Bundesministerium
des Innern

Organisationskonzept elektronische Verwaltungsarbeit

Baustein Datenschutz und Personaldaten

Version 1.0
Februar 2016

Fortschritt sichern
verwaltung-innovativ.de

Dokumentenhistorie

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Zweck und Funktion des vorliegenden Dokuments

Die Umstellung von der analogen auf die elektronische Verwaltungsarbeit ist für die öffentliche Verwaltung und ihre Beschäftigten von fundamentaler Bedeutung. Die gesetzliche Regelung der Grundsätze der elektronischen Aktenführung und des ersetzenden Scannens ist seit dem 1. August 2013 durch das E-Government-Gesetz[1] in Kraft und soll durch die Behörden des Bundes einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts bis 2020 umgesetzt werden. Dies schließt insbesondere auch den gesetzlichen Anspruch der Betroffenen auf den Schutz ihrer personenbezogenen Daten gemäß Bundesdatenschutzgesetz (BDSG) ein.

In Systemen zur elektronischen Verwaltungsarbeit werden auf unterschiedliche Weise immer auch personenbezogene Informationen erfasst, verarbeitet und ggf. auch übermittelt. Diese können als Primärinformationen in den elektronischen Dokumenten selbst, als Metadaten zu den Dokumenten, Vorgängen und Akten und auch als Bearbeitungs- und Protokollinformationen des elektronischen Geschäftsgangs vorliegen und unterschiedliche Personen und Persönlichkeitsrechte betreffen. Besonders hervorzuheben ist, dass im Gegensatz zur Arbeit mit Papierakten elektronische Systeme in der Regel Funktionalitäten bereitstellen, die personenbezogene Daten ohne größeren Aufwand recherchierbar machen.

Das vorliegende 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, als auch
- zur elektronischen Personalakte (eP-Akte) bieten.

Das in diesem Dokument in Kapitel 3 dargestellte, allgemeine Vorgehen bei der Planung und Umsetzung von Anforderungen des Datenschutzes orientiert sich an den bestehenden Regelungen und Leitlinien zum Datenschutz auf Bundes- und Landesebene – u. a. an dem vom BSI vorgeschlagenen Vorgehen[2].

In Kapitel 4 behandelt der Baustein das Thema Datenschutz in Hinblick auf die Einführung einer eP-Akte. Die rechtlichen Rahmenbedingungen zum Umgang mit Personaldaten finden sich in Kapitel 2.1.13.

1.2 Einordnung in das Organisationskonzept Elektronische Verwaltungsarbeit

Der Datenschutz ist ein grundlegender Bestandteil jedes Einführungsprojekts im Bereich der elektronischen Verwaltungsarbeit und bereits in der Projektvorbereitungsphase unter Beteiligung von Interessenvertretern und Datenschutzbeauftragten zu berücksichtigen und zu planen.[3]

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

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

[3] Siehe dazu auch in Baustein „Projektleitfaden“ die Anlage 3: Kommunikationsplan

Im Kontext des Organisationskonzepts elektronische Verwaltungsarbeit bildet der Baustein zum Datenschutz eine wichtige Basis, da die Einhaltung der Datenschutzanforderungen in der öffentlichen Verwaltung obligatorische Voraussetzung eines jeden IT-Einführungsprojekts ist.

Der Baustein will daher eine möglichst generische Beschreibung des Vorgehens bei der Erhebung der datenschutzrechtlichen Anforderungen liefern und 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 werden in den entsprechenden Bausteinen des Organisationskonzeptes behandelt und in dem vorliegenden Baustein an den jeweils geeigneten Stellen referenziert. Von besonderer Relevanz sind insbesondere

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

Die nachfolgende Abbildung gibt eine Übersicht über die Struktur des Baukastens und seine einzelnen Bestandteile.

Abbildung 1: Baukasten Organisationskonzept E-Verwaltungsarbeit

2 Allgemeine Aspekte des Datenschutzes in der elektronischen Aktenführung und Vorgangsbearbeitung

2.1 Datenschutzrechtliche Grundsätze

2.1.1 Allgemeines

Ziel des Datenschutzes ist es, durch das Aufstellen von Verwendungsregeln für personenbezogene Daten und über die Gestaltung und den Einsatz von Informationstechnik eine Gefährdung des Persönlichkeitsrechts des Einzelnen von vorneherein zu verhindern.

Wirksam unterstützt wird dieses Ziel dadurch, dass möglichst keine personenbezogenen Daten, oder – wo das nicht möglich ist – möglichst wenige personenbezogene Daten verwendet werden. Riesige Datenmengen sollen erst gar nicht entstehen (Datenvermeidung bzw. Datensparsamkeit, vgl. § 3a BDSG). Die technisch-organisatorischen Maßnahmen, die nach § 9 BDSG und seiner dazu ergangenen Anlage zu treffen sind, sollen die Daten u. a. gegen unerlaubten Zugriff und Verwendung sichern.

Das geltende Datenschutzrecht der Bundesrepublik Deutschland ist im Bundesdatenschutzgesetz (BDSG) und in bereichsspezifischen Gesetzen geregelt[4]. Es ist mithin Ausdruck der Tatsache, dass der Einzelne über garantierte und unveräußerliche Persönlichkeitsrechte verfügt, die er sowohl gegenüber dem Staat als auch gegenüber anderen gesellschaftlichen Akteuren verteidigen kann, wobei wiederum der Staat im Rahmen der Gewaltenteilung ihn zu unterstützen verpflichtet ist. Insofern kommt dem Schutz personenbezogener Daten im Rahmen der elektronischen Aktenführung durch die Stellen und Einrichtungen des Bundes eine entscheidende und für andere Akteure exemplarische Bedeutung zu.

Das Datenschutzrecht erschöpft sich keineswegs im BDSG. Neben diesem und darüber hinaus enthalten verschiedene Einzelgesetze, die Bestimmungen zum Umgang mit speziellen Arten personenbezogener Daten enthalten, sind etwa

- das Sozialgesetzbuch (SGB),
- das Bundesverfassungsschutzgesetz (BVerfSchG),
- das Bundespolizeigesetz (BPolG),
- das Telekommunikationsgesetz (TKG),
- das Telemediengesetz (TMG),
- das Gesetz über den militärischen Abschirmdienst (MADG)

Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (SÜG)

In diesem Sinne ist das BDSG ein so genanntes Auffanggesetz, das in den Fällen zur Anwendung kommt, in denen keine spezialgesetzlichen Bestimmungen zu personenbezogenen Daten vorliegen.

Für die Personalakten in den Stellen und Einrichtungen des Bundes gelten die folgenden Gesetze:

[4] Der vorliegende Baustein basiert auf der Fassung des BDSG vom 14.1.2003.

- Bundesbeamtengesetz (BBG)
- Bundespersonalvertretungsgesetz (BPersVG)
- Soldatengesetz (SG)

In den Landes- und Kommunalbehörden, gelten z.T. abweichende personalrechtliche Regelungen, wie bspw. das Beamtenstatusgesetz (BeamtStG).

Im Kontext der elektronischen Personalakte ist zwischen Personaldaten und Personalaktendaten zu unterscheiden (siehe dazu Kap. 2.1.13).

Das BDSG gilt uneingeschränkt für öffentliche Stellen des Bundes[5] und für nichtöffentliche Stellen (Private), sofern diese unter den in § 1 Abs. 2 Nr. 3 BDSG beschriebenen Anwendungsbereich fallen.

Öffentliche Stellen des Bundes sind

- 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, gelten für sie die §§ 4b und 4c BDSG. Sie basieren auf der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[6].

Die hinsichtlich der elektronischen Verwaltungsarbeit relevanten Regelungen des BDSG zu den Grundsätzen des Datenschutzrechts (Zulässigkeit, Erforderlichkeit, Zweckbindung, Datensparsamkeit, Transparenz) sowie zu den Rechten der Betroffenen (u. a. Recht auf Auskunft, Berichtigung, Löschung, Sperrung) werden in den folgenden Kapiteln beschrieben.

2.1.2 Verbot mit Erlaubnisvorbehalt (§§ 4, 4a, 28 BDSG)

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt. Die Erhebung, Verarbeitung und Nutzung von Daten sind verboten, es sei denn,

- sie sind durch eine Rechtsvorschrift ausdrücklich erlaubt oder angeordnet

oder

- der Betroffene hat dazu seine Einwilligung erklärt.

Wenn eine Rechtsvorschrift den Umgang mit personenbezogenen Daten ausdrücklich erlaubt oder sogar anordnet, kommt es auf die Einwilligung des Betroffenen nicht an.

[5] Siehe auch § 18 Durchführung des Datenschutzes in der Bundesverwaltung, http://www.gesetze-im-internet.de/bdsg_1990/__18.html

[6] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046&from=DE

Bei der Verarbeitung besonderer Arten personenbezogener Daten gem. § 3 Absatz 9 BDSG muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

2.1.3 Zweckbindungsgrundsatz (§§14, 28 BDSG)

Personenbezogene Daten dürfen durch öffentliche Stellen gespeichert, verändert oder genutzt werden, soweit

- dies zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und
- sie für die Zwecke erfolgt, für die die Daten erhoben worden sind (falls keine Erhebung voran ging: für die sie erstmalig gespeichert worden sind). Das heißt, dass personenbezogene Daten grundsätzlich nur zu den Zwecken verarbeitet werden dürfen, für die sie erhoben bzw. gespeichert worden sind (Zweckbindungsgrundsatz).

Die Verarbeitung personenbezogener Daten für einen anderen Zweck ist dann zulässig, wenn

- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
- der Betroffene eingewilligt hat,
- es offensichtlich im Interesse des Betroffenen liegt,
- Angaben des Betroffenen überprüft werden müssen, weil begründete Zweifel an ihrer Richtigkeit bestehen,
- die Daten allgemein zugänglich sind oder veröffentlicht werden dürften (aber nicht, wenn das entgegenstehende schutzwürdige Interesse des Betroffenen offensichtlich überwiegt),

oder wenn sie

- zur Gefahrenabwehr,
- zur Wahrung erheblicher Belange des Gemeinwohls,
- zur Verfolgung von Straftaten oder Ordnungswidrigkeiten,
- zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte eines anderen oder
- zur Durchführung wissenschaftlicher Forschung (nach näher bestimmten Voraussetzungen)

erforderlich ist.

In engem Zusammenhang mit dem Zweckbindungsgrundsatz steht das Prinzip der Datenvermeidung und Datensparsamkeit gemäß § 3a BDSG, wonach bei der Datenverarbeitung nur so viele personenbezogene Daten erhoben werden sollen, wie für die jeweilige Anwendung bzw. den jeweiligen Zweck unbedingt notwendig sind. An diesem Prinzip müssen sich auch IT-Systeme und IT-Anwendungen ausrichten, die personenbezogene Daten verarbeiten. (vgl. 2.1.9)

2.1.4 Besondere Arten personenbezogener Daten (§ 3 Absatz 9 BDSG)

Besondere Arten personenbezogener Daten sind in § 3 Absatz 9 BDSG definiert und beinhalten Angaben über

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder philosophische Überzeugungen,

- Gewerkschaftszugehörigkeit,
- Gesundheit oder
- Sexualleben.

Das Gesetz schränkt die Möglichkeiten der Erhebung, Verarbeitung und Nutzung dieser Daten an vielen Stellen ein.

2.1.5 Datenerhebung (§§ 4, 13, 28 BDSG)

Die Datenerhebung darf nur in dem erforderlichen Umfang erfolgen. Bei den öffentlichen Stellen heißt dies, dass die Daten für die Erfüllung der gesetzlichen Aufgaben erforderlich sind.

Besondere Arten personenbezogener Daten (vgl. 2.1.4) dürfen – ohne wirksame Einwilligung des Betroffenen – nur in vom Gesetz abschließend aufgeführten Ausnahmefällen erhoben werden.

Derartige Daten sind grundsätzlich beim Betroffenen zu erheben. Es ist ihm mitzuteilen, zu welchem Zweck dies geschieht. Nur in Ausnahmefällen dürfen die Daten bei anderen und ohne Kenntnis des Betroffenen erhoben werden. Ist der Betroffene gegenüber einer öffentlichen Stelle zur Auskunft verpflichtet (z.B. bei amtlichen Statistiken), so muss ihm gesagt werden, nach welchen Rechtsvorschriften das der Fall ist. Er ist auch aufzuklären, wenn er ohne die von ihm verlangten Auskünfte seine Ansprüche nicht durchsetzen kann oder ihm sonstige Rechtsvorteile entgehen.

2.1.6 Datenübermittlung (§§ 4b, 4c, 15, 16, 27, 28, 39 BDSG)

Das Übermitteln an eine öffentliche Stelle ist zulässig, wenn

- es für die Aufgabenerfüllung der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, erforderlich ist und
- der Verwendungszweck beim Dritten, an den die Daten übermittelt werden, gleich ist oder eine zulässige Zweckänderung vorliegt.

Werden Daten zur Erfüllung der eigenen Aufgaben an eine nicht-öffentliche Stelle übermittelt, so gelten dieselben Regelungen wie bei einer Übermittlung an eine öffentliche Stelle.

Die Übermittlung an eine nicht-öffentliche Stelle ist außerdem zulässig, wenn der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hat und der Betroffene keine schutzwürdigen Interessen am Ausschluss der Übermittlung hat. Der Betroffene muss in diesen Fällen informiert werden. Dies gilt nicht, wenn er von der Übermittlung schon auf anderem Wege weiß oder die öffentliche Sicherheit einer Unterrichtung im Wege steht.

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

Die Datenübermittlung in ein Land außerhalb der Europäischen Union, ein sogenanntes „Drittland“, ist zulässig, wenn der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat und insbesondere in dem Drittland ein angemessenes Datenschutzniveau gewährleistet ist. Ob in einem Drittland ein angemessenes Datenschutzniveau herrscht wird von der EU-Kommission durch einen förmlichen Beschluss festgelegt. Eine Datenübermittlung in nicht sichere Drittländer ist nach den europarechtlichen Vorgaben nur zulässig, wenn dies durch Verträge ab-

gesichert wird, die die sog. Standardvertragsklauseln enthalten, die die EU-Kommission mit Beschluss vom 5. Februar 2010[7] für Datenübermittlungen ab dem 15. Mai 2010 zwingend vorgeschrieben hat.

2.1.7 Beauftragter für den Datenschutz (§§ 4f und 4g BDSG)

Nach § 4f Absatz 1 BDSG sind alle Stellen und Einrichtungen des Bundes verpflichtet, einen Beauftragten für den Datenschutz zu bestellen. Dieser muss nach § 4f Absatz 2 Satz 1 BDSG die erforderliche Fachkunde und Zuverlässigkeit besitzen. Die Aufgaben des Datenschutzbeauftragten finden sich im Wesentlichen in § 4g BDSG. Danach muss der behördliche Datenschutzbeauftragte auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz hinwirken. Dies geschieht in aller Regel durch die Beratung, aber auch durch Kontrollen hinsichtlich der Einhaltung der gesetzlichen Bestimmungen. Darüber hinaus finden sich auch an anderen Stellen des BDSG weitere Aufgaben für den behördlichen Datenschutzbeauftragten, wie etwa in § 4f Absatz 5 Satz 2 BDSG die Verpflichtung, sich um die Belange der Betroffenen (dies sind außer den Bürgern auch die Beschäftigten der eigenen Stelle) zu kümmern.

2.1.8 Vorabkontrolle (§§ 4d Absätze 5 und 6 BDSG)

Für automatisierte Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, sieht das Bundesdatenschutzgesetz eine Prüfung vor Beginn der Verarbeitung (Vorabkontrolle) vor.

Beispielhaft nennt das Gesetz zwei Fallgestaltungen, in denen die Vorabkontrolle notwendig ist:

- bei der Verarbeitung von personenbezogenen Daten besonderer Art (§ 3 Absatz 9 BDSG),
- bei Verfahren, die dazu dienen, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

Die Vorabkontrolle muss in folgenden Fällen nicht durchgeführt werden:

- wenn eine gesetzliche Verpflichtung zur Durchführung der Datenverarbeitung besteht,
- wenn die Einwilligung des Betroffenen vorliegt,
- wenn die Erhebung, Verarbeitung oder Nutzung im Rahmen der Zweckbestimmung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erfolgt.

Ist eine Vorabkontrolle durch das Gesetz vorgeschrieben, ist sie eine weitere Voraussetzung für die Zulässigkeit der Datenverarbeitung. Wurde eine notwendige Vorabkontrolle vollständig unterlassen, ist die Datenverarbeitung rechtswidrig. Das inhaltliche Votum des Datenschutzbeauftragten ist für die verantwortliche Stelle aber nicht bindend.

Im Rahmen einer Vorabkontrolle prüft der Datenschutzbeauftragte sowohl die rechtliche Zulässigkeit der beabsichtigten Verarbeitung als auch, ob die vorgesehenen technischen und organisatorischen Maßnahmen nach dem Stand der Technik ausreichend und angemessen sind. Er kann hierzu eine Risikoanalyse durchführen und ein Sicherheitskonzept erstellen bzw. erstellen lassen.

[7] Beschluss der EU-Kommission vom 5. Februar 2010 (2010/87/EU) über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl.EG Nr. L 39, S. 5 ff

Durchgeführt wird die datenschutzrechtliche Vorabkontrolle anhand der Verfahrensübersicht nach § 4e BDSG (vgl. § 4d Abs. 6 Satz 2 BDSG).

2.1.9 Technische und organisatorische Sicherung des Datenschutzes (§§ 3a, 9, 9a, 10 BDSG)

Schon bei der Konzeption von IT-Systemen müssen Belange des Datenschutzes berücksichtigt werden („Privacy by Design“). Dabei geht es in erster Linie darum, den Umfang der erhobenen und verarbeiteten personenbezogenen Daten auf ein Minimum zu beschränken.

