132] von personenbezogenen Informationen im elektronischen Dokument muss möglich sein.	Vertraulichkeit

Tabelle 5: Funktionale Anforderungen an ein E-Akte-System mit den jeweils zu erreichenden Schutzzielen

[132] Hinweis: Das digitale Schwärzen/Unkenntlichmachen personenbezogener Daten in elektronischen Dokumenten ist fehlerträchtig, da bei unsachgemäßer Anwendung die vermeintlich unkenntlich gemachten Passagen im elektronischen Dokument wiederherstellbar sind. Das kann zu einer Verletzung des Schutzbedarfs vertraulicher Informationen führen. Hier bedarf es jedenfalls einer entsprechenden Richtlinie für die Bediensteten und ggf. des Einsatzes einer zusätzlichen Software-Komponente.

4 Besonderheiten bei der Einführung elektronischer Personalakten (eP-Akten)

Bei Personalakten handelt es sich um Akten, die in der Regel deutlich längere Laufzeiten im Vergleich zur Mehrzahl der Sachakten haben. Die sichernden Maßnahmen müssen – insbesondere mit Blick auf die Sensibilität der Daten – einen lückenlosen Schutz über Zeiträume von häufig mehreren Jahrzehnten gewährleisten. Des Weiteren sind – über die verschiedenen personalaktenrelevanten Vorgänge (Besoldung, Versorgung, Beurteilung, Beförderung, Aus- und Fortbildung, Gesundheit, ggf. Disziplinarmaßnahmen u. a. m.) hinweg betrachtet – zahlreiche mitwirkende Stellen involviert. Hierbei ist auf die Zuweisung und Verwaltung von geeigneten Zugriffsrechten zu achten.[133]

Die (vollständig) elektronische Personalaktenführung kann zahlreiche Funktionalitäten gewährleisten, insbesondere:

- automatisierte Fristenüberwachung,
- automatisierte Überprüfung von Vollständigkeit und Form,
- systemintegrierter Zugriffsschutz durch hinterlegte Rollen und Berechtigungen zur Vermeidung unberechtigter Zugriffe,
- raum- und zeitunabhängiger Zugriff.

Darüber ermöglicht eine Digitalisierung von Personalakten zusätzliche Effizienz- und Qualitätssteigerungseffekte. Insbesondere verkürzen sie Bereitstellungs- und somit der Gesamtbearbeitungszeiten.

Für elektronische Personalakten (**eP-Akten**) sind neben den allgemeinen datenschutzrechtlichen Regelungen des BDSG vor allem die Regelungen des BBG (hier insbesondere §§ 106 ff.) und BPersVG (v.a. dessen § 68 Abs. 2 S. 3) relevant.[134] Für die Landesverwaltungen sind zudem noch das BeamtStG, die Landesbeamtengesetze sowie die Landespersonalvertretungsgesetze zu beachten. Im Bereich der Tarifbeschäftigten ist § 3 Abs. 5 TVöD zu berücksichtigen.[135]

Entscheidungen mit rechtlicher oder vergleichbarer Wirkung, die ausschließlich auf einer automatisierten Verarbeitung von Personalaktendaten beruhen, erklärt Art. 22 Abs. 1 DSGVO für grundsätzlich unzulässig. Dies gilt aber nicht vorbehaltlos, sondern nur so lange, wie gesetzlich nichts anderes bestimmt ist (Art. 22 Abs. 1 DSGVO Art. 22 Abs. 2 lit. b DSGVO)). Das betrifft selbstverständlich auch bzw. gerade beamtenrechtliche Entscheidungen (§ 114 Abs. 4 BBG). Personalaktendaten darf die aktenführende Stelle daneben nur für Zwecke der Personalverwaltung oder der Personalwirtschaft automatisiert verarbeiten (vgl. § 114 Abs. 1 S. 1 BBG).

Andere Behörden dürfen Personalaktendaten nur automatisiert abrufen, soweit eine spezielle Rechtsvorschrift dies gestattet.

---

[133] Die Ausführungen dieses Kapitels nehmen Bezug auf das im Baustein „Projektleitfaden“ in Kapitel 4 beschriebene Phasenmodell zur Einführung der elektronischen Verwaltungsarbeit, http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/projektleitfaden.pdf?__blob=publicationFile&v=1. Die Planung der datenschutzrechtlichen Maßnahmen erfolgt nach diesem Modell in den Intervallen „Voruntersuchung“ und „Hauptuntersuchung“, ihre Umsetzung entsprechend in den nachfolgenden Phasen. Eine Zuordnung der datenschutzrechtlichen Aktivitäten zum genannten Phasenmodell findet sich im Anhang, Kapitel 5.2.

[134] Für Soldaten ist zudem § 29 SG i. V. m. der SPersAV und BPersVG relevant.

[135] Die (datenschutz-)rechtlichen Grundlagen beschreibt Kapitel 2.

Neben den Besonderheiten der Personalaktenführung sind bei der Einführung einer eP-Akte auch die allgemeinen Grundsätze zur Einführung einer elektronischen Akte zu beachten. Daher sollte auch hier der Projektleitfaden des Organisationskonzepts „Elektronische Verwaltungsarbeit“ Berücksichtigung finden. Dieser gibt einen ganzheitlichen Überblick auf die organisatorischen Fragestellungen und Probleme.[136]

4.1 Projektinitialisierung

Die Projektinitialisierungsphase unterscheidet sich in ihren Aufgaben der Zieldefinition und Konkretisierung des Projektauftrags sowie der groben Projektplanung nicht von Projekten zur Einführung allgemeiner elektronischer Verwaltungsakten. Grundlegend ist auch bei der Einführung der eP-Akte die Entscheidung, ob, wann und für welche (Teil-)Prozesse sich eine elektronische Vorgangsbearbeitung für eine elektronische Akte anbietet. Daraus ergeben sich die konkreten r vorzubereitenden Maßnahmen sowie deren zeitliche Abfolge.

4.2 Voruntersuchung und Datenschutz-Folgenabschätzung

Die Phase der Voruntersuchung dient dazu, das Vorhaben mit Blick auf seine Zielstellung, die Ausprägung des Prinzips der eP-Aktenführung (etwa hinsichtlich der Anbindung von Fachverfahren) sowie bzgl. der Einführungsstrategie zu konkretisieren.

In dieser Phase erfolgt außerdem die Prüfung der geltenden gesetzlichen und datenschutzrechtlichen Regelungen für das Vorhaben (Rechtsgrundlage der Datenverarbeitung) im Zuge der Datenschutz-Folgenabschätzung. Die Voruntersuchung entspricht praeter propter der Vorbereitungsphase der Folgenabschätzung.[137]

Bevor die Verwaltung die eP-Akte eingeführt, ist eine Datenschutz-Folgenabschätzung grundsätzlich zwingend (Art. 35 Abs. 1 lit. b DSGVO). Denn Personalakten können besonders sensible Daten enthalten, darunter auch besondere Arten personenbezogener Daten (nach Art. 9 Abs. 1 DSGVO bzw. § 22 BDSG; vgl. auch Art. 30 Abs. 1 lit. c DSGVO), etwa Gesundheitsdaten.[138] Die Einführung der eP-Akte weist damit insgesamt ein hohes Risiko für das informationelle Selbstbestimmungsrecht betroffener Personen auf.

4.3 Weitere fachliche Beteiligungen

Die eP-Akte nimmt Fakten und Daten auf, die insbesondere auch über das Verhalten des Beschäftigten Aufschluss geben.[139] Die Umstellung von der Papier- auf die eP-Akte fällt zwar nicht unmittelbar unter einen der Tatbestände des § 75 Abs. 3 BPersVG – auch nicht unter Abs. 3 Nr. 17. Denn sie dient nicht dazu,

[136] Organisationskonzept „Elektronische Verwaltungsarbeit“ – Projektleitfaden, S. 6.

[137] Dazu Kapitel 3.1.

[138] Dies gilt u. U. dann ausnahmsweise nicht, wenn bereits der Gesetzgeber eine Datenschutz-Folgenabschätzung im Rahmen der allgemeinen Gesetzesfolgenabschätzung bei der Schaffung gesetzlicher Regelungen zur eP-Akte durchgeführt hat.

[139] Vgl. hierzu BVerwG, NJW 1989, 848 (849).

technische Einrichtungen anzuwenden, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen. Sie kann *in ihrer praktischen Wirkung* aber womöglich geeignet sein, „Fakten oder Daten, denen Bedeutung für die zu überwachende Leistung oder das zu überwachende Verhalten der Beschäftigten zukommt, aufzunehmen, zu übermitteln, zu verarbeiten oder auszuwerten".[140] Nicht zuletzt löst eine elektronische Aktenführung ein spezifisches Gefährdungspotenzial für das informationelle Selbstbestimmungsrecht der betroffenen Beschäftigten aus. Bei der Entscheidung, eine eP-Akte einzuführen, ist es daher mindestens empfehlenswert, den Personalrat zu beteiligen. Um den Betriebsfrieden zu fahren, ist es insbesondere ratsam, im Zuge der Einführung der eP-Akte eine Dienstvereinbarung zu schließen. Diese könnte dem Personalrat Kontrollrechte einräumen, um insbesondere die Integrität der Datenverarbeitung zu sichern.