Ein sehr wichtiger Bereich des Datenschutzes sind die technischen und organisatorischen Maßnahmen, die zum Schutz von personenbezogenen Daten getroffen werden müssen, um sie vor Missbrauch und Verarbeitungsfehlern zu sichern.

Sowohl öffentliche als auch nicht-öffentliche Stellen (§ 2 BDSG), die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, sind gehalten, entsprechende technische und organisatorische Maßnahmen zu ergreifen. Welche Maßnahmen notwendig sind, hängt sowohl von der Art der Daten ab, als auch von der Aufgabe, den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen der Verarbeitung.

Die Maßnahmen müssen sich nach dem Stand der Technik richten und sind daher regelmäßig fortzuschreiben. Ziel dieser Maßnahmen ist das Erreichen bestimmter Schutzziele wie Verfügbarkeit, Vertraulichkeit, Integrität u. a.

Die Schutzziele der technisch-organisatorischen Maßnahmen zum Datenschutz werden in Kapitel 2.2.1 im Einzelnen beschrieben.

Für die Einrichtung automatisierter Verfahren zum Abruf personenbezogener Daten sind besondere Anforderungen zu beachten. Sie sind nur zulässig, wenn sie unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen einerseits und der Aufgaben oder Geschäftszwecke der beteiligten Stellen andererseits angemessen sind. Hinzuweisen ist auch darauf, dass bei automatisierten Abrufverfahren eine Pflicht zur Kontrolle der Abrufe besteht.

2.1.10 Datenverarbeitung im Auftrag (§ 11 BDSG)

Entschließt sich eine Stelle zum Outsourcing solcher Tätigkeiten, die auch die Erhebung, Verarbeitung und Nutzung personenbezogener Daten beinhalten, muss sie dabei verschiedene rechtliche, technische und organisatorische Voraussetzungen erfüllen.

Beispiele für die Datenverarbeitung im Auftrag sind u.a.

- Betrieb eines Rechenzentrums im Auftrag,
- Entsorgung von Datenträgern,
- technischer Betrieb einer virtuellen Poststelle.

Werden dem Auftragnehmer personenbezogene Daten zu diesem Zweck überlassen, findet datenschutzrechtlich gesehen keine Übermittlung statt, da der Auftragnehmer nicht Dritter ist. Gegenüber den Bürgerinnen und Bürgern bleibt der Auftraggeber (also die Stelle, um deren Aufgabe es geht) voll dafür verantwortlich, dass mit ihren personenbezogenen Daten rechtmäßig umgegangen wird.

Dies setzt voraus, dass

- der Auftraggeber einen schriftlichen Auftrag erteilen muss (was genau schriftlich geregelt werden muss, legt § 11 Absatz 2 detailliert fest),
- der Auftragnehmer nur im Rahmen der Weisungen seines Auftraggebers tätig werden darf und
- der Auftraggeber die erforderlichen Maßnahmen zur Datensicherheit vorgeben muss.

Der Auftraggeber muss sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen und das Ergebnis dieser Überprüfung dokumentieren.

Werden Aufträge an Auftragnehmer erteilt, die ihren Sitz im europäischen Wirtschaftsraum haben und die Datenverarbeitung dort ausführen, gelten dieselben Vorgaben wie für inländische Auftragnehmer.

2.1.11 Auskunft an den Betroffenen (§§ 19,19a, 34, 35 BDSG)

Betroffene, also natürliche Personen, über die Daten erhoben, verarbeitet und genutzt werden, haben gegenüber den öffentlichen (oder auch nicht-öffentlichen) Stellen das Recht auf Auskunft. Sie können hierzu einen Antrag an die entsprechende öffentliche Stelle richten, Auskunft zu folgende Sachverhalten zu erteilen:

1. die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen. Das bedeutet u.a., dass öffentlichen Stellen nur dann Auskünfte über personenbezogene Daten in Akten erteilen, wenn der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der Arbeitsaufwand nicht außer Verhältnis zum Informationsinteresse des Betroffenen steht. Weitere Voraussetzungen für die Auskunftserteilung sind in § 19 Abs. 2 und 3 definiert.

Öffentliche Stellen dürfen die Auskunft verweigern, soweit

- die Gefahr besteht, dass sie ihre Aufgabe nicht ordnungsgemäß erfüllen können, z.B. wenn laufende polizeiliche Ermittlungen gefährdet würden,
- die Auskunft die öffentliche Sicherheit oder Ordnung gefährden würde

  oder
- die Daten oder die Tatsache, dass die Stelle sie speichert, geheim gehalten werden müssen (aus gesetzlichen Gründen oder im Geheimhaltungsinteresse eines Dritten, z.B. Adoptionsgeheimnis), und deswegen das Interesse des Betroffenen an der Auskunft zurücktreten muss.

Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er gemäß § 19a BDSG von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten.

2.1.12 Berichtigung, Löschung und Sperrung sowie Widerspruchsrecht (§§ 20, 35 BDSG) unter Berücksichtigung von § 2 BArchG

Allgemeine Grundsätze zur Löschung von personenbezogenen Daten

Jede Stelle, die personenbezogene Daten verarbeitet, ist verpflichtet, unrichtige Daten zu berichtigen.

Personenbezogene Daten sind von öffentlichen Stellen zu löschen, wenn

- ihre Speicherung unzulässig ist, etwa weil schon die Erhebung unzulässig war, oder
- die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich ist.

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. Sind allerdings komplette Akten unzulässig angelegt, so sind sie ebenfalls zu vernichten. Ebenso ist im Allgemeinen mit nicht mehr erforderlichen Akten zu verfahren.

Grundsätze zur Löschung von Protokolldaten

Besondere Aufmerksamkeit verdienen Protokolldateien, die häufig bei der automatisierten Datenverarbeitung erzeugt, gespeichert und übertragen werden. Beispiele hierfür sind u. a.

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

Enthalten diese Protokolldateien personenbezogene Daten oder lassen sich anhand der Protokolldateien unmittelbare Rückschlüsse auf personenbezogene Daten ziehen, unterliegen die Protokolldateien den o.g. datenschutzrechtlichen Grundsätzen, wie u.a. der Zweckbindung und der Datensparsamkeit.

Hier findet ebenfalls § 20 BDSG Anwendung, nach dem personenbezogene Daten, die automatisiert verarbeitet werden, zu löschen sind, wenn ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Zur Erforderlichkeit von Protokollierungen enthält das BDSG keine expliziten Regelungen. Allerdings finden sich im Landesdatenschutzgesetz Schleswig-Holsteins entsprechende Anforderungen:

„Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.

Werden personenbezogene Daten ausschließlich automatisiert gespeichert, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. Entsprechendes gilt für die Veränderung und Übermittlung der Daten. Die Protokolldaten müssen zusammen mit den gespeicherten personenbezogenen Daten sichtbar gemacht werden können und für den gleichen Zeitraum aufbewahrt werden.“

Für diese Protokolldaten gelten die o.g. Grundsätze.

Grundsätze zur Sperrung von personenbezogenen Daten

Personenbezogene Daten sind immer dann zu sperren, wenn einer fälligen Löschung besondere Gründe entgegenstehen, wie etwa

- gesetzlich, satzungsmäßig oder vertraglich festgelegte Aufbewahrungsfristen,

- schutzwürdige Interessen des Betroffenen, etwa weil ihm Beweismittel verloren gingen, oder
- ein unverhältnismäßig hoher Aufwand wegen der besonderen Art der Speicherung.

Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu sperren, wenn der Betroffene ihre Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Die Tatsache dieser Sperrung darf dann gleichfalls nicht übermittelt werden.

Betroffene haben das Recht, unter bestimmten Voraussetzungen sogar einer rechtmäßigen Datenverarbeitung zu widersprechen. Für den öffentlichen Bereich ist das in § 20 Absatz 5 BDSG geregelt.

Der Widerspruch ist begründet,

- sofern besondere Umstände in der Person des Betroffenen vorliegen,
- das schutzwürdige Interesse des Betroffenen das Interesse der verantwortlichen Stelle an der Erhebung, Verarbeitung oder Nutzung der entsprechenden personenbezogenen Daten überwiegt.

Sonderregelung der Anbietungspflicht von Unterlagen

Entsprechend der in § 2 Abs. 1 des Bundesarchivgesetzes (BArchG) geregelten Anbietungspflicht sind alle „Verfassungsorgane, Behörden und Gerichte des Bundes, die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und die sonstigen Stellen des Bundes“ verpflichtet, „alle Unterlagen, die sie zur Erfüllung ihrer öffentlichen Aufgaben einschließlich der Wahrung der Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder nicht mehr benötigen, dem Bundesarchiv oder in Fällen des Absatzes 3 dem zuständigen Landesarchiv zur Übernahme anzubieten und, wenn es sich um Unterlagen von bleibendem Wert im Sinne des § 3 handelt, als Archivgut des Bundes zu übergeben. Von der Anbietungspflicht ausgenommen sind Unterlagen, deren Offenbarung gegen das Brief-, Post- oder Fernmeldegeheimnis verstoßen würde.“

Demnach unterliegen auch Personaldaten[8] der Anbietungspflicht gegenüber dem Bundesarchiv. Dieses hat nach § 2 Abs. 4 „von der Übergabe an ebenso wie die abgebende Stelle die schutzwürdigen Belange Betroffener zu berücksichtigen; insbesondere hat es bei Unterlagen mit personenbezogenen Daten bei der Erfüllung seiner Aufgaben die Vorschriften über die Verarbeitung und Sicherung dieser Unterlagen zu beachten, die für die abgebende Stelle gelten.“

Entsprechend weist auch § 113 Abs. 4 BBG auf die Anbietungspflicht gegenüber dem zuständigen Archiv nach § 2 BArchG hin.

Dem Gebot einer Datenlöschung, das für eine Personaldaten oder Personalaktendaten führende Stelle im Sinne des § 1 BArchG gilt, ist also auch dann genüge getan, wenn diese Daten dem Bundesarchiv übergeben und aus den eigenen Datenhaltungssystemen entfernt wurden.

2.1.13 Besonderheiten bei Personaldaten und Personalaktendaten (§ 12 Abs. 4, § 32 BDSG,§ 34 BDSG, §§ 106 ff. BBG, §29 SG)

Grundsätzlich muss zwischen Personaldaten (§12 Absatz 4 BDSG) und Personalaktendaten (§ 106 BBG[910]) unterschieden werden: „*Zur Personalakte gehören alle*

[8] Zur Definition vgl. Kap. 2.1.133

[9] Für Soldatinnen und Soldaten wird auf § 29 des Soldatengesetzes (SG) verwiesen.

Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit ihrem oder seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten).“ Und weiter heißt es in § 106 BBG: „*Nicht Bestandteil der Personalakte sind 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.*“

Bei der Verarbeitung von Personaldaten gelten die §§ 28 Absatz 2 Nummer 2 sowie 32-35 BDSG. Demnach dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist (§ 32 BDSG) Dies gilt auch für die nichtautomatisierte Verarbeitung der Daten. Dabei gelten die Bestimmungen zu den Rechten der Betroffenen (§§ 33-34 BDSG) sowie zur Berichtigung, Sperrung und Löschung der Daten (§ 35 BDSG).

Besonderheiten zur Führung von Personalakten für Beamtinnen und Beamte werden in §§ 106-115 BBG geregelt[11]. Für die Tarifbeschäftigten des Bundes findet sich in § 3 Absatz 5 TVöD lediglich das Recht auf Einsicht in die Personalakte. Die Vorschriften aus §§ 106-115 BBG können jedoch sowohl hinsichtlich der Führung der Personalakten durch den Arbeitgeber als auch zur Auslegung des § 3 Abs. 5 TVöD sinngemäß herangezogen werden.

Einer vollständig elektronisch geführten Personalakte stehen keinerlei Bestimmungen entgegen. 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), da die Zivilprozessordung öffentlichen, elektronischen Dokumenten unter bestimmten Maßgaben eine uneingeschränkte urkundliche Qualität zumisst (Zivilprozessordnung § 437 i. V. m. § 416a i. V. m. § 371a).

Der § 106 Abs. 2 BBG erlaubt das Führen von Teilakten und legt fest, dass Teilakten bei der für den betreffenden Aufgabenbereich zuständigen Behörde geführt werden können. Eine derartige Untergliederung in Teilakten erleichtert die technische und organisatorische Umsetzung eines stark reglementierten Zugriffs im Rahmen des Rollen- und Berechtigungskonzepts.

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

[10] Für Landes- und Kommunalverwaltungen gilt § 50 BeamtStG entsprechend.

[11] Für Soldatinnen und Soldaten wird die Führung von Personalakten in § 29 des Soldatengesetzes (SG) in Verbindung mit der Personalaktenverordnung Soldaten (SPersAV) geregelt.

- Nebentätigkeiten
- Dienstunfälle

Nebenakten dagegen („Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden“) dürfen nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für die Beamtin oder den Beamten zuständig sind; sie dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist. Damit sollen in erster Linie im weiteren Dokumentenlebenszyklus nur noch schwer zu steuernde Duplikate schutzwürdiger Unterlagen vermieden werden. Weiter heißt es in § 106 Absatz 2 BBG: „*In die Grundakte ist ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen. Wird die Personalakte nicht vollständig in Schriftform oder vollständig automatisiert geführt, legt die personalverwaltende Stelle jeweils schriftlich fest, welche Teile in welcher Form geführt werden und nimmt dies in das Verzeichnis nach Satz 4 auf.*“ Damit ist sicherzustellen, dass in der Grundakte alle Duplikate nachgewiesen sind.

Nach § 110 BBG haben Beamtinnen und Beamte (Tarifbeschäftigte nach § 3 Abs. 5 TVöD, Soldatinnen und Soldaten nach §29 SG) das Recht, nicht nur ihre Personalakte selbst einzusehen oder durch Bevollmächtigte einsehen zu lassen, sondern auch andere Unterlagen mit sie selbst betreffenden personenbezogenen Daten, die für ihr Dienstverhältnis verwendet werden, sofern dadurch nicht schutzwürdige Belange Dritter berührt werden.

Unter bestimmten, in § 111 BBG geregelten Bedingungen dürfen Personalakten auch Dritten vorgelegt werden oder diese aus Personalakten Auskünfte erhalten.

Eine weitere Besonderheit von Personalakten und abweichend vom Grundsatz der Unversehrtheit und Vollständigkeit der übrigen Sach- und Fallaktenführung ist die Entfernung von Unterlagen unter definierten Bedingungen aus einer Personalakte (§ 112 BBG).

2.2 Schutzziele und Schutzbedarf

2.2.1 Schutzziele

Personenbezogene Daten sind grundsätzlich schutzwürdig, d.h. der Einzelne ist davor zu schützen, „dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“ (§ 1 BDSG). Die Schutzwürdigkeit personenbezogener Daten leitet sich also ab aus der Schutzwürdigkeit der Person, der diese Daten zugeordnet werden können, und ihrer verfassungsmäßigen Freiheitsrechte.

Beim Einsatz der elektronische Aktenführung und Vorgangsbearbeitung stellen sich die Fragen der Sicherstellung des Schutzes personenbezogener Daten in besonderer Weise dahingehend, dass Verstöße gegen die datenschutzrechtlichen Grundsätze (vgl. Kapitel 2.1) schon bei der Konzeption und beim Systemdesign zu vermeiden sind. Es ist im Besonderen zu vermeiden, dass

- (personenbezogene) Daten unzulässig in der E-Akte gespeichert werden oder bleiben,
- auf in der E-Akte gespeicherte Daten unzulässig zugegriffen werden kann,
- Daten manipuliert werden und

- auf Protokolldaten der Beschäftigten zum Zweck der Leistungs- und Verhaltenskontrolle zugegriffen wird.

Damit sind bereits wesentliche konkrete Schutzziele definiert, weitere lassen sich direkt aus den unter 2.1 erläuterten datenschutzrechtlichen Grundsätzen ableiten. Demnach sind die sechs *Schutzziele der technisch-organisatorischen Maßnahmen zum Datenschutz* (vgl. Kapitel 2.1.9) zu verfolgen:

- **Verfügbarkeit**
  Verfahren und Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß angewendet werden.

- **Vertraulichkeit**
  Auf Verfahren und Daten darf nur befugt zugegriffen werden.

- **Integrität**
  Daten aus Verfahren bleiben unversehrt, zurechenbar und vollständig.

- **Transparenz**
  Erhebung, Verarbeitung und Nutzung personenbezogener Daten müssen mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden 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).

- **Intervenierbarkeit**
  Verfahren sind so zu gestalten, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen.

Die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit entsprechen den Grundwerten der Informationssicherheit. Ihre Sicherstellung verfolgt den technischen und organisatorischen Schutz der Informationsverarbeitung und gewährleistet somit mittelbar auch den Schutz der verarbeiteten personenbezogenen Daten (vgl. 2.1.9).

Die drei weiteren Schutzziele Transparenz, Unverkettbarkeit und Intervenierbarkeit hingegen folgen unmittelbar aus den datenschutzrechtlichen Grundsätzen. Die praktische Verfolgung dieser Schutzziele ermöglicht erst die datenschutzrechtliche Zulässigkeit der Datenverarbeitung.

Zu beachten ist, dass es bei der gleichrangigen Verfolgung der genannten Schutzziele zu Konflikten zwischen den Ansprüchen des Datenschutzes und der Informationssicherheit kommen kann, wenn bspw. aus Sicherheitsgründen erhobene Protokollinformationen technischer Systeme Daten der diese Systeme nutzenden Beschäftigten enthalten.

2.2.2 Schutzbedarf

Die sechs Schutzziele beziehen sich auf die Gesamtheit der Verarbeitung personenbezogener Daten in informationstechnischen Systemen. Allerdings sind nicht alle Daten, bzw., im Fall der E-Akte, nicht alle Dokumente gleich schutzbedürftig. So unterscheidet der Datenschutz zwischen „normalen“ und „besonderen“ personenbe-

zogenen Daten (vgl. Kapitel 2.1.4), wobei letztere als besonders schutzwürdig anzusehen sind.

Für die Auswahl und Begründung der technischen und organisatorischen Maßnahmen nach § 9 BDSG ist es darüber hinaus zielführend, über Kriterien zu verfügen, nach denen die Zweckmäßigkeit und Notwendigkeit der Maßnahmen bewertet und begründet werden kann. Hierfür findet der Begriff des *Schutzbedarfs* Anwendung. Der Schutzbedarf bezieht sich primär auf die Schwere der potenziellen Einschränkung des in § 1 BDSG festgestellten Persönlichkeitsrechts des Betroffenen und geht aus vom Schaden, den der Einzelne erleiden würde, wenn seine Daten missbraucht würden.

Ist also vom Schutzbedarf personenbezogener Daten die Rede, so sollte stets der Bezug zu den genannten sechs Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz, Unverkettbarkeit und Intervenierbarkeit hergestellt werden, um zu bewerten, ob und in welcher Schwere eine Verletzung eines dieser Schutzziele zu Beeinträchtigungen der Persönlichkeitsrechte des Betroffenen führen kann.

Wie Verletzungen der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu datenschutzrechtlichen Folgen führen können, zeigen die folgenden drei Beispiele:

- Die Verletzung der Vertraulichkeit durch Offenlegung medizinischer Informationen über eine Person kann diese in ihrem Recht auf freie Berufswahl einschränken oder zu anderweitigen Diskriminierungen führen.
- Die Verletzung der Integrität durch Verfälschung von Einkommens- und Steuerdaten einer Person kann zu deren strafrechtlicher Verfolgung führen.
- Der Verlust der Verfügbarkeit durch Löschen von Sozialdaten kann dazu führen, dass die betroffene Person keine Ansprüche auf Sozialleistungen geltend machen kann.

Eine Skalierung des Schutzbedarfs kann hinsichtlich der Höhe und Relevanz der Schadensfolgen vorgenommen werden, die ein Verstoß gegen eines der elementaren Schutzziele nach sich ziehen würde. Hierzu gibt es unterschiedliche Ansätze.

Die **IT-Grundschutzvorgehensweise** des BSI (BSI-Standard 100-2[12]) 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.

Bezogen auf die Verletzung der Schutzziele bei der Verarbeitung personenbezogener Daten lässt sich damit der Schutzbedarf sowohl in Bezug auf einen einzelnen Betroffenen (Massivität der Verletzung) als auch auf die datenverarbeitende Institution (Anzahl der Betroffenen) skalieren.

Die Norm **DIN 66399**[13] zur Datenträgervernichtung definiert drei Schutzklassen:

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

Schutzklasse 1 – normaler Bedarf für interne Daten:

Der Schutz von personenbezogenen Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, dass der Betroffene in seiner Stellung und seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Beispiele:

- Besoldung/Entgeltzahlungen,
- Abrechnungsdaten,
- Abfertigungsdaten, Steuerbescheide,
- personenbezogene Firmendaten,
- Ordnungswidrigkeitenverfahren,
- dienstliche Beurteilungen und Leistungseinschätzungen

Schutzklasse 2 – hoher Bedarf für vertrauliche Daten:

Gefahr, dass der Betroffene 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 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

Der niedersächsische Landesbeauftragte für Datenschutz (LfD) empfiehlt die Anwendung eines differenzierten Schutzstufenkonzeptes, welches zwischen fünf Schutzstufen personenbezogener Daten unterscheidet.[14]

Personenbezogene Informationen mit unterschiedlichen Schutzbedarfen können grundsätzlich in allen Aktentypen (Generalakten, Fallakten und Personalakten) vorkommen und sind hinsichtlich ihres Schutzbedarfs jeweils auf Dokumentebene zu bewerten.

Die Personalakte stellt in diesem Zusammenhang einen Sonderfall dar, auf den ergänzend in Kapitel 4 exemplarisch eingegangen wird.

[13] 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 SPEC 66399-3 „Büro- und Datentechnik - Vernichten von Datenträgern - Teil 3:Prozess der Datenträgervernichtung“

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

2.3 Arten von Informationen zu elektronischen Akten, Vorgängen und Dokumenten

Die elektronischen Schriftgutobjekte Akte, Vorgang, Dokument bestehen aus verschiedenen Arten elektronischer Daten, die jeweils auch personenbezogene oder personenbeziehbare Informationen enthalten können: Neben den Primärdaten sind dies die Metadaten und die Protokolldaten[15]. Primärdaten sind dabei die Inhalte der elektronischen Schriftgutobjekte. Metadaten sind Daten zur Beschreibung und Steuerung der elektronischen Schriftgutobjekte. Protokolldaten sind schließlich Daten zum Geschäftsgang bzw. zur allgemeinen Nutzung und Bearbeitung der elektronischen Schriftgutobjekte.

2.3.1 Primärdaten

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

Damit über das E-Akte-System auch Suchen in den Primärdaten möglich werden, wird für binär-codierte Dokumente häufig ein Volltextindex extrahiert16. Dieser ermöglicht die Suche in elektronischen Dokumenten - je nach Benutzerberechtigung - über mehrere Vorgänge und Aktenbereiche hinweg.

Die personenbezogenen Informationen, die in den Primärdaten elektronischer Dokumente enthalten sein können, sind je nach Aufgabe der Verwaltung unterschiedlich. Die Analyse des eingehenden und ausgehenden Schriftguts und seines jeweiligen Schutzbedarfs ist für jede Behörde unbedingt einzeln und auf Dokumentebene vorzunehmen. Detaillierte Informationen hierzu stellen die Kapitel 3.2 „Analyse des Prozessablaufs und der Prozessbeteiligten“ und Kapitel 3.3 „Grundlage der Schutzbedarfsanalyse“ dar.

Insbesondere die Volltextsuche über verschiedene Datenbestände (und Zuständigkeiten) hinweg birgt immense datenschutzrechtliche Probleme. Grundsätzlich muss hier gelten, dass Unterlagen, auf die nicht mindestens eine Leseberechtigung für den Suchenden besteht, auch nicht recherchiert werden können, so dass diese in der Trefferliste einer Suchanfrage nicht angezeigt werden. Welche Funktionen auf einer Menge von Daten durchgeführt werden können und welche Aggregationen dabei möglich sein sollen, muss daher auch unter organisatorischen Gesichtspunkten geprüft und in einem Rollen- und Berechtigungskonzept festgelegt werden.

Die prinzipiellen Möglichkeiten eines technischen Administrators, übergreifende Sichten auf einen oder mehrere Datenbestände zu erzeugen, sind ebenfalls als kritisch einzustufen. Entsprechende Risiken können durch eine klar definierte Einschränkung dieser Möglichkeiten auf das unbedingt Erforderliche und/oder die Etablierung des Vier-Augen-Prinzips bzw. eines Zwei-Schlüssel-Prinzips bei der Erzeugung bestimmter Abfragen reduziert werden.

[15] Zu den Begriffen vgl. das Glossar des Organisationskonzepts elektronische Verwaltungsarbeit; http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/glossar_e_verwaltung.pdf.

[16] Der Volltextindex wird beispielsweise 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.

2.3.2 Metadaten

Metadaten sind Daten über Daten und stellen damit eine wesentliche Komponente der Schriftgutverwaltung dar.

Metadaten dienen zum einen der Beschreibung, der Ordnung, der Indizierung und der Klassifizierung von Informationsobjekten – also der elektronischen Dokumente als kleinste logische Einheiten des Schriftguts im elektronischen Geschäftsgang sowie der Vorgänge und Akten. Sie enthalten beschreibende Informationen und treffen somit Aussagen über die Eigenschaften der elektronischen Schriftgutobjekte, deren Struktur und inhaltliche Zusammenhänge.

Durch ihren informativen Charakter ermöglichen Metadaten, redundante Datenerfassungen zu vermeiden und vorhandene Lücken in den Datenbeständen aufzudecken (Ermittlung fehlender Angaben). Ferner sind Metadaten von Bedeutung für die Qualitätssicherung, ermöglichen Vergleiche zwischen alternativen Datenbeständen und tragen erheblich zur Transparenz des Datenbestandes bei. Metadaten können umso sinnvoller genutzt werden, wenn darin standardisierte Begriffe und Informationen verwendet werden.

Zum anderen dienen Metadaten der Steuerung automatisierbarer Datenverwaltungsprozesse, wie z. B. der Gestaltung von Workflows, der Steuerung der Datenpflege (z.B. Versionierung) sowie der Aussonderung und Löschung von Daten.

Bestehende Normen und Standards zu Metadaten im Rahmen der Schriftgutverwaltung sind:

- DIN ISO 15489-1 Schriftgutverwaltung
- DIN ISO 23081-1 Information und Dokumentation - Metadaten für Verfahren der Schriftgutverwaltung
- MoReq2010 (Modular Requirements for Records Systems)[17].

Im Kontext des Datenschutzes sind einzelne Metadatenfelder ebenso bzgl. des Schutzbedarfs der in ihnen potentiell enthaltenen Informationen zu betrachten, die sich in manchen Fällen aus den Primärinformationen ableiten. 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 Scanstelle Informationen enthalten, die personenbezogen und damit datenschutzrechtlich relevant sind.

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

2.3.3 Protokolldaten

Unter Protokollierung ist der automatisierte Nachweis von Handlungen der Anwender eines E-Akte-Systems an den Schriftgutobjekten im Rahmen des elektronischen Geschäftsgangs zu verstehen (wie bspw. Erstellen, Ändern oder Löschen[18]). Diese bezieht sich üblicherweise auf alle Arten von Schriftgutobjekten – auf Dokumente und ihre Metadaten sowie auf die Vorgänge und Akten.

[17] 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 für das elektronische Dokumenten-, Archiv- und Schriftgutverwaltung etabliert.

[18] 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/SharedDocs/Publikationen/Orientierungshilfen/OHProtokollierung.html?nn=408912

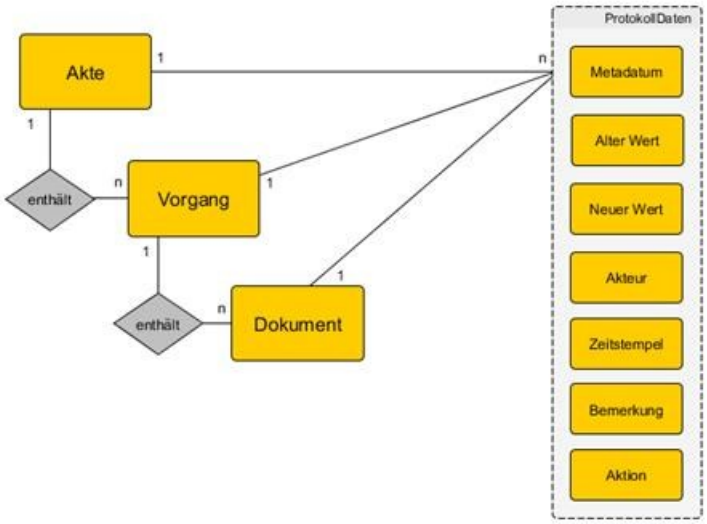

Abbildung 2: Relation von Protokolldaten zu elektronischen Schriftgutobjekten

Anhand der Protokolldaten wird festgehalten, 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 Ebenen der Hierarchie Akte, Vorgang, Dokument jeweils auf der nächsthöheren Ebene zur Verfügung gestellt, um insbesondere die Nachvollziehbarkeit des elektronischen Geschäftsganges zu gewährleisten. So würde der in dem obigen Beispiel der Löschung eines Dokuments erzeugte Protokolleintrag sinnvollerweise auch im betreffenden Vorgang zur Verfügung gestellt. Genauso wie die Bereitstellung der Protokolldaten über die zdA-Verfügung eines Vorgangs auch in der enthaltenden Akte erfolgen wird.

Das Gebot der behördlichen Aktenführung fordert die oben beschriebene Erfassung von Protokollinformationen durch das E-Akte-System.[19] Aus datenschutzrechtlicher Sicht sind die Betroffenen stets die Anwender– im elektronischen Geschäftsgang also die Bediensteten – die auf der Sozialebene mit jedem Protokolleintrag eindeutig, meist namentlich erfasst werden können.

Die durch das E-Akte-System erzeugten personen-, zeit- und aktivitätsbezogenen Informationen bieten potentiell die Möglichkeit der aggregierten Auswertung zum Zwecke der Leistungskontrolle. Dies stellt im Sinne des Datenschutzes eine Gefährdung der Persönlichkeitsrechte der Betroffenen dar und würde dem Grundsatz der Zweckbindung nach § 14 BDSG entgegenstehen.

Die Beschäftigten haben grundsätzlich auch im Arbeitsverhältnis ein Recht auf die Wahrung ihrer Persönlichkeitsrechte und damit einen Anspruch auf einen angemessenen Schutz ihrer personenbezogenen Daten.

Nicht betrachtet wird an dieser Stelle die Protokollierung auf anderen Ebenen – sog. Betriebsprotokolle, die bspw. Zugriffe oder Login-Versuche einzelner Benutzer auf Komponentenebene (Firewall, Applikationsserver, Datenbankserver etc.) protokollieren. Diese Art der Protokollierung kann bspw. als Sicherheitsmaßnahme umge-

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

setzt 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 Sollkonzeption detailliert zu definieren. Die Beteiligung des Datenschutzbeauftragten wird dringend empfohlen.

2.4 Besonderheiten im Lebenszyklus elektronischer Dokumente

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

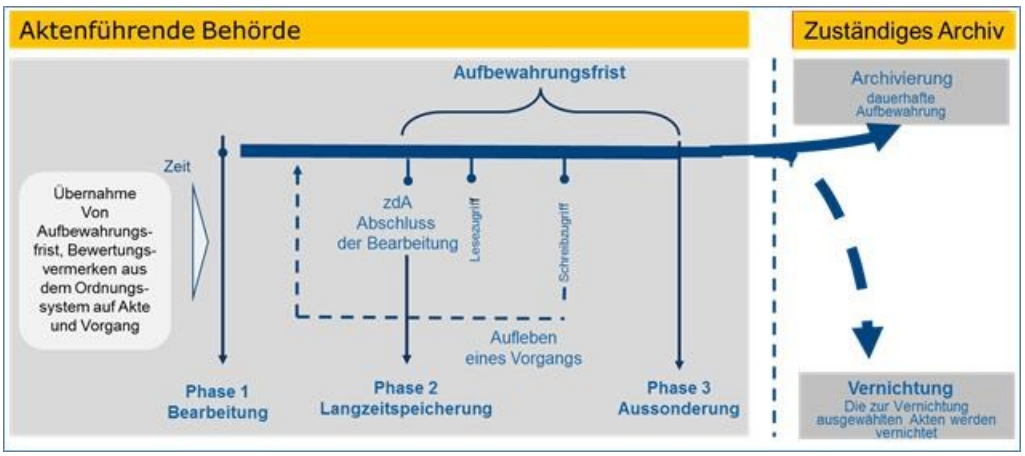

Abbildung 3: Lebenszyklus elektronischer Schriftgutobjekte

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

2.4.1 Eingangsbehandlung

Die unmittelbare Digitalisierung der Posteingänge[20] und die systematische elektronische Verteilung durch eine zentrale Post- und Scanstelle bergen einerseits in Behörden ein hohes Potential für eine höhere Effizienz im elektronischen Geschäftsgang. Häufig stellen aber die in ihrer Art sehr unterschiedlichen Posteingänge hohe Anforderungen an die mit der Ersterfassung betrauten Beschäftigten. Die Bausteine „E-Poststelle“ und „Scanprozess“ des Organisationskonzeptes E-Verwaltung behandeln die allgemeinen rechtlichen, fachlichen und funktionalen Anforderungen an die Digitalisierung des Posteingangs sowie die Prozesse der elektronischen Posteingangs- und -ausgangsbearbeitung.

Folgende Aspekte sind hinsichtlich des Datenschutzes u. a. zu berücksichtigen:

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

- Verfälschung der digitalisierten Dokumente durch fehlerhafte bzw. unvollständige OCR-Erkennung[21] (verfälscht wäre hier wohlgemerkt der zur binären Scan-Ausgabedatei hinterlegte Volltext des Posteingangs, was in der späteren Bearbeitung dazu führen kann, dass das Schriftgutobjekt bei der Recherche nicht gefunden wird).
- Bei der Ersterfassung könnten inhaltsbeschreibende Metadaten vergeben werden, die personenbezogene Informationen mit Schutzbedarf enthalten.[22]
- Dem ersetzenden Scannen[23] und der damit verbundenen Vernichtung des Papieroriginals stehen die gesetzlichen Anforderungen der Beweiswerterhaltung sowie des Rechts auf Rückgabe des Originals gegenüber. Beim automatisierten Scannen besteht die Gefahr, dass Schriftgut falsch klassifiziert und dadurch falsch zugeteilt wird (Verlust von Vertraulichkeit). Fragen zur Beweiswerterhaltung des gescannten Originals werden im Baustein „Scanprozess“ des Organisationskonzeptes elektronische Verwaltungsarbeit behandelt[24].
- Bei der Zuleitung der digitalisierten Posteingänge in Postmappen an die jeweils zuständige Abteilung kann es zu Fehlleitungen aufgrund von Fehleinschätzung der fachlichen Zuständigkeit oder aufgrund von Fehlbedienung kommen. Dies könnte für Posteingänge mit personenbezogenen Informationen von hohem Schutzbedarf zu einer Verletzung des Vertraulichkeitsgrundsatzes führen.
- Bei elektronischen Eingängen die als E-Mail nicht an zentrale Postfächer, sondern direkt an den Sachbearbeiter adressiert sind, ist sicherzustellen, dass das Schriftgut hinreichend frühzeitig in der Akte registriert wird.