Dem einzelnen Beschäftigten steht aber kein Widerspruchsrecht gegen die Umstellung von der Papier- zur eP-Akte zu.[141]

Es bedarf darüber hinaus der Klärung, welche internen Festlegungen und Vereinbarungen über die gesetzlichen Vorschriften hinaus bereits existieren. Zudem sollte eindeutig sein, welche betroffenen Bereiche – in der Regel nur temporär – Auskünfte über die Arbeitsabläufe und Prozessanforderungen geben können. Nur so erhalten die Mitglieder der Projektgruppe den unverzichtbaren fachlichen Input aus den operativen Bereichen. Dies können u. a. sein:

- Personalverwaltende Behördenbereiche für grundsätzliche Fragen der Aufbau- und der Ablauforganisation bzw. dienstvorgesetzte Behördenbereiche (falls abweichend von der personalverwaltenden Behörde) für Fragen der Abgrenzungen von Grund-, Teil- und Nebenakten sowie zu den entsprechenden Zugriffsberechtigungen;

  Personalnebenakten können geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für den Beamten zuständig sind.[142]
- die Personalvertretung, z. B. um zu konkretisieren, wie das Verfahren bei einer Einsichtnahme in das Projekt erfolgen soll; ein solches Prozedere kann die Zustimmung und Unterstützung eines Beschäftigten nach § 69 Abs. 2 BPersVG vorsehen.
- die Personalverwaltung (hauptakten-, teilakten- und nebenaktenführende Stelle), damit diese die operativen und ergonomischen Anforderungen darstellen;
- ggf. weitere Interessensvertretungen
- der Gleichstellungsbeauftragte;
- der Datenschutzbeauftragte;

[140] BVerwG, NJW 1989, 848 (849). Für eine Mitbestimmungspflicht plädierend: *Hitzelberger-Kijima*, Die elektronische Personalakte, öAT 2016, 87 (87 f.).

[141] Anderes kann sich aus besonderen persönlichen Gründen des Beschäftigten ergeben, sodass im Einzelfall ein Widerspruchsrecht aus Art. 21 Abs. 1 DSGVO in Betracht kommt.

[142] Nebenakten enthalten ausschließlich Unterlagen, die sich bereits in der Grundakte oder einer Teilakte befinden. Das bedeutet, dass Kopien aus einer Grund- oder Teilakte als Nebenakte angelegt werden. Die Führung von Nebenakten setzt voraus, dass die Personalverwaltung ohne Führung von Nebenakten nicht reibungslos funktionsfähig ist. Sobald die Notwendigkeit nicht mehr besteht, die Nebenakte zu führen, ist diese aufzulösen bzw. zu vernichten.

- die Innenrevision;
- Besoldungs- bzw. Versorgungsstellen;
- Zuständige für (amts-)ärztliche Unterlagen;
- der IT-Betrieb.

4.4 Erstellung eines Anforderungskatalogs

Der Anforderungskatalog, welcher auf den Analyseergebnissen aufbaut, sollte u. a.:

- die erforderliche Aktenstruktur (inkl. der jeweiligen Zugriffsberechtigungen) beschreiben. Diese ist bei Personalakten detailliert geregelt und enthält meist die folgenden Teilakten oder Registerbereiche:
  - Verwendungs- und Laufbahnvorgänge,
  - Beurteilungen,
  - Urlaub, Arbeits- und Dienstbefreiung,
  - Aus- und Fortbildung,
  - Krankheit / Gesundheit,
  - Besoldung,
  - Versorgung,
  - Disziplinarvorgänge,
  - Beihilfe / Heilfürsorge,
  - Nebentätigkeiten,
  - Dienstunfälle;
- die vorkommenden Dokumenttypen mit ihren jeweiligen rechtlichen Vorgaben (Beweiswert, Fristen etc.) benennen;
- die Soll-Geschäftsprozesse mit ihren besonderen Anforderungen darstellen, z. B.:
  - die gesonderte Posteingangsbehandlung (bspw. bei personalaktenrelevanten Dokumenten: ungeöffnetes Weiterleiten aus der zentralen Poststelle und Nachscannen im Personalreferat),
  - die erforderlichen Recherchen und die dafür benötigten Such-Parameter (Primärdaten, Metadaten) sowie die für den Personalaktenbestand geltenden Beschränkungen,
  - Maßnahmen zur Erhaltung des Beweiswertes beim Einscannen von Papierdokumenten,[143]
  - die Einsichtnahme durch die Betroffenen;
- besondere Anforderungen an die Protokollierung von Löschungen bzw. ggf. an die Vermeidung der Protokollierung für bestimmte Teilakten (wie bspw. Disziplinarangelegenheiten[144]) der eP-Akte behandeln;

[143] Siehe Baustein „Scanprozess“ des Organisationskonzeptes „Elektronische Verwaltungsarbeit“, http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/scanprozess.html.

- weitere besondere Anforderungen an die Protokollierung (bspw. Protokollierung lesender Zugriffe für bestimmte Dokumente bzw. Teilakten) definieren;[145]
- die Anbindung an bestehende Fachverfahren für die Verwaltung von Personaldaten gewährleisten.

4.5 Einführungsstrategie

Bei der Wahl der Einführungsstrategie sind insbesondere folgende Rahmenbedingungen zu beachten:

- der Grundsatz der Einheit und Eindeutigkeit der Personalakte,
- das Gebot der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO),
- das Gebot der Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO),
- das Gebot der Speicherbegrenzung: Personenbezogene Daten sind in einer Form zu speichern, welche die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist (Art. 5 Abs. 1 lit. e DSGVO).

Dem Gebot der Datenminimierung widerstreitet es grundsätzlich, neben der eP-Akte Vorgänge parallel in Papierform zu führen (vgl. Kapitel 2.13.14). Denn die doppelte Datenhaltung in verschiedenen Medien ist in der Regel nicht erforderlich. Sie erhöht die Gefahr unzulässiger Datenzugriffe. Gerade im Anwendungsbereich des Personalaktengeheimnisses, welches besonders sensible und daher auch besonders schutzwürdige Daten gegen unberechtigte Kenntnisnahme absichern soll, gilt es, dieser Gefahr frühzeitig wirksam zu begegnen. Für die Überführung in die eP-Aktenführung ermöglicht das Gesetz jedoch eine sukzessive Umstellung. Denn es lässt zu, die Akten ggf. auch nur teilweise in Papierform weiterzuführen (§ 106 Abs. 1 S. 3, Abs. 2 S. 5 BBG; vgl. auch die landesrechtlichen Regelungen, etwa Art. 104 Abs. 1 S. 5 BayBG, § 85 Abs. 3 BremBG, § 85 Abs. 3 S. 3 HmbBG, § 88 Abs. 3 S. 4 NBG, § 85 Abs. 3 S. 3 LBG Schl-H). Voraussetzung solcher **Hybridakten** ist allerdings, dass (der Normgeber oder) der Verantwortliche vorher eindeutig festlegt, welche Teile er in welcher Art führt. Es geht nämlich zu verhindern, dass Aktenteile parallel in beiden Formen vorhanden sind, ohne dass das erforderlich ist. Begrifflich wird also eine Personalakte im materiell-rechtlichen Sinne gemischt (teils in Papierform, teils elektronisch) geführt. Die hybride Struktur darf weder Zweifel an der Eindeutigkeit der Personalakte auslösen noch Rechte der betroffenen Beschäftigten einschränken. Aus zwingenden technischen Gründen als Sicherheitskopien und Back-ups abgelegte Versionen verstoßen nicht gegen den Grundsatz der Einheitlichkeit und Eindeutigkeit. Denn sie sind Teil des unionsrechtlich verankerten Gebots, die Verfügbarkeit der personenbezogenen Daten bei einem Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DSGVO).

[144] Wenn es sich bei den gelöschten Unterlagen um bspw. Beschwerden oder Behauptungen handelte, die sich als unbegründet oder falsch erwiesen haben – vgl. § 112 Abs. 1 BBG –, besteht ein berechtigtes Interesse des Betroffenen, dass auch der Protokolleintrag über die Löschung entfernt wird, da dieser den tatsächlichen Sachverhalt in der Regel nicht abbildet.

[145] Grundlage sollte hier das in Anhang 0 aufgeführte verfahrensspezifische Protokollierungskonzept sein.

Wenn bestehende Papierakten vollständig in eine elektronische Form überführt werden, sind die Papierakten nicht mehr erforderlich im Sinne des Gesetzes und dürfen nicht weiter aufbewahrt werden.