Für elektronische Eingänge aus E-Mail-, Fax- und Formularsystemen gelten grundsätzlich die gleichen Bearbeitungsregeln wie für konventionelle, papiergebundene Posteingänge. Gerade E-Mails machen den Hauptanteil der elektronischen Eingänge aus. Auch hier 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.[25]

Aus Sicht des Datenschutzes ist im Vorfeld zu prüfen, für welche elektronischen Schriftgutobjekte die Eingangsbehandlung zentralisiert erfolgen sollte und wo eine funktionsbezogene, dezentrale Behandlung der Posteingänge (bspw. zur Wahrung der Vertraulichkeit) geboten ist. Auch ist die Verwendung von Automatismen bei der Vergabe von Metadaten für das Schriftgut der jeweiligen Behörde zu prüfen und es sind ggf. ergänzend organisatorische Regelungen zu treffen.

2.4.2 Inhaltliche Ersterfassung und Registrierung

Auf die Eingangsbehandlung in der Poststelle folgen die inhaltliche Ersterfassung und das Registrieren des Posteingangs im E-Akte-System durch die Registratur oder die dafür zuständige Stelle[26], die den Eingang einer prinzipiellen Zuständig-

[21] Optische Zeichenerkennung (Optical Character Recognition); siehe dazu im Baustein „Scanprozess“, Kap. 2.4.5

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

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

[24] Baustein Scanprozess, Kapitel 2.2.10.

[25] Vgl. dazu Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Vorgangsbearbeitung, S. 16.

[26] 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“, Kap. 3 Umsetzungsszenarien)

keitsprüfung unterzieht, weitere Metadaten zum Dokument erfasst und es einem Aktenzeichen und Vorgang zuordnet.

Aus Sicht des Datenschutzes sind in dieser Phase Regelungen u. a. zu den folgenden Punkten zu treffen:

- Schriftgut mit schutzwürdigen, personenbezogenen Informationen darf nicht aufgrund falscher Zuordnung zu einer Akte oder einem Vorgang an den falschen Personenkreis innerhalb der Behörde adressiert werden bzw. mit den falschen Zugriffsrechten versehen werden.
- In den Metadaten dürfen keine besonderen personenbezogenen Informationen nach § 3 Abs. 9 BDSG zur Beschreibung des elektronischen Dokuments verwendet werden, da sie unmittelbar einen hohen Schutzbedarf haben.
- bei der Festlegung von Schlagworten im Zug der Registrierung von Schriftgut ist darauf zu achten, dass die elektronischen Schriftgutobjekte nicht in einem bestimmten Kontext recherchierbar werden, aus dem sich implizit Rückschlüsse auf schutzwürdige personenbezogene (oder personenbeziehbare) Informationen ziehen lassen.

Die o. g. Gefährdungen können aufgrund von Fehleinschätzung der Zuständigkeiten, fehlerhafte Klassifizierung in Unkenntnis der datenschutzrechtlichen Vorgaben oder durch Fehlbedienung bei der Zuordnung der elektronischen Dokumente zu Akten und Vorgängen entstehen und können durch entsprechende Regelungen bzw. organisatorische Maßnahmen reduziert werden.

Den Registratoren und den Mitarbeitern der Poststelle kommt bei der Einhaltung der Regelungen eine besondere Bedeutung zu. Die Beschäftigten sind entsprechend zu schulen und zu sensibilisieren[27].

2.4.3 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 seine Organisationseinheit bzw. für seine Funktion zugeordnet wurde.

Folgende Aspekte sind aus Sicht des Datenschutzes im Zuge der Erstellung und Bearbeitung von Dokumenten bzw. Schriftgutobjekten zu beachten:

- Sämtliche Bearbeitungsschritte und Änderungen von Primär- wie auch Metadaten sind durch das E-Akte-System nachvollziehbar zu halten und müssen eindeutig der jeweiligen sachbearbeitenden Person zugeordnet werden können[28].
- Als Anlagen dürfen nur solche Dokumente in den Geschäftsgang gegeben werden, die personenbezogene Informationen in dem Umfang enthalten, wie sie für die aktuelle Bearbeitung benötigt werden. Hierfür kann es ggf. erforderlich sein, eine Kopie des ursprünglichen Dokuments erstellen zu können, in der die für den konkreten Vorgang überflüssigen, personenbezogenen Daten geschwärzt sind.[29]
- Wo es möglich ist, sollten im elektronischen Geschäftsgang Kopien zum Verbleib vermieden und stattdessen mit Verweisen gearbeitet werden, durch die die

[27] Siehe dazu im Baustein „E-Poststelle“, Kap. 4.5

[28] Dies gilt insbesondere dann, wenn im Geschäftsgang personenbezogene Daten erfasst oder bearbeitet werden. Siehe dazu auch Punkt 5 der entsprechenden Anlage des §9 BDSG, Eingabekontrolle.

[29] Schwärzen von elektronischen Dokumenten kann auf verschiedenen 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.

referenzierten Dokumente in ihrem ursprünglichen Kontext mit den ursprünglichen Berechtigungen verbleiben.

- Kopien zum Verbleib sollten nur mit den entsprechenden Bearbeitungsrechten versehen sein und ggf. in einem unveränderbaren Format (PDF) übermittelt werden.

Grundsätzlich obliegt es stets der federführend sachbearbeitende Stelle eines Vorgangs, die inhaltlichen Zusammenhänge und die Erforderlichkeit der Beteiligung oder Information anderer Organisationseinheiten zu beurteilen und im elektronischen Geschäftsgang entsprechend umzusetzen. Dabei muss stets auch innerhalb einer Behörde das Prinzip der Datensparsamkeit berücksichtigt werden.[30]

2.4.4 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 der Ergänzung, Stellungnahme und auch Überarbeitung des Entwurfs. Wie oben für die federführend sachbearbeitende Stelle festgestellt, liegt auch hier die Verantwortung für den Umgang mit personenbezogenen Informationen bei der jeweiligen mitzeichnenden Stelle.

Aus Sicht des Datenschutzes ist Folgendes zu beachten.

- 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[31].
- Die angezeigten Dokumentversionen und die zugehörigen Zeichnungsdaten müssen im elektronischen Geschäftsgang nachvollziehbar und konsistent dargestellt und im E-Akte-System vorgehalten werden (Integrität und Authentizität).
- Es muss sichergestellt sein, dass die der zeichnenden Personen im E-Akte-System angezeigte Version des elektronischen Dokuments auch die Version ist, mit der ihre Zeichnungsinformationen verknüpft werden.
- Bei der Änderung gezeichneter Dokumente durch einer anderen sachbearbeitenden Stelle muss das System automatisch eine neue Version des Dokuments erzeugen, um einen im Sinne der Vollständigkeit und Nachvollziehbarkeit revisionssicheren elektronischen Geschäftsgang zu ermöglichen.
- Zeichnungen (im Sinne zusammengesetzter Informationsobjekte wie in Abbildung 4 dargestellt) müssen im System manipulationssicher vorgehalten werden. Abhängig vom Schutzbedarf und nach Bewertung der Risiken sind dafür geeignete Maßnahmen zu ergreifen. Hierzu können bspw. auch Maßnahmen auf Ebene der Fach- und Datenbankadministration gehören. Dies gilt sowohl für die Zeichnungsdaten selbst als auch für das gezeichnete Primärdokument. Letzteres könnte bspw. mit der Schlusszeichnung automatisch in ein unveränderbares Format (bspw. PDF/A) übertragen werden.

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.

[30] Vgl. dazu auch Organisationskonzept elektronische Verwaltungsarbeit. Baustein E-Akte, S. 33-35.

[31] zu den verschiedenen Arten der elektronischen Signatur siehe im Baustein „E-Poststelle“, Anlage 2

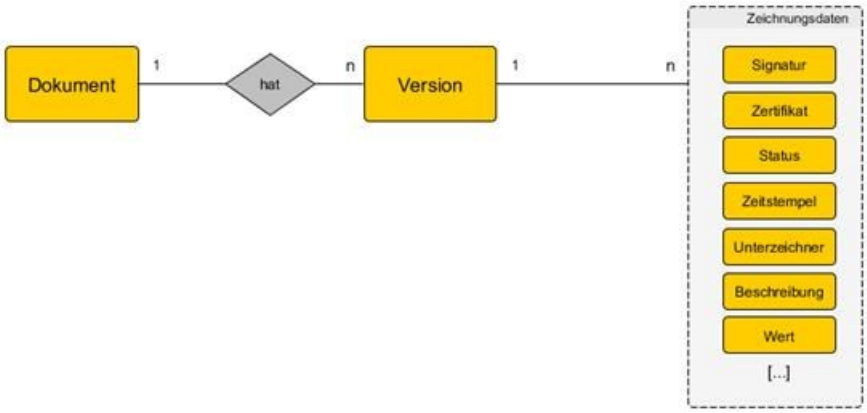

Abbildung 4: Relation von Dokument, Version und Zeichnungsdaten

Die Themen der langfristigen Sicherstellung der Gültigkeit elektronischer Signaturen während der Langzeitspeicherung und Archivierung sowie der Signaturerneuerung oder Übersignierung werden im Baustein „E-Langzeitspeicherung“[32] des Organisationskonzepts elektronische Verwaltungsarbeit behandelt.

2.4.5 Postausgang

Die Postausgangsbehandlung wird von den meisten E-Akte-Systemen mittels benutzerfreundlicher Funktionalitäten im Kontext des jeweiligen Schriftgutobjekts und ggf. des jeweiligen Prozessschritts unterstützt. Es besteht im Rahmen des elektronischen Geschäftsgangs einerseits die Möglichkeit des dezentralen Versands durch der aktuellen/federführenden sachbearbeitenden Stelle oder des zentralen Versands durch eine zentrale Poststelle.[33]

Auf die folgenden Punkte ist aus Sicht des Datenschutzes bei der Postausgangsbehandlung zu achten:

- Für den elektronischen Versand durch die sachbearbeitende Stelle oder eine zentrale Poststelle ist zu beachten, dass als Absenderadresse möglichst ein funktionsbezogenes Postfach und nicht die persönliche E-Mail-Adresse verwendet wird. Häufig erfolgt die Beantwortung elektronischer Ausgänge an den Absender. Somit würde eine zentrale Stelle zur Erfassung/Registrierung der elektronischen Eingänge umgangen und das Risiko der Unvollständigkeit der elektronischen Akte erhöht[34].
- Um die Nichtabstreitbarkeit des elektronischen Postausgangs zu gewährleisten, ist die Verwendung eines geeigneten Nachrichtenübermittlungs- und Zustelldienstes (elektronisches Gerichts- und Verwaltungspostfach (EGVP) oder De-Mail) obligatorisch, mit dem unter Verwendung elektronischer Signaturen eine rechtsverbindliche Empfangsbestätigung erzeugt wird.

[32] Siehe auch Organisationskonzept elektronische Verwaltungsarbeit, http://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung_node.html

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

[34] 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“.

- Durch den Einsatz von qualifizierten elektronischen Signaturen kann sichergestellt werden, dass der Beweiswert von Informationen, die elektronisch versendet werden, erhalten bleibt. [35]
- Bei der Ausgangsbehandlung von Dokumenten mit hohem Schutzbedarf sind folgende Maßnahmen 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. Bei Versand an Beteiligte mit Zugriff auf das E-Akte-System sollten möglichst immer nur die internen Links auf die abgelegten Dokumente und Vorgänge versendet werden. Dadurch bleibt das zugrundeliegende Rechtekonzept für die Schriftgutobjekte gewahrt und die Auswirkungen im Falle einer Fehladressierung gering. Damit dies möglich ist, müssen die Beteiligten über die entsprechenden Zugriffsberechtigungen verfügen. Wie diese ausgestaltet werden 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 ist zu beachten, dass mögliche Fehladressierungen (bspw. an verwaltungsexterne Adressen) auch durch das Hinterlegen einer Positivliste der in Frage kommenden Empfänger ausgeschlossen werden können.

2.4.6 Anbietung, Aussonderung und Archivierung

Die Aufbewahrungsfrist beginnt bei der E-Akte mit zdA-Verfügung, welche die Akte oder den Vorgang als abschließend bearbeitet kennzeichnet und abschließt. Die betreffenden Akten und Vorgänge dürfen aus Gründen der Rechts- und Beweissicherheit nicht mehr verändert oder gelöscht werden, können aber innerhalb der sog. Transferfrist[36] erneut in Bearbeitung genommen werden. Die zdA-Verfügung kann nur angebracht werden, wenn alle offenen Geschäftsgangvermerke und Verfügungen abgeschlossen wurden.

Wenn innerhalb der Transferfrist – in der Regel 1 Jahr – die Akten reaktiviert, d.h. einer erneuten Bearbeitung zugeführt werden, beginnen Transfer- und Aufbewahrungsfrist erneut.

Für die Dauer der Aufbewahrungsfrist verbleiben die Unterlagen in der Zuständigkeit der aktenführenden Behörde bzw. im Zwischenarchiv des Bundesarchiv (falls entsprechende Vereinbarungen getroffen wurden) und werden dort 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 (§ 2 BArchG). Alle als

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

[36] Die Transferfrist legt fest, für welchen Zeitraum z.d.A.-verfügte Akten und Vorgänge im aktiven Aktenbestand des DMS vorgehalten werden. (Siehe dazu im Baustein „E-Langzeitspeicherung“ das Kapitel 4 „Lebenszyklus der elektronischen Akte“)

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 sollen für die Übergabe an die Archivbehörde mit Angabe des Verfassers und des Datums im Klartext lesbar gespeichert werden. Elektronische Signaturen sind aufzulösen. Das Abgabeverfahren endet mit dem endgültigen Löschen der übergebenen Daten aus dem E-Akte-System der aktenführenden Behörde.

Die endgültige Abgabe ist in geeigneter Form zu protokollieren. Nach der Benachrichtigung über den erfolgreichen Import ins Archivsystem kann daraufhin auch das mit „A“ gekennzeichnete Schriftgut gelöscht werden.

Für die Archivierung gelten wiederum Sicherungen gegen den Missbrauch personenbezogener Daten wie Schutzfristen für die Nutzung des Archivguts, Pflicht zur ordnungsgemäßen und sicheren Aufbewahrung oder Schutzrechte der Betroffenen (§ 2 Abs. 4, § 5, § 11 BArchG)

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

2.4.7 Löschung

Löschungen von Akten oder Aktenbestandteilen, die nicht als Ergebnis eines regulären Anbieteverfahrens oder aufgrund einer Kassationsgenehmigung des zuständigen Archivs erfolgen oder die besonderen gesetzlichen Vorschriften entsprechen, sind prinzipiell nicht zulässig, sondern nur mit besonderen Berechtigungen möglich. Im schlimmsten Fall stellen unautorisierte Löschungen den Straftatbestand des Verwahrungsbruchs nach § 133 StGB dar.

Gemäß § 20 BDSG können für personenbezogene Daten berechtigte Anforderungen bestehen, diese zu löschen – bspw. wenn der Betroffene die Richtigkeit der Daten bestreitet (siehe hierzu Kap. 2.1.12).

Ob die vorgenommenen Löschungen nachgewiesen bzw. protokolliert werden müssen und wenn ja, wie – nämlich ohne zugleich zuzuordnende Angaben zu den zu löschenden Inhalten weiter mitzuführen – muss in entsprechenden Fach bzw. Rollen- und Berechtigungskonzepten definiert werden.

Zum Löschen vorgesehene oder gelöschte Schriftgutobjekte dürfen für nicht speziell berechtigte Anwender nicht mehr abrufbar sein oder 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 bewerteten Unterlagen sind vollständig zu löschen; das Archiv bewahrt als Nachweis eine Kassationsliste auf.

2.4.8 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.[37]

[37] Vgl. dazu Baustein „Scanprozess“, Kap. 3.3.1 „Metadatenvergabe/Indexierung/Volltextrecherche“

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

Entscheidend für den Datenschutz ist einerseits die Gültigkeit der für die einzelnen Schriftgutobjekte vergebenen Zugriffsrechte, damit ein nicht vorhandenes Suchrecht in Verbindung mit dem Profil des aktuellen Bearbeiters zu einer Trefferquote von null führt. Es kann andererseits Konstellationen geben, in denen Schriftgutobjekte, für die der angemeldete Benutzer kein Leserecht hat, in einer Trefferliste anzeigt werden sollen (bspw. in Bereichen der Fachadministration oder Registratur). Für solche Fälle ist mit Blick auf die Anforderungen des Datenschutzes der nachfolgende Hinweis zu beachten.

Hinweis

Im Falle von Schriftgutobjekten mit vertraulichen, personenbezogenen Inhalten (bspw. Personalakten) ist bereits das Erzeugen von Treffern zu Suchanfragen zu unterbinden, da schon durch die Feststellbarkeit des Vorhandenseins von Vorgängen zu bestimmten Suchbegriffen die Anforderungen des Datenschutzes verletzt werden können (bspw. das Vorhandensein von Abmahnungen in einer Personalakte).

Auch bieten die Systeme zur Unterstützung der elektronischen Verwaltungsarbeit berechtigten Benutzern häufig die Möglichkeit, Standardauswertungen zu definieren. Hier ist zu beachten, dass personenbezogene bzw. bearbeiterbezogene Auswertungen der Protokollinformationen des elektronischen Geschäftsgangs den datenschutzrechtlichen Grundsatz der Zweckgebundenheit verletzen, wenn sie zur Leistungskontrolle missbraucht werden.

2.4.9 Einsichtnahme

Betroffene haben nach § 19 BDSG bzw. nach § 34 BDSG i.V. mit § 12 (4) ein Recht auf Auskunft über die zu ihrer Person gespeicherten Daten sowie ein Recht auf Auskunft über deren Herkunft, Weitergabe und Zweck der Speicherung. Auf personenbezogene Daten Dritter bezieht sich der Auskunftsanspruch nicht, ggf. sind dabei daher Daten Dritter zu schwärzen.