4.6 Wirtschaftlichkeitsbetrachtung

Für alle finanzwirksamen Maßnahmen sind angemessene Wirtschaftlichkeitsuntersuchungen durchzuführen (§ 7 BHO).[146] Bei einer Wirtschaftlichkeitsbetrachtung sind neben den monetären Kriterien, wie z. B. der Arbeitszeitersparnis durch die hohe Verfügbarkeit, insbesondere folgende Kriterien zu berücksichtigen:

- die Dringlichkeit, das Altsystem abzulösen,[147]

  Hierbei sind die Vorgaben des E-Government-Gesetzes zu berücksichtigen.[148]

- der „qualitativ-strategische Nutzen“,

  Bei Personalakten liegt dieser mit Blick auf die hohen datenschutzrechtlichen Anforderungen i. V. m. der großen Anzahl der gleichartigen Akten in diesem Bereich in der Möglichkeit, das Effizienzpotenzial erheblich zu steigern und IT-gestützt standardisiert zu arbeiten.

- „externe Effekte“.

  Im Bereich der Personalakten sind diese zwar naturgemäß eher gering, da es für Personalakten nur in sehr eng definierten Geschäftsfällen eine Weitergabe nach außen geben darf. Dennoch sind folgende Szenarien als „extern“ aus der Sicht der Personalaktenverwaltung zu betrachten:

  - die Einsichtnahme von Beschäftigten oder deren Bevollmächtigten in die eigene Personalakte sowie
  - die Bereitstellung von Personalakten oder Teilen von diesen im Rahmen von behördenübergreifenden Bewerbungen oder Abordnungen.

Um Personalakten im Zuge der Einführung der eP-Akte einzuscannen, kann es wirtschaftlich sinnvoll sein, private Dienstleister zu beauftragen. Zwar stellt § 107 BBG für den Zugang Dritter zur Personalakte sehr hohe Anforderungen: Aufgrund der besonderen Sensibilität der Daten dürfen nur bestimmte Personen Zugang zu den Personalakten haben.[149] Auf Grundlage der Öffnungsklausel des Art. 88 Abs. 1 DSGVO hat der Bundesgesetzgeber für die Auftragsdatenverarbei-

[146] Eine methodische und inhaltliche Handreichung bietet insoweit die „Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT“. Abrufbar auf der Seite der CIO Bund, http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/Wirtschaftlichkeitsbetrachtungen/wirtschaftlichkeitsbetrachtungen_node.html.

[147] In diesem Sinne ist auch eine papierbasierte Personalaktenregistratur als Altsystem zu verstehen.

[148] Zum Vorbehalt der Wirtschaftlichkeit und der Soll-Vorschrift für bestimmte Teilbereiche von besonderer Komplexität bzw. mit besonderem Schutzbedarf (wie bspw. Personalakten oder Verschlusssachen) siehe § 6 EGovG.

[149] Namentlich „Beschäftigte […], „die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten betraut sind“ (§ 107 Abs. 1 S. 1 BBG) sowie in engen Grenzen im Rahmen ihrer spezifischen Aufgaben „Beschäftigte, die Aufgaben des ärztlichen Dienstes wahrnehmen“ (Abs. 1 S. 2), Gleichstellungsbeauftragte (Abs. 1 S. 3), ferner die Beauftragten für den Datenschutz (Abs. 2 S. 1) und „mit Angelegenheiten der Innenrevision beauftragte Beschäftigte“ (Abs. 2 S. 2). Ob auch Auftragsverarbeiter als Verwaltungshelfer „Beschäftigte“ im Sinne des Abs. 1 S. 1 sind, lässt sich dem Gesetz nicht zweifelsfrei entnehmen. Der Katalog von Zugriffsberechtigten macht zugleich aber deutlich, dass der Gesetzgeber den Zugriff auf die Personalakte bewusst einem sehr kleinen Kreis von Personen vorbehalten will. Als spezialgesetzliche Einschränkung steht er nicht für eine Erweiterung auf Personen offen, die nicht den besonderen persönlichen Voraussetzungen entsprechen, welche das Gesetz nennt: Beschränkt der Gesetzgeber den Katalog auf einen kleinen Kreis unter denjenigen, die kraft ihrer Funktion auf Amtsverschwiegenheit verpflichtet sind, schließt er sonstige Personen implizit aus – erst recht solche, die außerhalb der öffentlichen Verwaltung stehen.

tung im Bereich der Personalaktendaten aber in § 111a BBG eine spezielle gesetzliche Regelung getroffen, welche die Regelung des Art. 28 DSGVO spezifiziert.[150]

4.7 Hauptuntersuchung

Die Hauptuntersuchung klärt in einer umfassenden Ist-Analyse alle organisatorisch-fachlichen, organisatorisch-technischen sowie die rein technischen Fragen und Anforderungen.[151]

4.7.1 Ausführliche Ist-Analyse inkl. Schwachstellenanalyse

Die Gegenstände der Ist-Analyse sind vielfältig. Sie reichen von der Organisation der Schriftgutverwaltung (4.7.1.1.) bis hin zur Analyse der Gefährdungen, die von dem System ausgehen (4.7.1.5.).

4.7.1.1 Organisation der Schriftgutverwaltung

Großorganisationen Schriftgutverwaltung gehören insbesondere:

- die besondere Registratur der Personalverwaltung,
- besondere Schriftgutobjekte (z. B. Grund-, Teil-, Nebenakte),
- die Definition und Abgrenzung der Art der Aktenführung von Grund-, Teil- und Nebenakten – insbesondere der zulässigen Bestandteile der Nebenakte – bei ggf. bestehenden Nebenakten führenden Stellen
- Berechtigungen für den Aktenzugriff in der nebenaktenführenden Behörde[152]
- die Formierung der Akten (Teilaktenstruktur, Registerbildung, Inhaltsverzeichnis, Paginierung etc.)
- besondere Dokumententypen (z. B. „ärztlicher Umschlag“)

4.7.1.2 Allgemeiner Geschäftsgang

Als Teil des allgemeinen Geschäftsgangs kommt der Hauptuntersuchung insbesondere folgende Funktion zu:

- Identifizierung und Profilierung der Prozessbeteiligten und Betroffenen, namentlich
  - Beschäftigte und deren Angehörige (Versorgungsfälle), auf die sich die Personalakte bezieht
  - Mitglieder der Personalvertretung (mit Zustimmung des Beschäftigten) - § 69 Abs. 2 BPersVG
  - Leitungen der personalverwaltenden Behördenbereiche

[150] Vgl. dazu mit anderer Begründung (namentlich unter Rekurs auf Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO) BT-Drs. 18/3248, S. 31.

[151] Siehe dazu im Baustein „Projektleitfaden“, S. 37-39.

[152] Siehe Ausführungen zur Nebenakte in Kapitel 2.10.3.

- Leitungen der dienstvorgesetzten Behördenbereiche (ggf. abweichend von personalverwaltender Behörde),
- sachbearbeitende Stellen der Personalverwaltung (grund-, teil-, nebenaktenführende Stelle),
- sachbearbeitende Stellen - ggf. Leitungen - der Besoldungsstellen,
- (Amts-)ärztliche Beteiligte,
- Sonstige Berechtigte (etwa § 107 Abs. 1 S. 2 und Abs. 2 BBG).

- Spezifiziertes Rollen- und Berechtigungskonzept bezogen auf die einzelnen Schriftgutobjekte – aufgefächert in Recherchieren, Lesen, Bearbeiten (dies ggf. wiederum differenziert nach Bearbeitung, Verfügung und Ablage), Löschen.

4.7.1.3 Bearbeitung

Im Rahmen der Bearbeitung analysiert die Hauptuntersuchung insbesondere

- besondere Regeln für die Behandlung des Posteingangs (verschlossen Weiterleiten, Öffnen und Scannen durch Berechtigte, Aufbringen von Signaturen bei der Überführung in das elektronische System; weiterer Umgang mit den papiergebundenen Dokumenten),
- die Trennung der Aktenführung von den Workflows der Personalbewirtschaftung, die z. B. in Fachverfahren erfolgt,
- die persönliche Identifizierung gemäß dem Rollen- und Berechtigungskonzept für einzelne Zugriffe und/oder Bearbeitungen (über eine initiale Anmeldung am System hinaus),
- detaillierte Handlungsanweisungen und Verfahrensbeschreibungen
- die Unterbindung einer aktenübergreifenden Suche
- die elektronische Akteneinsicht durch Beamte oder Bevollmächtigte (§ 110 Abs. 1 BBG), Beschäftigte oder Bevollmächtigte (§ 3 Abs. 5 TVöD)

4.7.1.4 Postausgang

- Besondere Regeln für die Behandlung des Postausgangs (Versand, ggf. Ausdruck und Kuvertieren durch Berechtigte)

4.7.1.5 Termine, Wiedervorlagen

- Spezielle Beachtung von fristgesteuerten Löschungsgeboten (z. B. bei Disziplinarangelegenheiten oder bei Auskunft aus dem Bundeszentralregister)

4.7.1.6 Altregistratur

- Regelmäßig lange Aufbewahrungszeiten stellen Anforderungen an die langfristige Verfügbarkeit und Lesbarkeit der gespeicherten Informationen. Dies ist durch geeignete Maßnahmen zu gewährleisten (z. B. Formatumwandlung in PDF/A).
- Die Beweiswerterhaltung im Sinne der ZPO erlangt wegen ihrer besonderen Bedeutung für die Wahrung von Rechten (z. B. Pensions-, Renten- und Versorgungsansprüche) und aufgrund der langen Zeiträume, aus denen beweissichere Daten ggf. zur Verfügung stehen müssen, eine hohe Priorität. In diesem Kontext ist daher insbesondere beim ersetzenden

Scannen, bei der Datenhaltung sowie der Langzeitspeicherung[153] und Archivierung auf den Beweiswerterhalt zu achten.

4.7.1.7 Aussonderung, Entfernung, Löschung

- Löschungsgebot von Einzeldokumenten in der Akte: Die Personalaktenführung verlangt, bestimmte Dokumententypen (z. B. Erkrankungen) nach definierten Fristen zu löschen [154]. Darin unterscheidet sie sich von sonstigen Verwaltungsmaßnahmen, bei denen es prinzipiell nicht bzw. nur in einzelnen zu begründenden Ausnahmefällen möglich ist, einzelne Dokumente zu löschen.
  - Dabei darf die Berechtigung, Inhalte der eP-Akte zu löschen, nur einem sehr eingeschränkten Personenkreis zustehen (die Einführung organisatorischer Regelungen wie bspw. das Vier-Augen-Prinzip ist zu prüfen).
  - Auch bei einer Vereinbarung über ein automatisiertes Löschen sollte der Verantwortliche den Löschvorgang freigeben bzw. bestätigen.
  - In einer datenbankgestützten eP-Akte sind gelöschte Objekte in der Regel weiterhin als Dateien vorhanden, da lediglich der Indexeintrag bzw. die Referenz auf eine Datei gelöscht wird. Es ist daher zu prüfen, ob dieses Verfahren ausreicht oder ob es erforderlich ist, die elektronischen Dokumente vollständig zu löschen.
  - Auch über die Löschung ist Protokoll zu führen. Dieses sollte den löschenden Mitarbeiter identifizieren, das Löschungsdatum und die Uhrzeit enthalten und die Dokumentenart der gelöschten Datei nennen. Die Aufbewahrungsfrist des Protokolls ist zu vereinbaren.
- Beschreibung zu berücksichtigenden Rahmenbedingungen, um dem Bundesarchiv Personalakten anzubieten sowie evtl. bestehender Nebenakten auszusondern und zu löschen
- Synchronisierung relevanter Fristen zwischen Grund-, Teil- und Nebenakte
- Organisatorische Maßnahmen zur Löschung der Nebenakten bei Aussonderung (Abgabe an das zuständige Archiv) bzw. Löschung der Grundakten[155]

4.7.1.8 Spezifische Prozesse

- Bestehende IT zur Schriftgutverwaltung und zum Geschäftsgang (bspw. Einsatz von Personalmanagementsystemen)
- Bestehende Fachverfahren mit aktenrelevantem Output
- Bestehende Konzepte zu Datensicherung und zum Datenschutz
- Sperrung von Personalaktendaten und Dokumenten

[153] Vgl. Baustein „E-Langzeitspeicherung“ des Organisationskonzeptes „E-Verwaltung“.

[154] Besondere Aufbewahrungsfristen sind in § 113 Abs. 2 BBG festgelegt.

[155] Siehe dazu die „Informationen zur Aussonderung und Abgabe von Personalunterlagen der Bundesverwaltung“ des Bundesarchivs, https://www.bundesarchiv.de/imperia/md/content/bundesarchiv_de/fachinformation/infoblatt-pers.-akten_juni_2017___neu__+_besondere_biographie.pdf.

Aus der Ist-Analyse lässt sich eine Schwachstellenanalyse ableiten. Diese umfasst zum einen allgemeinere mögliche Defizite – etwa die unzureichende Verfügbarkeit (lange Akten-Beschaffungswege, Wartezeiten etc.), vermeidbare Bearbeitungsstationen oder die uneinheitliche Aktenformierung. Zum anderen ist sie insbesondere auf die vollständige Erfüllung der besonderen rechtlichen Anforderungen der Personalaktenführung ausgerichtet (vgl. Kapitel 2.10).

4.7.2 Erstellung eines Fachkonzepts

Die Konzeptionsphase berücksichtigt die erkannten besonderen Anforderungen der eP-Akte, indem sie diese im Hinblick auf die Schriftgutverwaltung und den Geschäftsgang spezifiziert und zudem die Sollprozesse selbst konkretisiert. Zu den zu beachtenden Aspekten gehören insbesondere:

- der spezifische Posteingangsprozess / Scanprozess,
- ein Rollen- und Berechtigungskonzept (ggf. Differenzierung nach Teilakten); die Regelung des Zugriffs auf die eP-Akte sowie einer Zugriffs- und Weitergabekontrolle,
- die Berücksichtigung besonderer Ermächtigungen / eines Aufgabenverteilungsplan,
- besondere Schriftgutobjekte („ärztlicher Umschlag“),
- die besondere Formierung der Akte,
- Besonderheiten der Altregistratur,
- Besonderheiten der Aussonderung, Entfernung, Löschung,
- die Anbindung von/an Fachverfahren.

Insbesondere die Nutzung von Fachverfahren ist unter dem Aspekt der Datenminimierung und Vermeidung von Datenredundanzen im Personalbereich problembeladen. Das betrifft vor allem das Verhältnis zwischen den dort geführten Beschäftigtendaten und den in einer Personalakte abgelegten Dokumenten.

Die Implikationen aus dem Fachkonzept, das den gesamten Personalakten verwaltenden Bereich organisatorisch beschreibt, münden in ein Sollkonzept. Aus diesem erwächst wiederum der Anforderungskatalog mit den funktionalen, technischen und allgemeinen Systemanforderungen an die künftige IT-Unterstützung.

4.7.3 Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung vor Einführung der eP-Akte erfolgt in mehreren Schritten und als übergreifender Prozess.[156]

Die meisten Aktivitäten fallen in die Phase der Hauptuntersuchung.

Zum Gegenstand der Voruntersuchung gehören:

- die Festlegung der Rechtsgrundlage und Zweck(e) der Datenverarbeitung.

Die Hauptuntersuchung umfasst wiederum die Bewertungsphase. Zu ihr gehören typischerweise[157]

[156] Siehe dazu Kapitel 3.1.

- die System- und Anwendungsbeschreibung,
- die Schutzbedarfseinstufung,
- eine Gefährdungs- und Risikoanalyse,
- ein Informationssicherheitskonzept (Definition von Maßnahmen) und
- die Beherrschung der Risiken (Bewertung und Umgang mit Restrisiken).

4.7.4 Schutzbedarfsanalyse

Der Schutzbedarf von Personalakten ist anhand der unter Kapitel 3.3 beschriebenen Methodik zu bestimmen.

Beispielhafte Schadensszenarien wirtschaftlicher und/oder gesellschaftlicher Art im Rahmen eines Bewerbungs- oder Beförderungsverfahrens sind:

- Der Zugriff auf ein Dokument ist zwar berechtigt. Zum Zeitpunkt des Zugriffs sind jedoch noch Informationen verfügbar, die bereits gelöscht sein müssten; z. B. Unterlagen zu disziplinarischen Maßnahmen.
- Der Zugriff auf eine Grund- oder Teilakte ist zwar berechtigt und die Dokumente sind auch noch gültiger Bestandteil der eP-Akte. Sie sind aber nicht der richtigen Teilakte zugeordnet.

Beispiele:

- Hinweise zu einem Betrieblichen Wiedereingliederungsmanagement (BEM), die klar auf eine länger als sechswöchige Krankheit schließen lassen, befinden sich in einer Teilakte, welche die Behörde im Rahmen eines Bewerbungsverfahrens einer externen Stelle zugänglich macht. Eigentlich sollten sich diese Informationen in einer separaten, nicht ohne Weiteres zugänglichen Krankenakte wiederfinden.
- Informationen zu gesundheitlich bedingten Abwesenheiten im Rahmen von Aus- und Fortbildungsmaßnahmen enthalten Anhaltspunkte zu den konkreten Erkrankungen („fehlende Teilnahme wegen Sucht-Rehabilitation“).

4.7.5 Analyse der Gefährdungen und Maßnahmen

Eine Liste der Gefährdungen nach IT-Grundschutz für die eP-Akte findet sich im Anhang in Kapitel 5.1.

4.8 Einführung des Systems

In die Phase der Einführung fallen die folgenden, hinsichtlich der eP-Akte relevanten, Aktivitäten:

- Umsetzung der Konfigurationskonzepte des E-Akte-Systems (jeweils unter Berücksichtigung der spezifischen Anforderungen der eP-Akte),
  - Rechte- und Rollenkonzept,
  - Protokollierungskonzept,

[157] Ein beispielhaftes Vorgehen bei der Umsetzung einer Datenschutz-Folgenabschätzung für die eP-Akte findet sich im Anhang in Kapitel 5.1.