Nach dem Informationsfreiheitsgesetz des Bundes[38] hat darüber hinaus gegenüber den Behörden des Bundes jeder einen Anspruch auf Zugang zu amtlichen Informationen.

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

Das Recht auf Einsichtnahme sollte entweder als technische Funktionalität (Konfiguration eines entsprechenden Berechtigungsprofils) des E-Akte-Systems oder als organisatorische Regelung[39] im Rahmen eines Standardprozesses bereits in der Planungsphase eines Einführungsprojekts berücksichtigt werden.

[38] Siehe auch Gesetz zur Regelung des Zugangs zu Informationen des Bundes, http://www.gesetze-im-internet.de/ifg/

[39] Mit Bezug auf das Informationsfreiheitsgesetz §1 Absatz 2 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,*

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

2.4.10 Verfügen

Auch im elektronischen Geschäftsgang übernimmt die federführende Sachbearbeitung die Verantwortung für die Abstimmung der Entscheidungsvorlage. Der Laufweg und die Bearbeitung von Dokumenten und Vorgängen können durch Verfügungen (z. B. „zur Mitzeichnung“, „zur Schlusszeichnung“, „zur Kenntnis“) gesteuert werden. Die Laufwege werden durch die zuständige Sachbearbeitung in der Regel ad hoc definiert.

In Zusammenhang mit dem Datenschutz sind die folgenden Aspekte beim Verfügen von Dokumenten und Vorgängen zu beachten:

- Der Versand von Objektkopien zum Verbleib sollte nur in unveränderlichen Formaten erfolgen (dabei wird insbes. PDF/A empfohlen[40]).
- Bei der Verfügung von Container-Objekten (wie Mappen, Vorgängen oder Akten) werden ggf. untergeordnete Dokumente mitverfügt. Es wird daher die Verwendung von Zeichnungsmappen (für Zeichnungsverfahren) bzw. Versandmappen (für den Versand von Kopien zum Verbleib) empfohlen, denen die zu verfügenden Schriftgutobjekte explizit zugeordnet werden müssen.
- Fehladressierungen können leichter erkannt werden, wenn die Bearbeitungsreihenfolge und die Adressaten (oder die Stellenkennzeichen) in den Informationen zum elektronischen Geschäftsgang vermerkt werden.
- Fehladressierungen durch Verwechslungen können leichter vermieden werden, wenn dem Benutzer in den Dialogen zur Suche und Auswahl von Mitarbeitern und Organisationseinheiten (OE) zusätzlich zum Namen des Bearbeiters auch dessen OE- oder Stellenkennzeichen angezeigt werden.
- Die Geschäftsgangvermerke sind grundsätzlich aktenrelevant und dürfen im weiteren Verlauf weder verändert noch gelöscht werden können.

2.4.11 Stellvertretung

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

Wesentlich aus Sicht des Datenschutzes sind

- die Beschränkung der Stellvertretung auf den erforderlichen Zeitraum,
- die Beschränkung der Stellvertretung auf explizit zu wählende Benutzer,
- die Protokollierung der Einnahme der Stellvertretung an sich sowie
- die lückenlose Protokollierung aller im Rahmen des elektronischen Geschäftsgangs an Schriftgutobjekten in Stellvertretung vorgenommenen Änderungen

wenn unterstellt werden kann, dass die technische Konfiguration eines entsprechend eingeschränkten Zugriffs auf die Informationen des E-Akte-Systems einen deutlich höheren Aufwand darstellt.

[40] Siehe auch Baustein E-Langzeitspeicherung des Organisationskonzeptes Elektronische Verwaltungsarbeit http://www.verwaltunginnovativ.de/SharedDocs/Publikationen/Organisation/e_langzeitspeicherung.html

Eine mögliche Form der Protokollierung am obigen Beispiel 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 werden 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:

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

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

2.4.12 Zugriffsrechte und Rollenprofile

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

Folgende Punkte sind dabei aus Sicht des Datenschutzes zu beachten:

- Die Protokollierung der 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) sollten möglichst aus Verzeichnisdiensten übernommen bzw. in Verzeichnisdiensten verwaltet werden, um sicher zu stellen, 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 vergeben werden können.
- Das System sollte die Möglichkeit bieten, bestimmte Aktenplanbereiche mit den entsprechenden (bspw. OE-bezogenen) Berechtigungen vorbelegen zu können.
- Sonderberechtigungen wie der Export, der Versand / die Weiterleitung an externe Stellen und die Nutzung von Schnittstellen zu anderen Verfahren müssen als in Berechtigungsprofilen gebündelte Benutzerrechte verwaltet werden können.
- 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.
- Es sollte auf Ebene der Schriftgutobjekte möglich sein, die Vergabe von Zugriffsrechten an benutzerspezifische Sicherheitsfreigaben zu binden, die mit

entsprechenden Vertraulichkeitsstufen für Systemobjekte verknüpft sind (wie bspw. VS-NfD).

- Für den Zugriff auf Metadaten sollte bis auf Feldebene differenziert werden können, ob die jeweilige Information für den aktuellen Bearbeiter sichtbar, lesbar oder änderbar ist.

2.4.13 Mobile Vorgangsbearbeitung

Die Möglichkeit des ortsunabhängigen Arbeitens wird auch durch die Beschäftigten der öffentlichen Verwaltung (in der Projektarbeit wie auch in den Führungspositionen) zunehmend wahrgenommen. Voraussetzung ist der dezentrale Zugriff auf die für die Aufgabenerfüllung erforderlichen Daten und IT-Verfahren. Für das mobile Arbeiten ist es erforderlich, auf Dokumente und Vorgänge auch ohne Datenverbindung zugreifen zu können.

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

- Das System muss das Erstellen einer lokalen Kopie eines Schriftgutobjektes auf dem mobilen Endgerät in Verbindung mit Sperrung des Originals (Check-out) und die anschließende Synchronisierung bei erneuter Verbindung (Check-in) 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.
- Für die mobile Bearbeitung kopierte Schriftgutobjekte müssen auf dem jeweiligen Endgerät verschlüsselt gespeichert werden können.
- Kommunikationsverbindungen müssen eine Ende-zu-Ende-Verschlüsselung zwischen mobilem Client und dem zentralen Verfahren unterstützen.

Bestimmte Schriftgutobjekte – wie bspw. Personalakten, Beihilfeakten – sollten prinzipiell nur innerbehördlich und zentral bearbeitet werden, um die nach dem BDSG in der Anlage zu § 9 Satz 1 formulierten Maßnahmen (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Verfügbarkeitskontrolle) umsetzen zu können.

2.4.14 Hybridaktenführung

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

Aus Sicht des Datenschutzes sind hinsichtlich der Hybridaktenführung die folgenden Punkte relevant:

- Die Vollständigkeit des Bearbeitungskontextes der elektronischen Dokumente wie auch der Dokumente in Papier stellt eine Herausforderung dar – das Prinzip der Verfügbarkeit aller relevanten Informationen ist durch eine schwierig herzustellende gemeinsame Sicht auf die in der Akte enthaltenen Dokumente gefährdet (bspw. bei der Suche nach Schlagworten)

- Die automatisierte Steuerbarkeit der in der Akte enthaltenen Dokumente ist nur für den elektronischen Teil der Schriftgutobjekte gegeben und daher schwer synchron zu halten (bspw. bei Aussonderung oder Abgabe oder im Falle spezifischer Sicherheitsfreigaben)

2.4.15 Umstrukturierung des Aktenbestands (Umprotokollierung)

Umstrukturierungen der Aufbauorganisation einer Behörde erfordern i. d. R. auch die entsprechenden Umstrukturierungen des Aktenbestands. Als auslösende Szenarien seien die Umbenennung, Neubildung oder Auflösung von Organisationseinheiten mit Aufgabenübertragung genannt bzw. der Wechsel der übergeordneten Organisationseinheit, ggf. der Wechsel des Ressorts.

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

2.4.16 Langzeitspeicherung

Die Langzeitspeicherung bezeichnet die Aufbewahrung elektronischer Dokumente innerhalb des Zeitraums der Aufbewahrungsfrist in Verantwortung der aktenführenden Verwaltung vor Abgabe an das zuständige Archiv (siehe auch Kapitel 2.4.6).

Der Übergang 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 Metadaten, Protokoll- und Signaturdaten.[41]

Da elektronische Personalakten - wie in Kapitel 4 dargestellt - personenbezogene Informationen mit ggf. hohem Schutzbedarf enthalten sowie besondere Bedeutung für die Wahrung von Rechten (z.B. Pensions-, Renten- und Versorgungsansprüche) haben können, sind die o. g. Anforderungen an Verfügbarkeit und Integrität sowie an den Beweiswerterhalt im Sinne der Zivilprozessordnung (ZPO) bei der Langzeitspeicherung zwingend zu berücksichtigen.

[41] zu den Anforderungen an die Langzeitspeicherung vgl. Baustein E-Langzeitspeicherung des Organisationskonzeptes E-Verwaltung, Kapitel 3.4 ff.

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

In diesem Kapitel wird ein allgemeines Vorgehen bei der Erhebung der datenschutzrechtlichen Anforderungen und bei der Planung der Umsetzung entsprechender technischer und organisatorischer Maßnahmen beschrieben.

Die nachfolgende Grafik gibt einen Überblick über die dabei durchzuführenden Schritte. Eine Übersicht der zu erstellenden bzw. zu bearbeitenden Dokumente findet sich im Anhang in Kap. 0.

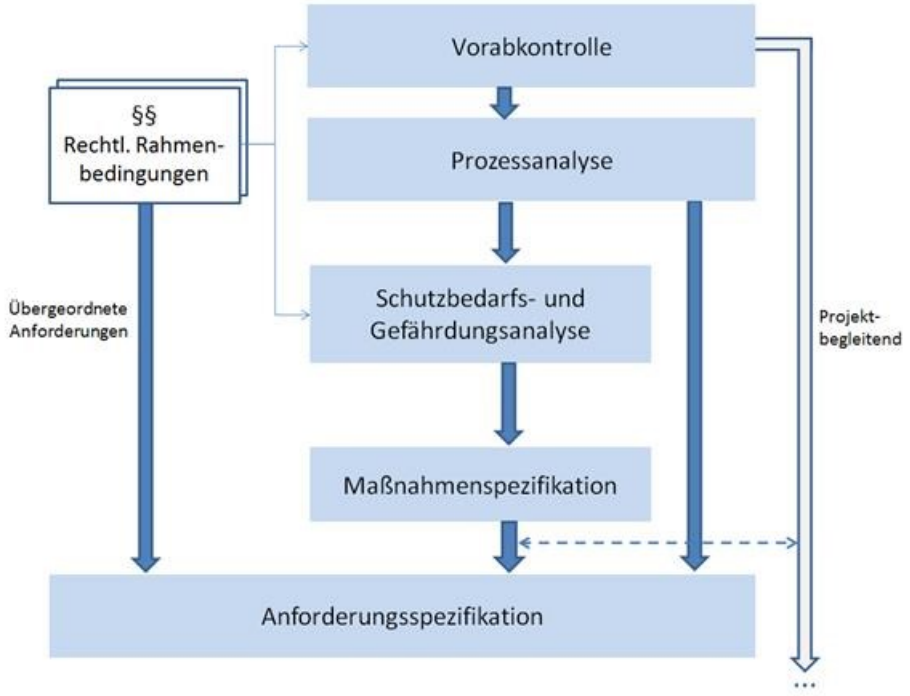

Abbildung 5: Prozessablauf - Planung und Umsetzung von Maßnahmen zum Datenschutz

In Einführungsprojekten im Bereich der elektronischen Verwaltungsarbeit ist für alle möglicherweise im jeweiligen Bereich anfallenden Arten personenbezogener Daten zu prüfen, ob sich die Zielstellungen des Datenschutzes im Sinne des BDSG in dem geplanten, elektronischen Verfahren verbindlich umsetzen lassen.

Dabei sind sowohl die Posteingänge und der (Papier-)Aktenbestand der Behörde als auch die Erfassung der Bearbeitungsprozesse der jeweiligen Schriftgutobjekte 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.

Es wird hierbei ausdrücklich ein Vorgehen nach der Systematik des IT-Grundschutzes (Schutzbedarf ermitteln, Maßnahmen definieren, Gefährdungen- und Risiken analysieren) unter Verwendung der entsprechenden Gefährdungs- und Maßnahmenkataloge empfohlen, siehe Kapitel 2.2.2, 3.3 und 4.7.4.

3.1 Grundlegende Prüfung der geltenden gesetzlichen und datenschutzrechtlichen Regelungen (Vorabkontrolle)

Generelles Ziel der Vorabkontrolle ist es, die Beherrschbarkeit neuer Informations- und Kommunikationsverfahren vor deren Einführung zu überprüfen. Mit ihr werden die Abläufe der automatisierten Datenverarbeitung transparent gemacht, Gefahren für die Rechte der betroffenen Personen aufgezeigt, Risiken abgeschätzt und Sicherheitskonzepte entworfen. Die Methodik ist auch geeignet, Lösungen für einen datenschutzgerechten Technikeinsatz zu finden.

Gerade bei Entwicklungs- und Einführungsprojekten kann die Vorabkontrolle nicht als einmalige, dem Projekt vorangestellte Aktivität angesehen werden, sondern stellt sich als komplexer, projektbegleitender Prozess dar. Die Einführung von IT-Verfahren ist häufig mit Änderungen der ursprünglichen Konzeptionen und Planungen verbunden, so dass auch die datenschutzrechtliche Bewertung der technischen und organisatorischen Maßnahmen entsprechend zu prüfen ist.

Die Vorabkontrolle sollte wie folgt gegliedert werden:

1. Systembeschreibung,
2. Rechtsgrundlage der Datenverarbeitung,
3. Schutzbedarfseinstufung,
4. Gefährdungs- und Risikoanalyse,
5. Informationssicherheitskonzept,
6. Beherrschung der Risiken.

Die datenschutzrechtlichen Grundlagen für die Vorabkontrolle sind in Kapitel 2.1.7 beschrieben.

Ein beispielhaftes Vorgehen bei der Vorabkontrolle für die Einführung der elektronischen Personalakte findet sich im Anhang 5.1.

3.2 Analyse des Prozessablaufs und der Prozessbeteiligten

Die Analyse des Prozessablaufs hat zum Ziel, aus fachlicher Sicht alle beteiligten Personen, Anwendungen[42], 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[43] benötigten Informationen.

Sinnvollerweise werden zunächst die bestehenden Arbeitsprozesse des ggf. papiergebundenen Verwaltungshandelns einer Behörde als Grundlage in einem Ist-Stand erfasst und dann im Rahmen der Sollkonzeption eines IT-gestützten, elektronischen Geschäftsgangs modelliert.

Hinweis

Nach dem Phasenmodell zur Einführung der elektronischen Verwaltungsarbeit (Baustein Projektleitfaden, Kapitel 4)[44] sind die Ist-Analyse und die Soll-

[42] Nach § 18 (2) BDSG haben die Bundesbehörden die Pflicht, ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen zu führen.

[43] Die einzelnen Schritte der Strukturanalyse werden im Detail in Kapitel 4.2 der IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2) in Form einer Handlungsanweisung beschrieben. Das Ergebnis der Strukturanalyse ist der vollständig modellierte Informationsverbund, auf den Maßnahmen zugeschnitten werden.

[44] http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/projektleitfaden.pdf

Konzeption in den Phasen Vor- und Hauptuntersuchung vorgesehen. Dies ist mit dem Vorgehen aus Sicht des Datenschutzes (Voruntersuchung und Planung von Maßnahmen) vereinbar. Ist-Analyse und Soll-Konzeption und die entsprechende Modellierung sind also als übergreifende Projektaufgaben zu sehen, innerhalb derer der Datenschutz als ein grundlegender Aspekt zu berücksichtigen ist.

Eine mögliche Notation zur Erfassung der Ist- und Soll-Prozesse ist die BMPN 2.0[45], mit deren Hilfe sich die verschiedenen Ebenen (fachliche Prozesse, Daten-Input und -Output, Akteure, Systeme, manuelle und automatisierte Aktivitäten) in einem Prozessmodell darstellen lassen.

Die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen, wird auch Informationsverbund genannt. Dieser definiert den Geltungsbereich des zu erstellenden Sicherheitskonzepts.

Die Modellierung der behördenspezifischen Abläufe ermöglicht im nächsten Schritt das Ableiten von Risiken und Maßnahmen wie in Kapitel 3.3.4 beschrieben.

3.2.1 Behördeninterne Abläufe

Die Prozessanalyse sollte möglichst alle von der Einführung des E-Akte-Systems betroffenen behördeninternen Bearbeitungsabläufe umfassen und dabei. die und dabei die spezifischen, datenschutzrechtlichen Fragestellungen berücksichtigen.

Ziel der Modellierung ist die Spezifikation von Anforderungen des Datenschutzes an den elektronischen Geschäftsgang, die Identifikation von Risiken und die Planung und Verortung technischer und organisatorischer Maßnahmen im Prozess. Beispielhaft sind die folgenden Fragen zu nennen:

- Welche Informationen und Dokumenttypen (bspw. Verträge, rechtsbildende Dokumente) sollen in der Behörde elektronisch erfasst und bearbeitet werden?
- Welche Metadaten erfordern die einzelnen Dokumenttypen?
- Wie soll die Posteingangsbehandlung und Digitalisierung (zentrale Post- und Scanstelle, Abteilungsscanstelle) 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 z.d.A.-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 im IT-Grundschutz[46] als „Komplexitätsreduktion durch Gruppenbildung“

[45] Business Process Model and Notation der OMG, http://www.omg.org/spec/BPMN/2.0/

[46] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf

bezeichnet wird und in BPMN 2.0 in der Verwendung von Subprozessen seine Entsprechung hat, siehe Kapitel 5.6..

Ein Beispiel für die Definition eines Sollprozesses der elektronischen Verwaltungsarbeit und der aus dem Prozessmodell abzuleitenden Fragestellungen in Bezug auf den Datenschutz findet sich im Anhang in Kapitel 5.6.