  - weitere funktionale Anforderungen,
- Erstellung von Testkonzepten und Testplanung,
- Evaluierung der Testergebnisse, insbesondere hinsichtlich der Umsetzung der Schutzziele des Datenschutzes,
- Schulungsplanung (rollenbasiert) für die
  - Beschäftigten des Personalreferats,
  - Beschäftigten der Poststelle,
  - Registratoren,
  - Fachadministratoren,
- Prüfen und ggf. Erstellen der notwendigen organisatorischen Regelungen für die Arbeit mit der eP-Akte,
- Evaluierung der Umsetzung der getroffenen datenschutzrechtlichen Maßnahmen im Zuge der Pilotierung und ggf. auch Freigabe des Verfahrens, damit der Datenschutzbeauftragte dieses sachgerecht nutzen kann.

5 Anhang

5.1 Muster zur Datenschutz-Folgenabschätzung bei Einführung der elektronischen Personalakte

5.1.1 Vorbereitungsphase

- Rechtsgrundlage der Datenverarbeitung
  - Unterscheidung von Personaldaten (nach Art. 88 DSGVO, § 26 BDSG) und Personalaktendaten (nach § 106 BBG, § 29 SG bzw. § 50 BeamtStG)
  - Rechte des Betroffenen (Benachrichtigung, Auskunft, Sperrung, Löschung u. w.) aus Art. 13-18 sowie 21 DSGVO, §§ 35, 36 BDSG bzw. ergänzend (auf der Grundlage des Art. 88 DSGVO) §§ 109–112 BBG und § 29 SG (Anhörung, Einsicht, Vorlage, Entfernung von Unterlagen u. w.)
  - Weitere Regelungen für die Personalakte (§§ 107, 109, 113, 114 BBG)

- System- und Anwendungsbeschreibung
  - Darstellung der mit der eP-Akte zu bearbeitenden Geschäftsprozesse (Art, Dauer, Umfang, betroffene Datenkategorien, Zugriffsrechte, Transparenz für Betroffenen etc.),
  - Auflistung der einzusetzenden IT-Systeme (Server, Clients, Netze, Speichersysteme, Drucker, Scanner etc.),
  - Beschreibung der Schnittstellen zu anderen Geschäftsprozessen und IT-Systemen,
  - Auflistung beteiligter Institutionen und Unternehmen und deren Rolle bei der E-Akte-Einführung,
  - Netzplan,
  - Beschreibung der mit der Einführung der eP-Akte verfolgten Zwecke und Interessen (Erforderlichkeit),
  - Benennung der aus der Einführung der eP-Akte erwachsenden Risiken.

5.1.2 Bewertungsphase

- Schutzbedarfs- und Gefährdungsanalyse

  Die Einstufung des Schutzbedarfs der Daten, welche die eP-Akte erhebt und verarbeitet, richtet sich nach dem Ausmaß des Schadens, der den Betroffenen durch eine Verletzung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sowie Transparenz, Belastbarkeit, Unverkettbarkeit oder Intervenierbarkeit (im Sinne des BDSG) entstehen könnte (siehe dazu Kapitel 3.3.3).

Eine Schutzbedarfsanalyse für die eP-Akte ist für die einzelnen Teilaktenbereiche gesondert durchzuführen. Denn die enthaltenen Primärdokumente könnten ggf. unterschiedliche Einstufungen erfahren (bspw. Aus- und Fortbildung und Gesundheit/Krankheit).

Als Ergebnis einer generellen Schutzbedarfsanalyse für die eP-Akte ergibt sich folgende typisierende Einstufung:

- Die Primärdaten haben einen sehr hohen Schutzbedarf (insbesondere weil in einigen Teilakten Dokumente mit besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO, § 22 BDSG enthalten sind).
- Die Metadaten haben einen hohen Schutzbedarf.
- Die Protokolldaten haben einen hohen Schutzbedarf.

Die folgende Tabelle erfasst beispielhaft ausgewählte Gefährdungen (vgl. Kapitel 3.3.4) für ein eP-Aktensystem. Zudem zeigt sie auf, welche Schutzziele signifikant beeinträchtigt sein könnten, um technisch-organisatorische Gegenmaßnahmen ergreifen zu können:

Gefährdung	Vertr.	Integr.	Verfüg.	Trans.	Un-verk.	Inter-ven.	Be-lastb.
Verlust gespeicherter Daten			X	X			
Überlastung von Informationssystemen	X	X	X	X			X
Fehlfunktion von Geräten oder Systemen	X	X	X	X			x
Software-Konzeptionsfehler	X	X	X	X	x	X	X
Software-Schwachstellen oder –Fehler	X	X	X	X	x	X	X
Ausspähen von Informationen / Spionage	X						
Abhören	X						
Sorglosigkeit im Umgang mit Informationen	X	X		X	x		
Missbrauch von Berechtigungen	X	X	X		x		

Tabelle 6: Ausgewählte Gefährdungen für die eP-Akte

- Risikobewertung

  Das Risiko für die Objekte, die zum Verfahren gehörenden, bestimmt sich aus der Wahrscheinlichkeit eines Schadenseintritts und dem Ausmaß des potenziellen Schadens. Die Höhe des Schadens im Eintrittsfall ergibt wiederrum sich aus der Schutzbedarfseinstufung.

  Die Wahrscheinlichkeit dafür, dass ein Schaden eintritt, bestimmt sich insbesondere aus:

- dem Missbrauchsinteresse (d. h. dem Interesse Unbefugter, Daten zu missbrauchen: zu löschen, zu manipulieren, unbefugt zu nutzen):

  Ein hohes Missbrauchsinteresse liegt z. B. vor, wenn ein Missbrauch von Daten persönliche Bereicherungen ermöglicht, Maßnahmen gegenüber Straftätern verhindert, Konkurrenten massiv benachteiligt oder Entscheidungen von Entscheidungsträgern widerrechtlich und unsachgemäß beeinflussen könnte;
- dem Aufwand, der notwendig ist, um einen Schaden herbeizuführen;
- dem Risiko, bei einem Missbrauch entdeckt zu werden;
- der Verarbeitungshäufigkeit (Häufigkeit der Vorgänge, bei denen ein Missbrauch oder eine sonstige Beeinträchtigung möglich ist).

Als Hilfsmittel, um eine Risikoanalyse durchzuführen, bietet sich das Modul „Risikoanalyse“ des Umsetzungsrahmenwerks (UMRA) Notfallmanagement des BSI (Standard 100-4) zu nutzen.[158] Für Behörden, die bereits mit der IT-Grundschutz-Methodik arbeiten und möglichst direkt eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten, ist der neue BSI-Standard 200-3[159] eine geeignete Handreichung. Dieser enthält erstmals gebündelt alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes.

Eintrittswahrscheinlichkeit	
Unwahrscheinlich	alle 10 Jahre oder seltener
möglich	etwa einmal pro Jahr
wahrscheinlich	etwa einmal pro Monat
sehr wahrscheinlich	einmal pro Woche oder öfter

Das Risiko der jeweiligen Gefährdung für die Daten und Objekte der elektronischen Schriftgutverwaltung lässt sich nach der folgenden Formel ermitteln:

Risiko = Schutzbedarf x Eintrittswahrscheinlichkeit

5.1.3 Maßnahmenphase

- Informationssicherheitskonzept (siehe dazu im Einzelnen das zugehörige Informationssicherheitskonzept nach dem IT-Grundschutzstandard):

  Das Informationssicherheitskonzept muss Maßnahmen definieren, welche die Eintrittswahrscheinlichkeit der aufgelisteten Risiken oder das Schadensausmaß bei deren Eintritt reduzieren.

[158] Siehe unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html.

[159] Der BSI-Standard 200-3 löst den Standard 100-3 ab und ist abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf?__blob=publicationFile&v=5.

- Einleitung geeigneter Maßnahmen zum Schutz der Rechte und Freiheiten betroffener Personen:

  Fördert die Vorbereitungs- und Bewertungsphase ein hohes Risiko zu Tage, sind technische und organisatorische Maßnahmen zu ergreifen, um das Risiko auf ein vertretbares Maß zu begrenzen.

- Beherrschung der Risiken:

  Die datenschutzrechtliche Wirksamkeit der laut Informationssicherheitskonzept getroffenen Abhilfemaßnahmen ist einzuschätzen und die verbleibenden Restrisiken sind zu bewerten.

- Bericht:

  Das Ergebnis der Analyse und ergriffene technische und organisatorische Maßnahmen zur Minimierung des Risikos sind zu dokumentieren und ggf. den zuständigen Aufsichtsbehörden zur Verfügung zu stellen. Letzteres ist Teil der Rechenschaftspflicht, die Art. 5 Abs. 2 DSGVO formuliert.