3.2.2 Beteiligung externer Stellen

Hinsichtlich der nachgelagerten Prozesse und der Beteiligung externer Stellen sind im Sinne des Datenschutzes für die einführende Behörde die Aktivitäten zu berücksichtigen, die Übergabepunkte im Sinne von Schnittstellen bezeichnen.

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

- Was sind die nachgelagerten Prozesse und 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?
- Auf welche Informationen bezieht sich ein Recht auf Einsichtnahme?
- Wie erfolgen Anbietung, Archivierung und Aussonderung?

Auch für die Beteiligung externer Stellen kann das Prozessmodell im Anhang in Kapitel 5.6 exemplarisch betrachtet werden. Es enthält zwei Schnittstellen zu zwei externen Prozessteilnehmern, dem zuständigen Archiv und einer anderen Behörde.

3.2.3 Prozessbeteiligte und Betroffene

In der Analyse sollen die prozessbeteiligten Organisationen, Personengruppen und Stellen (analog zu den oben genannten, internen und externen Prozessbeteiligten) erfasst und hinsichtlich ihrer Rolle und/oder Betroffenheit im Sinne des Datenschutzes eingeordnet werden. Einzelne Subprozesse sind zu diesem Zwecke weiter zu detaillieren, wie bspw. in dem oben genannten Beispiel der Subprozess „Anbietung und Abgabe“ zur Feststellung der beteiligten Akteure und Rollen.

Betroffene Personengruppen im Sinne des Datenschutzes 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 als Protokollinformationen erfasst werden und in IT-Systemen potentiell ausgewertet werden können (Leistungskontrolle)
- Bedienstete, deren personenbezogene Daten in elektronischen Personalakten geführt werden

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 verarbei-

tenden elektronischen Dokumente und Informationen im Zuge der oben beschriebenen Prozessanalyse.

3.3.1 Zweck der Schutzbedarfsanalyse

Wie bereits in Kap. 2.2 angeführt, geht es bei der Analyse des Schutzbedarfs elektronischer Dokumente und auch sonstiger im E-Akte-System erhobener, erzeugter und verarbeiteter personenbezogener Daten darum festzustellen, welche negativen Folgen im Falle der Offenlegung, der Verfälschung oder des Verlusts dieser Daten für den oder die Betroffenen entstehen könnten, inwiefern also das informationelle Selbstbestimmungsrecht des oder der Betroffenen dadurch beeinträchtigt würde.

Gemäß den Ausführungen in Kapitel 2.3 werden Primärdaten, Metadaten und Protokolldaten unterschieden. Für jeden dieser drei Datentypen 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 gemäß (§ 3 Absatz 9 BDSG) enthalten könnten. Dabei sollten auch die bereichsspezifischen Regelungen, wie z.B. Sozialrecht, Arbeitsrecht oder Personalrecht besondere Berücksichtigung finden.

Anhand der Schutzbedarfsanalyse ist es im Regelfall erst möglich, begründete Aussagen über Risiken der elektronischen Aktenführung zu treffen und darauf aufbauend Schutzmaßnahmen festzulegen und umzusetzen. Die Ergebnisse der Schutzbedarfsanalyse legen somit die Grundlage für die Erhebung datenschutzrechtlicher Anforderungen an das E-Akte-System, seine Betriebsumgebung sowie weitere organisatorische und personelle Nutzungsbedingungen und 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[47] kann je nach eingenommener Perspektive unterschiedlich skaliert werden.

Die DIN 66399 befasst sich ursächlich mit der Vernichtung von Datenträgern und fokussiert somit auf den Verlust von Vertraulichkeit als Schadenszenario. 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 Offenlegung und Missbrauch personenbezogener Daten und deren Folgen für den Betroffenen. Indem es fünf Schutzstufen unterscheidet, ist es etwas granularer als der DIN-Ansatz, erfasst damit aber ebenso nicht alle Aspekte der Schutzbedürftigkeit personenbezogener Daten.[48]

Der BSI-Standard 100-2 übernimmt in seiner (weiter gefassten) Szenarienbetrachtung den Begriff des informationellen Selbstbestimmungsrechts, der deutlich mehr umfasst als den Vertraulichkeits- und Missbrauchsschutz, und entspricht damit eher den Anforderungen des technisch-organisatorischen Datenschutzes (vgl. 2.1.9).

Der Vorteil besteht einerseits darin, dass das Schadensszenario *Beeinträchtigung des informationellen Selbstbestimmungsrechts* auf alle drei Schutzziele *Vertraulichkeit, Integrität und Verfügbarkeit* Anwendung findet, und andererseits, wie bereits in Kap. 2.2 festgehalten wurde, die Verletzung eines dieser Schutzziele bei der elekt-

[47] Siehe Kapitel 2.2.2 Schutzbedarf.

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

ronischen Aktenführung negative Auswirkungen auf das informationelle Selbstbestimmungsrecht des Betroffenen haben kann.

Abhängig von den Auswirkungen einer Offenlegung, Kompromittierung oder Missbrauch der entsprechenden personenbezogenen Daten werden dabei folgende Schutzbedarfskategorien betrachtet:

Schutzbedarfskategorie Normal:

der Betroffene kann in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden,

Schutzbedarfskategorie Hoch:

der Betroffene kann in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden,

Schutzbedarfskategorie Sehr hoch:

eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen kann gegeben sein.

Es wird empfohlen, die Schutzbedarfsanalyse nach der Methodik des BSI-Standards 100-2 durchzuführen.

Das bedeutet, entsprechend dem o. g. Vorgehen sollte in der Schutzbedarfsanalyse für die einzelnen Datentypen resp. Subtypen eingeschätzt werden, ob und in welcher Größenordnung der Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit der Daten das informationelle Selbstbestimmungsrecht der Betroffenen beeinträchtigen könnte. Dabei sind stets auch die **mittelbaren Folgen** einer Kompromittierung der Daten zu berücksichtigen.

3.3.3 Form der Schutzbedarfsanalyse

Die Schutzbedarfsanalyse wird am besten in tabellarischer Form dokumentiert. Nachfolgend ein Beispiel.

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 könnten aber nur mit erheblichem Aufwand gewährleistet werden.

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

Tabelle 1: Beispiel für eine Schutzbedarfsanalyse von Datenarten

3.3.4 Gefährdungsanalyse

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

Direkte Gefährdungen für den Datenschutz können entstehen, wenn die datenschutzrechtlichen Grundsätze aus Kapitel 2.1 nicht oder nur ungenügend eingehalten werden. Nachfolgend werden die unmittelbaren Gefährdungen unter Verweis auf die jeweils korrespondierenden Abschnitte in 2.1 tabellarisch erfasst.

Gefährdung	Gefährdete Schutzziele	Verweis
Fehlende Zulässigkeit der Verarbeitung perso-	Unverkettbarkeit	2.1.2

nenbezogener Daten		
Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten	Unverkettbarkeit	2.1.3
Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten	Unverkettbarkeit	2.1.5
Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten	Unverkettbarkeit	2.1.3
Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten	Vertraulichkeit	2.1.6
Fehlende oder nicht ausreichende Vorabkontrolle	alle	2.1.7
Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten	Intervenierbarkeit	2.1.11
Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten	Alle	2.1.9

Tabelle 2: Direkte Gefährdungen für den Datenschutz

Indirekte Gefährdungen für den Datenschutz können sich ergeben, wenn bei der Realisierung, beim Betrieb oder bei der Nutzung des E-Akte-Systems keine oder nur unzureichende technisch-organisatorischen Maßnahmen umgesetzt werden, um die Schutzziele entsprechend dem Schutzbedarf der Daten zu erreichen.

Um eine Liste der indirekten Gefährdungen zusammenzustellen, kann der Katalog der Elementargefährdungen aus den IT-Grundschutzkatalogen des BSI herangezogen werden. Nachfolgend werden exemplarisch einige indirekte Gefährdungen aus diesem Katalog unter Verweis auf die jeweils korrespondierenden Abschnitte in 2.1 aufgelistet.

Gefährdung	**Gefährdete Schutzziele**	**Verweis**
Verlust gespeicherter Daten	Verfügbarkeit, Transparenz, Intervenierbarkeit	2.1.9, 2.1.11
Überlastung von Informationssystemen	Integrität, Verfügbarkeit	2.1.9
Fehlfunktion von Geräten oder Systemen	alle	2.1.9, 2.1.11
Software-Konzeptionsfehler	alle	2.1.2, 2.1.3
Software-Schwachstellen oder -Fehler	alle	2.1.2, 2.1.3, 2.1.9
Ausspähen von Informationen / Spionage	Vertraulichkeit	2.1.6, 2.1.10
Abhören	Vertraulichkeit	2.1.6, 2.1.10
Sorglosigkeit im Umgang mit Informationen	Vertraulichkeit, Intervenierbarkeit	2.1.6
Missbrauch von Berechtigungen	alle	2.1.3, 2.1.4, 2.1.10

Tabelle 3: Beispiele indirekter Gefährdungen für den Datenschutz

3.4 Planung und Umsetzung von Maßnahmen

Die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes sind in einem auf das geplante elektronische Verfahren abgestimmten Datenschutz- und Datensicherheitskonzept (inkl. Rollen- und Rechtekonzept, Protokollierungskonzept) zu definieren.

Darin werden die spezifischen Gefährdungen und Maßnahmen für die Anwendung zur elektronischen Vorgangsbearbeitung und Aktenhaltung im Rahmen der definierten Soll-Prozessen behandelt (nicht betrachtet werden bspw. Maßnahmen in den Bereichen Netzwerksicherheit, Virenschutz etc.).

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

In diesem Abschnitt wird exemplarisch die Anwendung relevanter Schutzmaßnahmen im Rahmen des elektronischen Geschäftsgangs beschrieben. Die Auswahl orientiert sich an den Empfehlungen des IT-Grundschutzbausteins B 1.5 Datenschutz.[49]

Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten

Bei der Prüfung der rechtlichen Rahmenbedingungen als Voraussetzung der Datenverarbeitung müssen folgende Aspekte betrachtet werden:

- Prüfung, ob personenbezogene Daten verarbeitet werden,
- Zulässigkeit der Datenverarbeitung,
- Erforderlichkeit der Datenverarbeitung,
- Verwendung der Daten hinsichtlich der Zweckbindung,
- Verwendung der Daten hinsichtlich der besonderen Zweckbindung,
- Durchführung einer Vorabkontrolle.

Bei der Betrachtung dieser Aspekte sollte wegen eventuell schwieriger Rechtsmaterie, insbesondere zu Datenschutzfragen, auf juristische Unterstützung zurückgegriffen werden.

Im Rahmen der Vorabkontrolle ist vor dem erstmaligen Einsatz automatisierter Verfahren zur Bearbeitung personenbezogener Daten zu prüfen, welche Gefahren hierdurch für das informationelle Selbstbestimmungsrecht erwachsen können.

Es empfiehlt sich, die Vorabkontrolle auf der Grundlage eines IT-Sicherheitskonzeptes nach IT-Grundschutz vorzunehmen, in dem die Umsetzung

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

der erforderlichen technischen und organisatorischen Maßnahmen für das E-Akte-System dokumentiert ist.[50]

Hinweis

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.

Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

Entscheidend bei Planung und Durchführung der technischen und organisatorischen Maßnahmen ist, dass sie als ein zusammenwirkendes Schutzsystem verstanden werden. Ein solches Schutzsystem sichert neben dem rechtlich erforderlichen Datenschutz auch die ordnungsgemäße Aufgabenerfüllung und einen ordentlichen Betriebsablauf. 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 für die notwendigen Maßnahmen sollte in einem angemessenen Verhältnis zum angestrebten Schutzzweck und zum ermittelten Schutzbedarf stehen (vgl. § 9 BDSG).

Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten

Die bei der Datenverarbeitung beschäftigten Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten[51] bzw. darüber zu unterrichten. Die Verpflichtung zur Wahrung des Datengeheimnisses besteht auch nach Beendigung ihrer Tätigkeit fort. Die Verpflichtung/Unterrichtung muss in geeigneter Weise durchgeführt werden, die Durchführung ist zu dokumentieren und sollte bei Bedarf wiederholt werden.

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

Es sind technisch-organisatorische Verfahren zu entwickeln, um die Durchsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht in Dateien- bzw. Verfahrensverzeichnisse (soweit solche Verzeichnisse vorgeschrieben sind) sicherzustellen.

Diese Verfahren sollen so beschaffen sein, dass die Rechte der Betroffenen schnell und zweckmäßig umgesetzt werden können.

Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten

Automatisierte Abrufverfahren werden als eine Phase der Datenverarbeitung definiert, bei der gespeicherte oder durch Datenverarbeitung gewonnene personenbe-

[50] 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.

[51] Mit Blick auf Satz 2 § 5 BDSG ist eine Verpflichtung für Personen relevant, die bei nicht-öffentlichen Stellen beschäftigt werden. Ggf. kann eine Empfehlung ausgesprochen werden, ungeachtet dessen eine Belehrung des Personals (on top) durchzuführen

zogene Daten an einen Dritten in der Weise bekannt gegeben werden, dass die Daten durch die datenverarbeitende Stelle zum Abruf bereitgestellt werden und der Abruf durchgeführt wird.

Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger.

Für die Einrichtung eines automatisierten Abrufverfahrens sind die besonderen Zulässigkeitsvoraussetzungen in den einschlägigen Gesetzen dargestellt. Zur Kontrollierbarkeit der Zulässigkeit sind die wesentlichen Details des Abrufverfahrens schriftlich festzulegen.

Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten

Wenn das E-Akte-System von einem öffentlich-rechtlichen oder ggf. privaten Dienstleister betrieben wird, ist der Tatbestand der Auftragsdatenverarbeitung gegeben (siehe § 11 BDSG / Kapitel 2.1.10).

Werden personenbezogene Daten im Auftrag verarbeitet, bleibt der Auftraggeber für die Einhaltung der Gesetze und Vorschriften über den Datenschutz verantwortlich. Er hat den Auftragnehmer sorgfältig auszuwählen.

Je nachdem, wie schutzbedürftig die personenbezogenen Daten sind, die im Auftrag verarbeitet werden sollen, sind die Anforderungen an den Vertrag mit dem Auftragnehmer zu stellen: Je schutzbedürftiger, umso enger und präziser der Auftrag. Bei besonders sensiblen Verarbeitungen kann sich eine Vergabe an Außenstehende verbieten (z. B. Fahndungsdaten).

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 der IT-Anwendung vorgesehenen Werkzeugen (z. B. Script-Sprachen, SQL-Editoren) auf Datenbankinhalte zuzugreifen. Damit lassen sich Informationen abfragen und aggregieren sowie Auswertungen vornehmen, die in der IT-Anwendung so nicht vorgesehen und ggf. datenschutzrechtlich unzulässig sind.

Die Daten, auf die mit solchen Werkzeugen zugegriffen werden soll, und die zu eröffnenden Abfragearten müssen vorab geprüft werden.

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.

Datenschutzaspekte bei der Protokollierung

Unter Protokollierung beim Betrieb von IT -Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: "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?"

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

Benutzeraktivität	Anforderungen an die Protokollierung
Eingabe von Daten	Die so genannte Eingabekontrolle erfolgt grundsätzlich verfahrens-

	orientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, dass Befugnisüberschreitungen anderweitig protokolliert werden, dürfte eine vollständige Protokollierung von Dateneingaben als Regelfall angesehen werden müssen.
Datenübermittlungen	Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, kann eine selektive Protokollierung als ausreichend angesehen werden.
Benutzung von automatisierten Abrufverfahren	In der Regel dürfte eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich sein, 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	Dies kann erforderlich sein bei besonders "sensiblen" Programmen, die z. B. nur zu bestimmten Zeiten oder Anlässen benutzt werden dürfen. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

Tabelle 4: Anforderungen an die Protokollierung aus Sicht des Datenschutzes

Die Effektivität der Protokollierung und ihre Auswertung im Rahmen von Kontrollen hängen im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang sollten folgende Aspekte Berücksichtigung finden:

- Es sollte ein Konzept erstellt werden, 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 werden wie die Manipulationssicherheit der Einträge in Protokolldateien.
- Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden.
- 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 sollten so zeitnah durchgeführt werden, dass bei aufgedeckten Verstößen noch Schäden abgewendet sowie Konsequenzen gezogen werden können. Kontrollen müssen rechtzeitig vor dem Ablauf von Löschungsfristen von Protokolldateien stattfinden.
- Kontrollen sollten nach dem Vier-Augen-Prinzip erfolgen.
- Die Mitarbeiter sollten darüber informiert sein, dass Kontrollen durchgeführt werden, ggf. auch unangekündigt.
- Für Routinekontrollen sollten automatisierte Verfahren verwendet werden.
- Personalräte sollten bei der Erarbeitung des Protokollierungskonzeptes und bei der Festlegung der Auswertungsmöglichkeiten der Protokolle beteiligt werden.

Aufrechterhaltung des Datenschutzes im laufenden Betrieb

Die interne Datenschutzkontrolle, die meist dem Datenschutzbeauftragten obliegt, überprüft die Einhaltung der aus den Datenschutzgesetzen herrührenden Anforderungen. Dazu gehören:

- die Kontrolle der Verfahren auf Einhaltung der Rechtsgrundlage und der Zweckbestimmung,
- die Sicherstellung der Rechte des Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung und Schadensersatz,
- die Unterrichtung über bzw. die Verpflichtung der Mitarbeiter auf den Datenschutz,
- das Führen von Datei- bzw. Verfahrensübersichten und Geräteverzeichnissen und
- die Kontrolle der aus den gesetzlichen Vorschriften abgeleiteten technisch-organisatorischen Maßnahmen zur Kontrolle von Zutritt, Zugang, Zugriff, Weitergabe, Eingabe, Auftrag, Verfügbarkeit und "getrennter Verarbeitung gemäß der Zweckbestimmung".

Datenschutzgerechte Löschung/Vernichtung

Sowohl aus der Sicht des Datenschutzes als auch der Informationssicherheit ist beim Löschen von sensiblen oder vertraulichen Daten auf magnetischen Datenträgern zu gewährleisten, dass die Daten sicher, d. h. vollständig und unumkehrbar gelöscht werden. Der Zustand, in dem die Unterlagen als vernichtet gelten können, ist festzulegen.

Als Orientierung kann hierzu die Norm DIN 66399 (Vernichten von Datenträgern) herangezogen werden. Hiernach reicht es aus, wenn die Informationsträger so vernichtet werden, dass die Reproduktion 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 liegt immer dann vor, wenn die Schutzbedarfsfeststellung entsprechend der BSI-Methodik einen hohen oder sehr hohen Schutzbedarf ergeben hat oder entsprechend DIN 66399 Daten der Schutzklassen 2 oder 3 verarbeitet werden.

In jedem Fall besteht ein erhöhter Schutzbedarf dann, wenn besondere personenbezogene Daten nach § 3 Absatz 9 BDSG erhoben, verarbeitet, gespeichert oder übermittelt werden.

Verwendung von TLS/SSL

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

Bei erhöhtem Schutzbedarf der verarbeiteten personenbezogenen Daten sollten die Datenkommunikationsverbindungen mittels des Sicherheitsprotokolls TLS/SSL (Transport Layer Security/Secure Socket Layer) verschlüsselt werden.

Das BSI hat hierzu 2013 einen „Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung“[52] veröffentlicht, der einzuhalten ist.

[52] https://www.bsi.bund.de/DE/Publikationen/Mindeststandards/SSL-TLS-Protokoll/SSL-TLS-Protokoll_node.html

Datenbank-Verschlüsselung

Werden personenbezogene Daten mit sehr hohem Schutzbedarf bzw. der Schutzklasse 3 im Sinne von DIN 66399 verarbeitet, kann es notwendig sein, diese Daten in der Datenbank zu verschlüsseln.

Dabei kann zwischen einer Online- und einer Offline-Verschlüsselung unterschieden werden:

- Bei einer Online-Verschlüsselung werden die Daten während des laufenden Betriebs ver- und entschlüsselt, ohne dass die betroffenen Benutzer davon etwas merken. Dafür können Tools eingesetzt werden, mit denen entweder auf Betriebssystemebene die gesamte Festplatte verschlüsselt wird, oder solche, mit denen nur die Anwendungsdaten der Datenbank verschlüsselt werden.
- Bei einer Offline-Verschlüsselung werden die Daten erst nach ihrer Bearbeitung verschlüsselt und vor ihrer Weiterverarbeitung wieder entschlüsselt. Dies wird im Allgemeinen mit Tools durchgeführt, die nicht in das Datenbanksystem integriert sind, und kann insbesondere für Datensicherungen oder Datenübertragungen sinnvoll sein. Dabei ist zu beachten, dass genügend Platz auf der Festplatte vorhanden ist, da die Ver- bzw. Entschlüsselung nur dann erfolgreich ausgeführt werden kann, wenn auf der Festplatte genügend Platz für das Original und die verschlüsselte Version der Datenbank verfügbar ist.

Darüber hinaus besteht die Möglichkeit, Daten weiterhin im Klartext in der Datenbank abzuspeichern, beim Zugriff über ein Netz jedoch eine verschlüsselte Datenübertragung zu realisieren (vgl. TLS/SSL).

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

Falls die Anforderungen durch keine der am Markt verfügbaren Datenbank-Standardsoftware abgedeckt werden können, sollte man den Einsatz von Zusatzprodukten prüfen, um die entsprechende Sicherheitslücke zu schließen.

3.5 Anforderungsspezifikation

Die nachfolgenden Anforderungen an E-Akte-Systeme sind als Ergänzung des im Baustein „Projektleitfaden“ genannten Anforderungskatalogs in Kapitel 7.2.3 zu verstehen. Die Aufstellung nennt exemplarisch typische Anforderungen und deren Beitrag zur Sicherstellung der Schutzziele des Datenschutzes und erhebt keinen Anspruch auf Vollständigkeit. Sie muss entsprechend der jeweiligen Sollkonzeption des einzuführenden Systems ausgeprägt und bewertet/priorisiert werden).

Nr.	Bezeichnung	Beschreibung	Schutzziele
FA-001	Anzeige von OE und Stellenkürzel	Das System muss die Anzeige von OE und Stellenkürzel 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 Aktenbetreff, Aktenplaneintrag, OE, Anzahl Vorgänge etc. unterstützen, um so fehlerhaften Zuordnungen elektronischer Dokumente zu Akten und Vorgängen vorzubeugen.	Vertraulichkeit

Nr.	Bezeichnung	Beschreibung	Schutzziele
FA-003	Keine Auswahlmöglichkeit zdA-verfügter Vorgänge	Das System darf zdA-verfügte Vorgänge in Dialogen zur Registrierung von Posteingängen nicht anzeigen, damit fehlerhafte Zuordnungen elektronischer Dokumente zu Akten und Vorgängen vormieden werden.	Integrität
FA-004	Protokollierung von Änderungen	Alle Änderungen von Primär- und Metadaten von Schriftgutobjekten sind durch das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Integrität, Transparenz
FA-005	Protokollierung lesender Zugriffe	Lesende Zugriffe auf von Primärdaten sind durch 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) sind durch das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Vertraulichkeit, Integrität, Transparenz
FA-007	Protokollierung von Löschungen	Löschungen elektronischer Schriftgutobjekte sind durch das System mit Bezug auf Sozial-, Zeit- und Sachebene zu protokollieren.	Integrität, Verfügbarkeit, Transparenz
FA-008	Protokollierung der Registrierung	Alle Zuordnungen elektronischer Posteingänge zu Vorgängen und Akten sowie Änderungen in der Zuordnung elektronischer Schriftgutobjekte zu elektronischen Akten sind durch 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 sind durch 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	Die Einnahme von Stellvertretungen und die in Stellvertretung vorgenommenen Änderungen an Schriftgut sind durch 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 u. a.) sind in den jeweils übergeordneten Objekten verfügbar zu halten.	Integrität, Transparenz

Nr.	Bezeichnung	Beschreibung	Schutzziele
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 Signaturschlüssel). (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) übertragen werden können. (Das diesbezügliche Verhalten sollte systemweit konfigurierbar sein.)	Integrität
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 fristengesteuerter Workflows bieten (bspw. für Transfer- und Aufbewahrungsfristen). (Die Funktionalität kann entscheidend dazu beitragen, dass Schriftgutobjekte mit personenbezogenen Informationen nicht länger als erforderlich im System vorgehalten werden.)	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 im Rahmen der Abgabe an die Archivbehörde die elektronisch verschlüsselten Dokumente mit Angabe des Verfassers und des Datums im Klartext lesbar übergeben werden.	Verfügbarkeit

Nr.	Bezeichnung	Beschreibung	Schutzziele
FA-022	Berechtigungen für Aussonderung und Löschung	Für die Aussonderung und das Löschen von Schriftgut müssen Benutzer- bzw. Rollenberechtigungen explizit vergeben werden können.	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	Berechtigungen i. S. von Objektrechten müssen für Schriftgutobjekte differenziert nach Erstellen, Lesen, Suchen, Ändern und Löschen vergeben werden können.	Vertraulichkeit, Unverkettbarkeit
FA-025	Vorbelegung von Objektrechten und Metadaten im Aktenplan	Für einzelne Bereiche des Aktenplans müssen Standard-Objektrechte und Werte für Metadatenfelder (insbes. Aufbewahrungsfrist, Bewertung des Archivs, etc.) vorbelegt werden können.	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
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 der 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

Nr.	Bezeichnung	Beschreibung	Schutzziele
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)[53] von personenbezogenen Informationen im elektronischen Dokument soll möglich sein.	Vertraulichkeit

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

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

4 Besonderheiten bei der Einführung elektronischer Personalakten

In diesem Kapitel wird das Szenario der Einführung einer elektronischen Personalakte betrachtet. Dabei wird Bezug zu dem im Baustein „Projektleitfaden“ in Kapitel 4 beschriebenen Phasenmodell zur Einführung der elektronischen Verwaltungsarbeit genommen[54]. Die Planung der datenschutzrechtlichen Maßnahmen erfolgt nach diesem Modell in den Phasen „Voruntersuchung“ und „Hauptuntersuchung“, die Umsetzung entsprechend in den nachfolgenden Phasen.

Eine Zuordnung der Aktivitäten des Datenschutzes zum genannten Phasenmodell findet sich im Anhang, im Kapitel 0.

Für elektronische Personalakten (eP-Akten) sind neben den allgemeinen datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes (BDSG) insbesondere die Regelungen des Bundesbeamtengesetzes (BBG) und Bundespersonalvertretungsgesetzes (BPersVG) relevant[55]. Für die Landesverwaltungen sind zudem noch das Beamtenstatusgesetz (BeamtStG), die Landesbeamtengesetze sowie die Landespersonalvertretungsgesetz zu beachten. Im Bereich der Tarifbeschäftigten ist § 3 Abs. 5 TVöD zu berücksichtigen. Die rechtlichen Grundlagen sind in den Kapiteln 2.1 und 2.1.13 beschrieben.

Bei Personalakten handelt es sich um Akten mit in der Regel deutlich längeren Laufzeiten im Vergleich zu der Mehrzahl der Sachakten, d.h. die sichernden Maßnahmen müssen 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. Disziplinaria u. a. m.) hinweg betrachtet – zahlreichende mitwirkende Stellen involviert. Hierbei ist auf die Zuweisung und Verwaltung von geeigneten Zugriffsrechten zu achten.

Die (vollständige) elektronische Personalaktenführung kann folgende Funktionalitäten gewährleisten:

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

Darüber hinaus sind durch eine Digitalisierung von Personalakten weitere Effizienz- und Qualitätseffekte durch die Verkürzung der Bereitstellungs- und somit der Gesamtbearbeitungszeiten.

Neben den Besonderheiten der Personalaktenführung sind bei der Einführung einer elektronischen Personalakte auch die allgemeinen Grundsätze zur Einführung einer elektronischen Akte zu beachten. Daher ist auch hier der Projektleitfaden des Organisationskonzepts elektronische Verwaltungsarbeit zu berücksichtigen. Dieser gibt einen ganzheitlichen Überblick auf die organisatorischen Fragestellungen und Probleme“.[56]

[54] http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/projektleitfaden.pdf?__blob=publicationFile&v=1

[55] Für Soldatinnen und Soldaten ist zudem §29 SG in Verbindung mit der SPersAV und BPersVG relevant.

[56] Organisationskonzept elektronische Verwaltungsarbeit – Projektleitfaden, S. 6.

Dem Phasenmodell des Projektleitfadens folgend, werden nachstehend die Besonderheiten bei der Einführung einer elektronischen Personalakte hervorgehoben.

4.1 Projektinitialisierung

Die Projektinitialisierungsphase unterscheidet sich mit den Aufgaben der Zieldefinition und der Konkretisierung des Projektauftrags sowie der groben Projektplanung nicht von Projekten zur Einführung allgemeiner elektronischer Verwaltungsakten. Grundlegend ist auch bei der Einführung der elektronischen Personalakte die Entscheidung zu treffen, ob, wann und für welche (Teil-)Prozesse eine elektronische Vorgangsbearbeitung für eine elektronische Akte eingeführt werden soll. Daraus ergeben sich die Auswahl der vorzubereitenden Maßnahmen sowie deren zeitliche Abfolge.

4.2 Voruntersuchung

Die Phase der Voruntersuchung dient der Konkretisierung des Vorhabens hinsichtlich der Zielstellung, der Ausprägung des Prinzips der elektronischen Personalaktenführung (etwa hinsichtlich der Anbindung von Fachverfahren) sowie der Einführungsstrategie.

In der Phase der Voruntersuchung beginnt außerdem die nach dem in Kapitel 3.1 beschriebene Prüfung der geltenden gesetzlichen und datenschutzrechtlichen Regelungen für das Vorhaben (Rechtsgrundlage der Datenverarbeitung) im Rahmen der Vorabkontrolle durch den Datenschutzbeauftragten.

Die Vorabkontrolle ist insbesondere bei Einführung der elektronischen Personalakte verpflichtend durchzuführen, weil in der Personalakte auch besondere Arten personenbezogener Daten (nach § 3 Abs. 9 BDSG) verarbeitet werden (vgl. § 4d Absatz 5 Satz 2 BDSG).

4.3 Weitere fachliche Beteiligungen

Es soll geklärt werden, welche internen Festlegungen und Vereinbarungen über die formalen Vorschriften hinaus bereits existieren und welche betroffene Bereiche zusätzlich zu den Mitgliedern der Projektgruppe – in der Regel nur temporär - zu Auskünften über die Arbeitsabläufe und Prozessanforderungen einbezogen werden können, um den unverzichtbaren fachlichen Input aus den operativen Bereichen zu erhalten. Dies können u.a. sein:

- personalverwaltende Behördenbereiche zu grundsätzlichen Fragen der Aufbau- und der Ablauforganisation bzw. dienstvorgesetzte Behördenbereiche (falls abweichend von personalverwaltender Behörde) zu 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 die Beamtin oder den Beamten zuständig sind.[57]

[57] Nebenakten enthalten ausschließlich Unterlagen, die sich bereits in der Grundakte oder Teilakte befinden. Das bedeutet, dass Kopien aus z. B. einer 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 zur Führung einer Nebenakte nicht mehr besteht, muss zur Wahrung der Vertraulichkeit die Nebenakte aufgelöst bzw. vernichtet werden.

- Personalvertretung, z.B. um in das Projekt die Verfahrensweise bei einer Einsichtnahme einzubringen, die mit Zustimmung und zur Unterstützung eines Beschäftigten nach § 69 (2) BPersVG erfolgen kann.
- Personalverwaltung (hauptaktenführende, teilaktenführende und nebenaktenführende Stelle) zur Darstellung der operativen und ergonomischen Anforderungen sowie ggf. weitere Interessensvertretungen
- Gleichstellungsbeauftragte/r
- Datenschutzbeauftragte/r
- Innenrevision
- Besoldungs- bzw. Versorgungsstellen
- Zuständige für (amts-)ärztliche Unterlagen
- IT-Betrieb

4.4 Erstellung eines Anforderungskatalogs

In dem auf den Analyse-Ergebnissen aufbauenden Anforderungskatalog sollten u.a.

- die erforderliche Aktenstruktur (inkl. der jeweiligen Zugriffsberechtigungen) beschrieben sein, die bei Personalakten detailliert geregelt ist und meist die folgenden Teilakten oder Registerbereiche enthält
    - Verwendungs- und Laufbahnvorgänge
    - Beurteilungen
    - Urlaub, Arbeits- und Dienstbefreiung
    - Aus- und Fortbildung
    - Krankheit / Gesundheit
    - Besoldung
    - Versorgung
    - Disziplinarvorgänge
    - Beihilfe / Heilfürsorge
    - Nebentätigkeiten
    - Dienstunfälle
- die vorkommenden Dokumententypen mit ihren jeweiligen rechtlichen Anforderungen (Beweiswert, Fristen etc.) beschrieben sein
- die Soll-Geschäftsprozesse mit ihren besonderen Anforderungen beschrieben sein, z.B.
    - gesonderte Posteingangsbehandlung (bspw. bei personalaktenrelevanten Dokumenten ungeöffnetes Weiterleiten aus der zentralen Poststelle und Nachscannen im Personalreferat)
    - erforderliche Recherchen und die dafür benötigten Such-Parameter (Primärdaten, Metadaten) sowie die für den Personalaktenbestand geltenden Beschränkungen
    - Maßnahmen zum Erhalt des Beweiswertes beim Einscannen von Papierdokumenten[58]
    - Einsichtnahme durch die Betroffenen

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

- besondere Anforderungen an die Protokollierung von Löschungen bzw. ggf. an die Vermeidung der Protokollierung für bestimmte Teilakten (wie bspw. Disziplinarangelegenheiten[59]) der elektronischen Personalakte behandelt werden
- weitere besondere Anforderungen an die Protokollierung (bspw. Protokollierung lesender Zugriffe für bestimmte Dokumente bzw. Teilakten) definiert werden[60]
- Anbindung an bestehende Fachverfahren für die Verwaltung von Personaldaten.

4.5 Einführungsstrategie

In der Wahl der Einführungsstrategie sind folgende Rahmenbedingungen zu beachten:

- der Grundsatz der Einheit und Eindeutigkeit der Personalakte
- das Gebot der Datensparsamkeit und
- der Grundsatz der Erforderlichkeit.

Daher ist es z. B. unzulässig, neben der elektronischen Personalakte Vorgänge parallel in Papier zu führen. Für die Überführung in die elektronische Personalaktenführung ermöglicht das Gesetz jedoch eine sukzessive Umstellung, indem es zulässt, dass die Akten ggf. auch nur teilweise in Papierform weitergeführt werden (§ 106 Abs. 1 Satz 3 BBG, § 106 Abs. 2 S. 5 BBG). Voraussetzung dafür ist, dass vorher eindeutig festgelegt wird, welche Teile in welcher Form geführt werden, so dass keine Aktenteile parallel in beiden Formen vorhanden sind. 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

Gemäß § 7 der Bundeshaushaltsordnung (BHO) für alle finanzwirksamen Maßnahmen angemessene Wirtschaftlichkeitsuntersuchungen durchzuführen. Eine methodische und inhaltliche Unterstützung für die Umsetzung der BHO und der dazu erlassenen Vorschriften auf die speziellen Erfordernisse der Informationstechnik bietet die „Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT“[61]. Wie darin beschrieben, sollten bei einer Wirtschaftlichkeitsbetrachtung neben den monetären Kriterien, wie z.B. der Arbeitszeitersparnis durch die hohe Verfügbarkeit, insbesondere auch die Kriterien aus den folgenden Bereichen angemessene Berücksichtigung finden:

- „Ermittlung der Ablösedringlichkeit des Altsystems[62]“. Hierbei sind die Vorgaben des E-Government-Gesetzes zu berücksichtigen.[63]

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

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

[61] Abrufbar auf der Seite der CIO Bund, http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/Wirtschaftlichkeitsbetrachtungen/wirtschaftlichkeitsbetrachtungen_node.html

[62] Hinweis: In diesem Sinne ist auch eine papierbasierte Personalaktenregistratur als Altsystem zu verstehen.