5.2 Einordnung in das Phasenmodell zur Einführung der elektronischen Verwaltungsarbeit

Die folgende Übersicht setzt die einzelnen Phasen und Aktivitäten des Planungs- und Umsetzungsprozesses der datenschutzrechtlichen Maßnahmen[160] in Relation zum Phasenmodell zur Einführung der elektronischen Verwaltungsarbeit.

Für die Datenschutz-Folgenabschätzung als übergreifender Prozess wurden stellvertretend der Start- und Endpunkt im Phasenmodell markiert. Aktivitäten der Folgenabschätzung finden aber insbesondere auch in der Phase „Hauptuntersuchung“ im Rahmen der Ist-Analyse und Sollkonzeption statt.

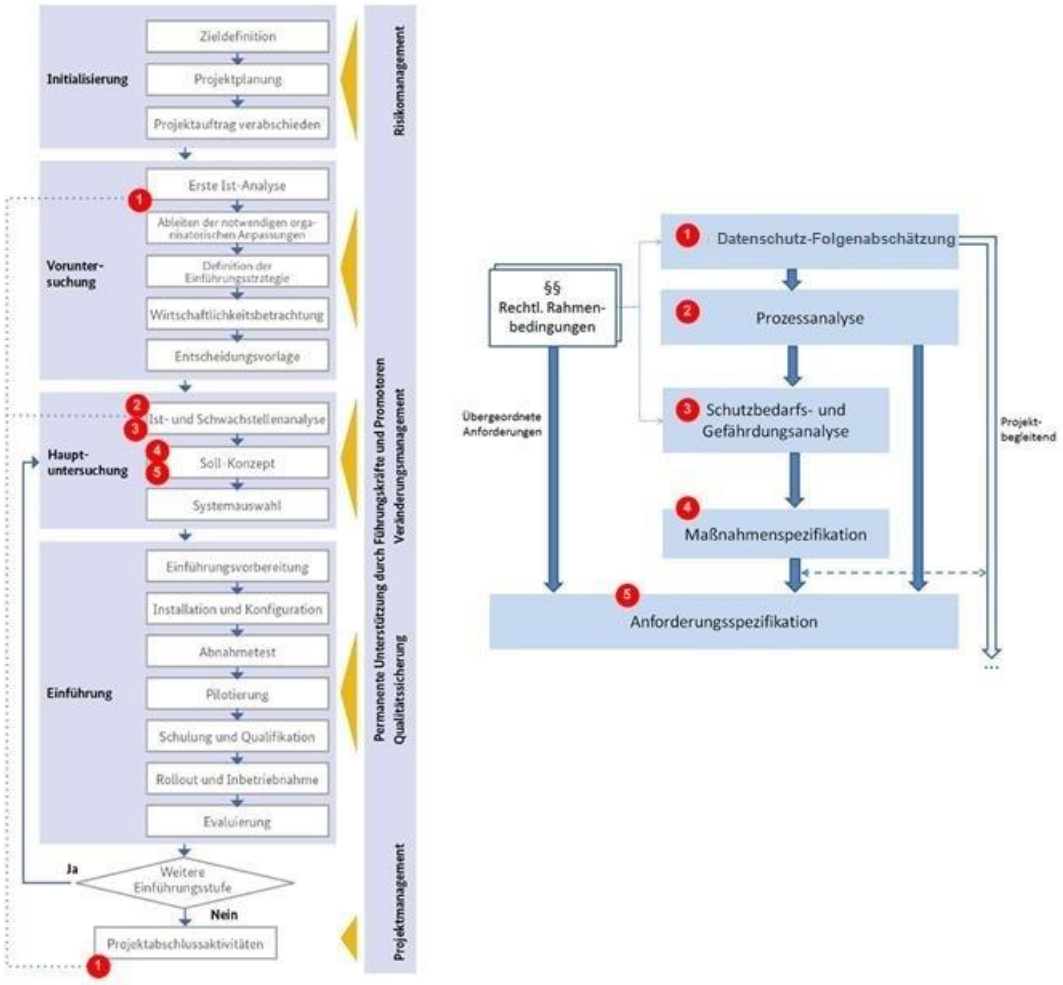

Abbildung 12: Planung und Umsetzung von Datenschutzmaßnahmen in Einführungsprojekten

[160] Siehe Kapitel 3.

5.3 Checkliste „Vollständigkeitsprüfung der erstellten Dokumente“

Nr.	Bezeichnung	Beschreibung
K-01	Fachkonzept/Organisationskonzept	Dokumentation der Prozesse und der Organisationsstruktur sowie der funktionalen und nichtfunktionalen Anforderungen als Ergebnis der Ist-Analyse und Soll-Konzeption; Entwurf/Beschreibung der Zielsystemarchitektur
K-02	Ergebnisbericht Datenschutz-Folgenabschätzung	Dokumentation des Ergebnisses der Prüfung der Rechtsgrundlage, der Zwecke und des Umfangs der Datenverarbeitung sowie deren Notwendigkeit und Verhältnismäßigkeit
K-03	Verfahrensspezifisches Datenschutz- und Datensicherheitskonzept	Schutzbedarfsfeststellung; verantwortliche Stelle; Beschreibung der technisch-organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes
K-04	Rollen- und Rechtekonzept	Beschreibung der organisations- und rollenbezogenen Zugriffsrechte auf die zu verarbeitenden Informationen; Beschreibung der standardmäßig eingeschränkten Objektrechte für bestimmte Aktenplanbereiche
K-05	Protokollierungskonzept	Beschreibung von Art und Umfang der verfahrensspezifischen Protokollierung
K-06	Verfahrensspezifisches Betriebskonzept	Konzept, in dem die Betriebsinfrastruktur und die entsprechenden Prozesse des IT-Managements zur Störungsbeseitigung, Änderungen von Komponenten, Einspielen neuer Releases, Datensicherung etc. beschrieben sind
K-07	Übersicht der geltenden organisatorischen Regelungen	Übersicht über die getroffenen Dienstvereinbarungen und -anweisungen, welche die organisatorischen Regelungsbedarfe, wie bspw. Zweckbindung der Protokollierung, Posteingangsbehandlung etc.,, Umsetzen
K-08	Wirtschaftlichkeitsbetrachtung	Sofern die eP-Akte als gesondertes Projekt realisiert wird, sind Wirtschaftlichkeitsbetrachtungen zu den einzelnen Phasen der Einführung zu erstellen (siehe Kapitel 4.6).

Tabelle 7: Wichtige Dokumente für Planung und Umsetzung des Datenschutzes

5.4 Vorlage „Datenschutzkonzept“

Die nachfolgende Vorlage orientiert sich am Baustein M 2.503 „Aspekte eines Datenschutzkonzeptes“ des BSI[161] und kann als Grundlage für die Struktur eines Datenschutzkonzepts dienen.

Inhaltsverzeichnis

[161] Siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02503.html.

5.5 Checkliste „Prüffragen zu den Datenschutzmaßnahmen“

Maßnahme	Prüffragen
Prüfung rechtlicher Rahmenbedingungen und Datenschutz-Folgenabschätzung bei der Verarbeitung personenbezogener Daten	• Erfolgt vor der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eine Prüfung, ob dies erforderlich und rechtlich zulässig ist? • Sind bei allen Geschäftsprozessen und Verfahren personenbezogene Daten angemessen geschützt?
Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten (siehe Kapitel 3.4.1.3)	• Werden alle Mitarbeiter auf das Datengeheimnis verpflichtet bzw. darüber unterrichtet, sobald sie ihre Tätigkeit aufnehmen? • Werden die Mitarbeiter regelmäßig für die Belange des Datenschutzes sensibilisiert?
Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten	• Ist bei der Einrichtung von Abrufverfahren eine Kontrolle vorgesehen, um sicherzustellen dass alle datenschutzrechtlichen Rahmenbedingungen eingehalten sind?
Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten	• Berücksichtigt der Vertrag zur Auftragsdatenverarbeitung alle relevanten Datenschutz-Aspekte? • Ist sichergestellt, dass externe Dienstleister die Auftragsdaten nur entsprechend den Weisungen des Auftraggebers verarbeiten? • Erfolgte auch beim Auftragnehmer für alle Mitarbeiter bei der Aufnahme ihrer Tätigkeit eine Verpflichtung auf das Datengeheimnis? • Enthält der Auftragsvertrag alle Regelungsgegenstände des Art. 28 Abs. 3 UAbs. 1 S. 2 DSGVO? Lässt sich für den Vertragsschluss auf Standardvertragsklauseln zurückgreifen, um die Bürokratiekosten des Vertragsschlusses zu senken? (Vgl. Art. 28 Abs. 6 und 7 DSGVO)
Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten	• Ist die Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten geregelt? • Erfolgt vor Verarbeitung personenbezogener Daten die Prüfung der datenschutzrechtlichen Unbedenklichkeit?
Datenschutzaspekte bei der Protokollierung	• Gibt es ein Konzept, das den Zweck der Protokollierung, deren Kontrollen sowie Schutzmechanismen für die Rechte der betroffenen Personen be-

	schreibt? • Erfährt die Zweckbindung der Protokolldaten Beachtung, insbesondere bei den Zugriffsregelungen? • Lässt die Form der Protokollierung effektive Auswertungsmöglichkeiten zu? • Wurden die Auswertungsmöglichkeiten mit dem Datenschutzbeauftragten und der Personalvertretung abgestimmt?
Aufrechterhaltung des Datenschutzes im laufenden Betrieb	• Wird regelmäßig überprüft, ob die datenschutzrechtlichen Anforderungen eingehalten werden? • Sind die Zuständigkeiten und Kompetenzen von IT-Revision und Datenschutzkontrolle abgestimmt? • Ist die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) sowie die Benachrichtigung Betroffener (Art. 34 DSGVO) gewährleistet und innerhalb der Zuständigkeitsordnung abgebildet?
Datenschutzgerechte Löschung/Vernichtung	• Werden Datenträger, die personenbezogene Daten enthalten, sicher gelöscht bzw. vernichtet? • Kontrolliert der Datenschutzbeauftragte regelmäßig, dass Datenträger mit personenbezogenen Daten datenschutzgerecht gelöscht bzw. vernichtet werden?
Empfohlene Maßnahme[162]	**Prüffragen**
Einbeziehung des Datenschutzbeauftragten und Datenschutz-Folgenabschätzung	• Ist vorgesehen, dass vor den Software-Tests mit Daten, die Personenbezug haben könnten, und vor der Datenschutz-Folgenabschätzung (Art. 35 Abs. 2 DSGVO) der Rat des Datenschutzbeauftragten einzuholen ist? • Ist vor der Freigabe von IT-Verfahren, die personenbezogene Daten verarbeiten, eine datenschutzrechtliche Prüfung eingeplant? • Ist (insbesondere in der Zuständigkeitsordnung) sichergestellt, dass bei verbleibendem hohen oder mittleren Restrisiko vor der Verarbeitung eine Konsultation der Aufsichtsbehörde erfolgt (Art. 36 Abs. 1 DSGVO)?

Tabelle 8: Prüffragen zu möglichen Datenschutzmaßnahmen

[162] Der IT-Grundschutz sowie die Datenschutzgesetze einiger Länder fordern zusätzlich eine schriftliche datenschutzrechtliche Freigabe beim erstmaligen Einsatz von IT-Verfahren, mit denen personenbezogene Daten verarbeitet werden.

5.6 Beispiel – Prozessmodell BPMN 2.0

Der folgende, prototypische elektronische Geschäftsgang in einem E-Akte- und Vorgangsbearbeitungssystem ist aus fachlich-operationeller Sicht in einem hohen Abstraktionsgrad dargestellt (durch die Verwendung von Subprozessen). Das Prozessmodell bildet einen möglichen Standardverlauf ohne Sonderfälle ab.

In dem Beispiel verfügt Behörde A über eine zentrale Post- und Scanstelle und über Abteilungsregistraturen. Im Zuge der Bearbeitung beteiligt sie die Behörde B in einem Mitzeichnungsverfahren. Nach Ablauf der Transfer- und Aufbewahrungsfristen wird der Vorgang der zuständigen Archivbehörde angeboten und von dieser übernommen.

Die Schnittstellen setzt dieses Beispiel als bidirektionale Software- und Datenschnittstellen voraus (bspw. in Form eines Nachrichtentauschs über XDOMEA[163]). Sie bezeichnen aus organisatorischer Sicht den Übergang der übermittelten Daten von einem Zuständigkeitsbereich zum anderen.

Hinweis

Die Datenobjekte werden in der Regel auf Ebene der einzelnen Prozessaktivitäten (als Input bzw. Output des jeweiligen Bearbeitungsschritts) dargestellt. Der unten dargestellte Standardprozess wäre insoweit daher noch weiter zu detaillieren (bspw. um im Subprozess „Erfassung“ der Post- und Scan-Stelle zwischen Posteingängen in Papier und elektronischen Posteingängen zu unterscheiden).

[163] Siehe http://www.xoev.de/detail.php?gsid=bremen83.c.11406.de.

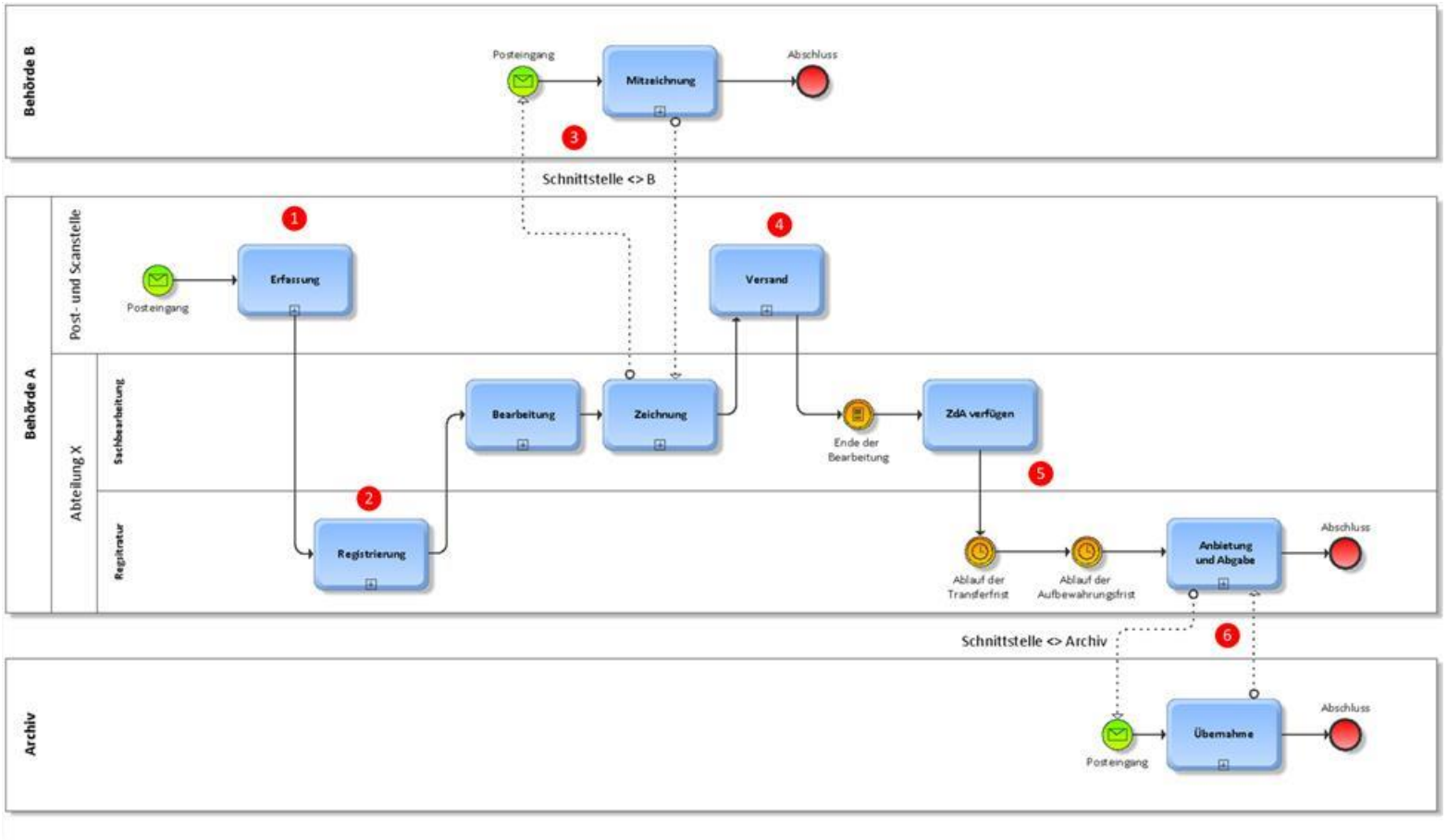

Abbildung 13: Beispiel eines Sollprozesses in BPMN 2.0

Folgende datenschutzrechtlichen Fragestellungen und Anforderungen lassen sich im Prozessmodell verorten (die entsprechenden Stellen sind in der Abbildung rot nummeriert; die Aufzählung ist nicht abschließend).

Nr.	Fragestellung	Antwort
1	Ersterfassung der zentralen Posteingänge durch Mitarbeiter der Post- und Scanstelle	
1.1	Sind organisatorische Maßnahmen vorgesehen, um zu vermeiden, dass Schriftgut digitalisiert und in das E-Akte-System überführt wird, das nicht für die Bearbeitung in elektronischer Form vorgesehen ist?	
1.2	Gibt es technische und organisatorische Maßnahmen, die gewährleisten, dass der Beweiswert der Dokumente bei Übernahme erhalten bleibt? Wurden für das beweiswerterhaltende Scannen Aufbewahrungsfristen der Papieroriginale definiert?	
1.3	Existieren organisatorische Maßnahmen, die vermeiden, dass personenbezogene Informationen mit besonderem Schutzbedarf in Metadaten erscheinen?	
1.4	Gibt es entsprechende technische und organisatorische Maßnahmen, um Fehlleitungen aus der zentralen Post- und Scanstelle zu verhindern?	
2	Registrierung durch die Abteilungsregistratur	
2.1	Sind die entsprechenden technischen und organisatorischen Maßnahmen vorgesehen, um Fehler bei der Zuordnung des Posteingangs zu einem Aktenzeichen und Vorgang zu vermeiden?	
2.2	Gibt es organisatorische Maßnahmen, die vermeiden, dass personenbezogene Informationen mit besonderem Schutzbedarf in Metadaten erscheinen?	
3	Mitzeichnungsverfahren, Beteiligung einer anderen Behörde	
3.1	Erfolgt die Beteiligung externer Stellen über ein standardisiertes Austauschformat (bspw. XDOMEA)?	
3.2	Ist festgelegt, welche Metadaten an externe Stellen zu übertragen sind?	
3.3	Erfolgte eine Übertragung des Primärdokuments in einem unveränderlichen Format wie bspw. PDF/A?	
3.4	Gibt es eine definierte Vorgehensweise, um die Informationen über die Mitzeichnung zur mitgezeichneten Version des Dokuments ablegen und nachvollziehbar halten zu können?	
4	Versand des schlussgezeichneten Dokuments	
4.1	Kann der Versand in elektronischer Form erfolgen? Besteht für den Postausgang das Erfordernis der Schriftform?	
4.2	Muss eine Empfangsbestätigung auf den Versand erfolgen? Ist De-Mail oder eine VPS zu verwenden?	
5	zdA-Verfügen des Vorgangs	
5.1	Für welchen Benutzerkreis ist der zdA-verfügte Vorgang im	

	System noch recherchierbar?	
5.2	Wie wird gewährleistet, dass der Vorgang nach Ablauf der Transferfrist vollständig in das Zwischenarchiv/die Altregistratur übernommen wird?	
6	Anbietung und Abgabe an das zuständige Archiv	
6.1	Welche Schnittstelle besteht zum zuständigen Archiv?	
6.2	Wie wird gewährleistet, dass das Schriftgut dem Archiv vollständig angeboten und übermittelt wird?	
6.3	Wie wird gewährleistet, dass das vom Archiv übernommene Schriftgut vollständig aus dem System gelöscht wird?	

Tabelle 9: Übersicht aus der Prozessanalyse abgeleiteter Fragestellungen

6 Glossar

Anonymisieren	Verändern personenbezogener Daten derart, dass sich die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zuordnen lassen. Auf anonyme Daten ist die DSGVO nicht anwendbar.
Authentizität (von Daten)	Verbindlichkeit von Daten (insbesondere Dokumente und Urkunden) und Informationen, die im Rahmen der elektronischen Verwaltungsarbeit zwischen den Akteuren übertragen werden.
Automatisierte Verarbeitung	Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen (vgl. auch Art. 2 Abs. 1 DSGVO).
Besondere Kategorien personenbezogener Daten (vgl. Art. 9 DSGVO; § 22 BDSG))	Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.
BDSG	Bundesdatenschutzgesetz in der ab dem 25. Mai 2018 geltenden Fassung.
BDSG a. F.	Bundesdatenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung.
Betroffener	(identifizierte oder identifizierbare) natürliche Person, deren personenbezogene Daten verarbeitet werden.
Belastbarkeit	Fähigkeit eines Systems, mit Veränderungen (etwa durch Störungen) umgehen zu können, also die Toleranz und Ausgleichsfähigkeit eines Systems gegenüber Störungen.
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BPMN 2.0	Business Process Model and Notation der Object Management Group, http://www.omg.org/spec/BPMN/2.0/.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
Dritter (Art. 4 Nr. 10 DSGVO)	jede Person oder Stelle außerhalb der verantwortlichen Stelle; Dritte sind nicht • der Betroffene sowie • diejenigen Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
Einwilligung (Art. 4 Nr. 11; Art. 7 DSGVO)	„jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“ (Art. 4 Nr. 11 DSGVO).
Empfänger (Art. 4 Nr. 9	jede Person oder Stelle, die Daten erhält (unabhängig davon, ob es sich bei

DSGVO)	ihr um einen Dritten handelt oder nicht).
Erheben (personenbezogener Daten)	Beschaffen von Daten über den Betroffenen.
Informationsverbund	Gesamtheit der infrastrukturellen, organisatorischen, personellen und technischen Objekte (definiert den Geltungsbereich des IT-Sicherheitskonzepts).
Integrität (von Daten)	Unversehrtheit der elektronischen Daten und der enthaltenen Informationen bei Übertragung im Rahmen der elektronischen Kommunikation wie auch bei Speicherung (in bspw. einem E-Akte-System).
Intervenierbarkeit	verfahrensrechtliche Absicherung, dass Betroffene die ihnen zustehenden Rechte wirksam ausüben können.
Löschen (personenbezogener Daten)	Unkenntlich-Machen gespeicherter personenbezogener Daten.
Mobile personenbezogene Speicher- und Verarbeitungsmedien	Datenträger, die an den Betroffenen ausgegeben werden, auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.
Nachvollziehbarkeit (von Daten)	Möglichkeit, nachvollziehen zu können, wie die Erhebung, Übermittlung und sonstige Verarbeitung von Daten erfolgt.
Nichtabstreitbarkeit	Nichtabstreitbarkeit[164] zielt auf eine Nachweisbarkeit gegenüber Dritten. Sie soll gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es ist zu unterscheiden zwischen: • Nichtabstreitbarkeit *der Herkunft*: Es soll einem Absender einer Nachricht unmöglich sein, nachträglich zu bestreiten, dass er eine Nachricht abgesendet hat. • Nichtabstreitbarkeit *des Erhalts*: Es soll einem Empfänger einer Nachricht unmöglich sein, nachträglich zu bestreiten, dass er eine gesendete Nachricht erhalten hat.
Nicht automatisierte Datei	jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist, nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.
Nutzen (von Daten)	Verwenden von Daten, soweit nicht Verarbeiten vorliegt (z. B. Abruf auf dem Bildschirm).
OCR	optische Zeichenerkennung (Optical Character Recognition – OCR): bezeichnet eine Komponente der Scan-Software, die aus einem Scan-Produkt (Bilddatei) elektronisch verwertbare Textinformationen (Volltext) generiert.
Personenbezogene Daten	Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), wie z. B. Alter, Anschrift, Vermögen, Äußerungen, Überzeugungen (Art. 4 Nr. 1 DSGVO).
Pseudonymisierung	Schwächung des Personenbezugs einer Verarbeitung dadurch, dass die Identifikation einer bestimmten Person nur dadurch möglich ist, dass der Verarbeitende ergänzende Informationen hinzuzieht (Art. 4 Nr. 5 DSGVO, vgl. auch Art. 32 Abs. 1 Hs. 2 lit. a DSGVO). Zu den Voraussetzungen erfolgreicher Pseudonymisierung gehört es, die zusätzliche Information ge-

[164] Siehe BSI, IT-Grundschutz-Kataloge, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/glossar/04.html.

	sondert aufzubewahren sowie technische und organisatorische Maßnahmen zu ergreifen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zuordenbar sind.
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz).
Speichern (personenbezogener Daten)	Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung.
Sperren	Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.
Transparenz (Art. 5 Abs. 1 lit. a DSGVO)	Erhebung, Verarbeitung und Nutzung personenbezogener Daten müssen mit zumutbarem Aufwand nachzuvollziehen, zu überprüfen und zu bewerten sein können.
Unverkettbarkeit	Verfahren sind so einzurichten, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (technisch-organisatorische Gewährleistung der Zweckbindung).
Übermitteln (personenbezogener Daten)	Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.
Verändern (personenbezogener Daten)	inhaltliches Umgestalten gespeicherter personenbezogener Daten.
Verantwortlicher	natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO).
Verarbeiten (von Daten)	jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte „Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ (Art. 4 Nr. 2 DSGVO).
Verfügbarkeit (von Daten)	Abrufbarkeit von Daten und Informationen im elektronischen Geschäftsgang in dem jeweils benötigten Umfang (in E-Akte-Systemen besteht insbesondere der Anspruch auf Vollständigkeit der elektronischen oder ggf. hybrid geführten Akten).
Vertraulichkeit (von Daten)	Schutz gegen unberechtigte Zugriffe Dritter (vgl. Art. 5 Abs. 1 lit. f; Art. 32 Abs. 1 Hs. 2 lit. b DSGVO).
VPS	Virtuelle Poststelle, also eine Komponente, welche die Authentizität, Integrität und Nichtabstreitbarkeit des Empfangs elektronisch übermittelter Dokumente zwischen registrierten Kommunikationspartnern herstellen soll.[165]

[165] Für weitere Informationen siehe auch: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/VirtuellePoststelle/virtuellepoststelle_node.html.