[63] 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 bzw. den Minikommentar des BMI zum Gesetz unter http://www.gesetze-im-internet.de/bundesrecht/egovg/gesamt.pdf

- „Ermittlung des qualitativ-strategischen Nutzens“, der bei Personalakten in der Möglichkeit liegt, angesichts der hohen schutzrechtlichen Anforderungen in Verbindung mit der großen Anzahl der gleichartigen Akten in diesem Bereich ein großes Effizienzpotential zu heben und IT-gestützt standardisiert zu bearbeiten.
- „Ermittlung der externen Effekte“, die im Bereich der Personalakten zwar naturgemäß eher gering sind, da es für Personalakten nur in sehr eng definierten Geschäftsfällen eine Weitergabe nach Außen geben kann. Dennoch sind folgende Szenarien als „extern“ aus der Sicht der Personalaktenverwaltung zu betrachten:
    - Einsichtnahme von Beschäftigten oder deren Bevollmächtigten in die eigene Personalakte
    - Bereitstellung von Personalakten oder Teilen von Personalakten im Rahmen von behördenübergreifenden Bewerbungen oder Abordnungen

4.7 Hauptuntersuchung

In der Hauptuntersuchung werden in einer umfassenden Ist-Analyse alle organisatorisch-fachlichen, alle organisatorisch-technischen sowie die rein technischen Fragen und Anforderungen geklärt.[64]

4.7.1 Ausführliche Ist-Analyse inkl. Schwachstellenanalyse

Entsprechend den Ergebnissen der Voruntersuchung werden die Anforderungen detailliert ermittelt.

- Organisation der Schriftgutverwaltung:
    - Besondere Registratur der Personalverwaltung
    - besondere Schriftgutobjekte (z.B. Grund-, Teil-, Nebenakte)
    - 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[65]
    - Formierung der Akten (Teilaktenstruktur, Registerbildung, Inhaltsverzeichnis, Paginierung etc.)
    - besondere Dokumententypen (z.B. „ärztlicher Umschlag“)
- Allgemeiner Geschäftsgang
    - Identifizierung und Profilierung der Prozessbeteiligten und Betroffenen
        - Beschäftigte und deren Angehörige (Versorgungsfälle), zu denen die Personalakte geführt wird
        - Mitglieder der Personalvertretung (mit Zustimmung des Beschäftigten) (§ 69 (2) BPersVG
        - Leitungen der personalverwaltenden Behördenbereiche

[64] siehe dazu im Baustein Projektleitfaden, S. 37-39.

[65] siehe Ausführungen zur Nebenakte in Anm. 51

        - Leitungen der dienstvorgesetzten Behördenbereiche (ggf. abweichend von personalverwaltender Behörde)
        - sachbearbeitende Stellen der Personalverwaltung (grundaktenführende, teilaktenführende, 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, differenziert nach Recherchieren, Lesen, Bearbeiten (ggf. differenziert nach Bearbeitung, Verfügung und Ablage), Löschen

- Bearbeitung

    - 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)
    - Trennung der Aktenführung von den Workflows der Personalbewirtschaftung, die z.B. in Fachverfahren erfolgen
    - Persönliche Identifizierung gemäß dem Rollen- und Berechtigungskonzept für einzelne Zugriffe und/oder Bearbeitungen (über eine initiale Anmeldung am System hinaus)
    - Erstellung detaillierter Handlungsanweisungen und Verfahrensbeschreibungen
    - Unterbindung einer aktenübergreifenden Suche
    - Elektronische Akteneinsicht durch Beamte/Beamtinnen oder Bevollmächtigte (§ 110 Abs. 1 BBG), Beschäftigte oder Bevollmächtigte (§ 3 Abs. 5 TVöD)

- Postausgang

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

- Termine, Wiedervorlagen

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

- 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)
    - Wegen der besonderen Bedeutung für die Wahrung von Rechten (z.B. Pensions-, Renten- und Versorgungsansprüche) und wegen der langen Zeiträume, aus denen beweissichere Daten ggf. zur Verfügung stehen müssen, hat der Stellenwert des Beweiswerterhalts im Sinne der Zivilprozessordnung (ZPO) eine hohe Priorität. In diesem Kontext ist insbesondere beim ersetzenden Scannen, der Datenhal-

tung sowie bei der Langzeitspeicherung[66] und Archivierung auf den Beweiswerterhalt zu achten.

- Aussonderung, Entfernung, Löschung
    - Löschungsgebot von Einzeldokumenten in der Akte: Die Personalaktenführung erfordert die Löschung bestimmter Dokumententypen (z.B. Erkrankungen) nach definierten Fristen[67], im Gegensatz zu den sonstigen Verwaltungsakten, bei denen das Löschen von Einzeldokumenten prinzipiell nicht bzw. nur in einzelnen zu begründenden Ausnahmefällen möglich sein darf.
        - Dabei darf die Berechtigung, Inhalte der elektronischen Personalakte zu löschen, nur ein sehr eingeschränkter Personenkreis haben (die Einführung organisatorischer Regelungen wie bspw. das Vier-Augen-Prinzip ist zu prüfen).
        - Auch bei einer Vereinbarung über ein automatisiertes Löschen sollte die Bestätigung durch einen Verantwortlichen erfolgen.
        - In einer Datenbank-gestützten elektronischen Personalakte 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 eine vollständige physische Vernichtung der elektronischen Dokumente erfolgen muss.
        - Auch über die Löschung muss es ein Protokoll geben, das den löschenden Mitarbeiter identifiziert, das Löschungsdatum und die Uhrzeit enthält und die Dokumentenart des gelöschten Dokuments nennt. Die Aufbewahrungsfrist des Protokolls ist zu vereinbaren.
    - Beschreibung zu berücksichtigender Rahmenbedingungen für Anbietung von Personalakten an das Bundesarchiv, Aussonderung und Löschung inkl. evtl. bestehender Nebenakten.
    - 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[68]

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

Aus der skizzierten Ist-Analyse lässt sich eine Schwachstellenanalyse ableiten, die neben allgemeineren möglichen Defiziten wie unzureichende Verfügbarkeit (lange Akten-Beschaffungswege, Wartezeiten etc.), vermeidbare Bearbeitungsstationen

[66] Vgl. Baustein E-Langzeitspeicherung des Organisationskonzeptes E-Verwaltung.

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

[68] Siehe dazu die „Informationen zur Aussonderung und Abgabe von Personalunterlagen der Bundesverwaltung“ des Bundesarchivs, http://www.bundesarchiv.de/fachinformationen/02544/index.html.de

oder uneinheitliche Aktenformierung insbesondere auf die vollständige Erfüllung der besonderen rechtlichen Anforderungen der Personalaktenführung ausgerichtet ist (vgl. Kap. 2.1.13).

4.7.2 Erstellung eines Fachkonzepts

In der Konzeptionsphase werden die erkannten besonderen Anforderungen der elektronischen Personalakte in der Spezifikation der Anforderungen an die Schriftgutverwaltung und den Geschäftsgang sowie der Spezifikation der Sollprozesse berücksichtigt.

- Spezifischer Posteingangsprozess / Scanprozess
- Zugriff / Rollen- und Berechtigungskonzept; ggf. Differenzierung nach Teilakten
- Berücksichtigung besonderer Ermächtigungen / Aufgabenverteilungsplan
- Besondere Schriftgutobjekte („ärztlicher Umschlag“)
- Besondere Formierung der Akte
- Besonderheiten der Altregistratur
- Besonderheiten der Aussonderung, Entfernung, Löschung
- Anbindung von/an Fachverfahren

Insbesondere die Nutzung von Fachverfahren im Personalbereich stellt hinsichtlich des Verhältnisses der dort geführten Personaldaten zu den in einer Personalakte geführten Dokumenten eine besondere Herausforderung unter dem Aspekt der Datensparsamkeit und Vermeidung von Datenredundanzen dar.

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

4.7.3 Vorabkontrolle

Die Durchführung der Vorabkontrolle bei Einführung der elektronischen Personalakte erfolgt in mehreren Schritten und als übergreifender Prozess – wie in Kap. 3.1 dargestellt. Die meisten Aktivitäten fallen in die Phase der Hauptuntersuchung.

Als Ergebnis aus der Phase Voruntersuchung muss vorliegen:

- Rechtsgrundlage der Datenverarbeitung

Die folgenden Aktivitäten des Datenschutzes sind in der Hauptuntersuchung durchzuführen bzw. fertigzustellen:

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

Ein beispielhaftes Vorgehen bei der Umsetzung einer Vorabkontrolle für die elektronische Personalakte findet sich im Anhang in Kapitel 5.1.

Als Hilfsmittel zur Durchführung der Vorabkontrolle findet sich auf den Seiten der BfDI zudem eine Checkliste.[69]

4.7.4 Schutzbedarfsanalyse

Die Feststellung des Schutzbedarfs von Personalakten folgt der unter 3.3 beschriebenen Methodik.

Beispielhafte Schadensszenarien wirtschaftlicher und/oder gesellschaftlicher Art im Rahmen eines Bewerbungs- oder Beförderungsverfahrens durch ein erhöhtes Risiko, einen neuen Dienstposten nicht zu erhalten:

Der Zugriff auf ein Dokument ist zwar berechtigt, aber zum Zeitpunkt des Zugriffs sind noch Informationen verfügbar, die bereits gelöscht sein müssten; z.B. Unterlagen zu disziplinarischen Maßnahmen.

Der Zugriff auf eine Grund- oder Teilakte ist zwar berechtigt, die Dokumente sind auch noch gültiger Bestandteil der eP-Akte, aber sie sind 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, die im Rahmen eines Bewerbungsverfahrens einer externen Stelle zugänglich gemacht wird, und nicht in einer separaten, in einem solchen Szenario nicht zugänglichen Krankenakte.
- Hinweise auf gesundheitlich bedingte Abwesenheiten im Rahmen von Aus- und Fortbildungsmaßnahmen enthalten Hinweise auf die konkreten Erkrankungen („fehlende Teilnahme wegen Sucht-Rehabilitation“).

4.7.5 Analyse der Gefährdungen und Maßnahmen

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

4.8 Einführung

In die Phase der Einführung fallen die folgenden, hinsichtlich der elektronischen Personalakte relevanten Aktivitäten:

- Umsetzung der Konfigurationskonzepte des E-Akte-Systems (jeweils unter Berücksichtigung der spezifischen Anforderungen der eP-Akte)
    - Rechte- und Rollenkonzept
    - Protokollierungskonzept
    - weitere funktionale Anforderungen
- Erstellung von Testkonzepten und Testplanung
- Evaluierung der Testergebnisse insbes. hinsichtlich der Umsetzung der Schutzziele des Datenschutzes
- Schulungsplanung (rollenbasiert) für die
    - Beschäftigten des Personalreferats
    - Beschäftigten der Poststelle

[69] http://www.bfdi.bund.de/bfdi_wiki/index.php/Checkliste_Vorabkontrolle

  - Registratoren
  - Fachadministratoren

- Prüfen und ggf. Erstellen der notwendigen organisatorischen Regelungen für die Arbeit mit der elektronischen Personalakte
- Evaluierung der Umsetzung der getroffenen Maßnahmen des Datenschutzes im Zuge der Pilotierung und ggf. auch Freigabe des Verfahrens zur produktiven Nutzung durch den Datenschutzbeauftragten

5 Anhang

5.1 Muster zur Vorabkontrolle bei Einführung der elektronischen Personalakte

1 - System- und Anwendungsbeschreibung

- Darstellung der mit der eP-Akte zu bearbeitenden Geschäftsprozesse
- 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

2 - Rechtsgrundlage der Datenverarbeitung

- Unterscheidung von Personaldaten (nach § 12 Abs. 4 BDSG) und Personalaktendaten (nach § 106 BBG, § 29 SG bzw. § 50 BeamtStG)
- Es gelten nach § 12 Abs. 4 BDSG der § 28 Abs. 2 Nr. 2 BDSG und die § 32 bis § 35 BDSG für die Nutzung personenbezogener Daten für Beschäftigungsverhältnisse soweit die bereichsspezifischen Rechtsgrundlagen keine abschließende Regelung beinhalten.
- Die Rechte des Betroffenen (Benachrichtigung, Auskunft, Sperrung, u. w.) sind im in §§ 33 – 35 BDSG beschrieben bzw. in den §§ 109 – 112 BBG und § 29 SG (Anhörung, Einsicht, Vorlage, Entfernung von Unterlagen, u. w.);
- Weitere Regelungen für die Personalakte finden sich in den §§ 107, 109, 113, 114 BBG
- Werden personenbezogene Daten für frühere, bestehende oder zukünftige Beschäftigungsverhältnisse erhoben, erarbeitet oder genutzt, gelten gemäß § 12 Abs. 4 BDSG, § 28 Abs. 2 Nummer 2 BDSG und die §§ 32 bis 35 BDSG anstelle der §§ 13 bis 16 und 19 bis 20 BDSG, soweit die bereichsspezifischen Rechtsgrundlagen keine abschließende Regelung beinhalten.

3 - Schutzbedarfs- und Gefährdungsanalyse

Die Einstufung des Schutzbedarfs der in der eP-Akte verarbeiteten und erhobenen Daten richtet sich nach dem Ausmaß des Schadens, der durch Verletzung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sowie Transparenz, Unverkettbarkeit oder Intervenierbarkeit für die Betroffenen (im Sinne des BDSG) entstehen könnte (siehe dazu Kap. 3.3.3).

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

Als Ergebnis einer generellen Schutzbedarfsanalyse für die elektronische Personalakte ergibt sich folgende Einstufung:

- Die Primärdaten haben einen sehr hohen Schutzbedarf (insbes. weil in einigen Teilakten Dokumente mit besonderen, personenbezogenen Daten nach § 3 Absatz 9 BDSG enthalten sind).
- Die Metadaten haben einen hohen Schutzbedarf.
- Die Protokolldaten haben einen hohen Schutzbedarf.

In der folgenden Tabelle sind beispielhaft ausgewählte Gefährdungen (vgl. 3.3.4) für ein elektronisches Personalaktensystem erfasst. Für diese ist festzuhalten, welche Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz, Unverkettbarkeit oder Intervenierbarkeit) signifikant beeinträchtigt werden könnten, so dass Gegenmaßnahmen technisch-organisatorischer Art ergriffen werden sollten.

Gefährdung	Vertr.	Integr.	Verfüg.	Trans.	Unverk.	Interven.
Verlust gespeicherter Daten			x	x		
Überlastung von Informationssystemen	x	x	x	x		
Fehlfunktion von Geräten oder Systemen	x	x	x	x		
Software-Konzeptionsfehler	x	x	x	x	x	X
Software-Schwachstellen oder -Fehler	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

4 - Risikobewertung

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

Die Wahrscheinlichkeit für den Eintritt eines Schadens ergibt sich wiederum aus:

- dem Missbrauchsinteresse (Interesse Unbefugter, Daten zu missbrauchen: löschen, manipulieren, unbefugt nutzen). Ein hohes Missbrauchsinteresse liegt z. B. vor, wenn durch den Missbrauch von Daten persönliche Bereicherungen möglich erscheinen, Maßnahmen gegenüber Straftätern verhindert, Konkurrenten massiv benachteiligt und Entscheidungsträger erheblich beeinträchtigt werden können (Erpressung, Rache).
- dem Aufwand, der notwendig ist, um einen Schaden herbeizuführen,
- dem Risiko, bei einem Missbrauch entdeckt zu werden, und

- der Verarbeitungshäufigkeit (Häufigkeit der Vorgänge, bei denen ein Missbrauch oder eine sonstige Beeinträchtigung möglich ist).

Als Hilfsmittel zur Durchführung der Risikoanalyse können das Modul „Risikoanalyse“ des Umsetzungsrahmenwerks (UMRA) Notfallmanagement des BSI (Standard 100-4) oder auch der BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz genutzt werden. [70]

Dort wird je nach Eintrittswahrscheinlichkeit das Risiko als gering, mittel, hoch bzw. sehr hoch eingestuft.

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 kann nach folgendem Schema ermittelt werden:

Risiko = Schutzbedarf x Eintrittswahrscheinlichkeit

5 - Informationssicherheitskonzept

Hier kann auf das zugehörige Informationssicherheitskonzept nach dem IT-Grundschutzstandard verwiesen werden.

Das Informationssicherheitskonzept muss Maßnahmen definieren, die die Eintrittswahrscheinlichkeit der aufgelisteten Risiken oder das Schadensausmaß bei deren Eintritt reduzieren. Bezüglich der personenbezogenen Daten kann das Schadensausmaß in der Regel nicht reduziert werden.

6 - Beherrschung der Risiken

Einschätzung der datenschutzrechtlichen Wirksamkeit der lt. Informationssicherheitskonzept getroffenen Maßnahmen und Bewertung verbleibender Restrisiken.

[70] siehe jeweils https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

5.2 Einordnung in das Phasenmodell zur Einführung der elektronischen Verwaltungsarbeit

In der nachfolgenden Übersicht werden die einzelnen Phasen und Aktivitäten des in Kapitel 3 skizzierten Prozesses zur Planung und Umsetzung von Maßnahmen zum Datenschutz in Relation zum Phasenmodell zur Einführung der elektronischen Verwaltungsarbeit gebracht.

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

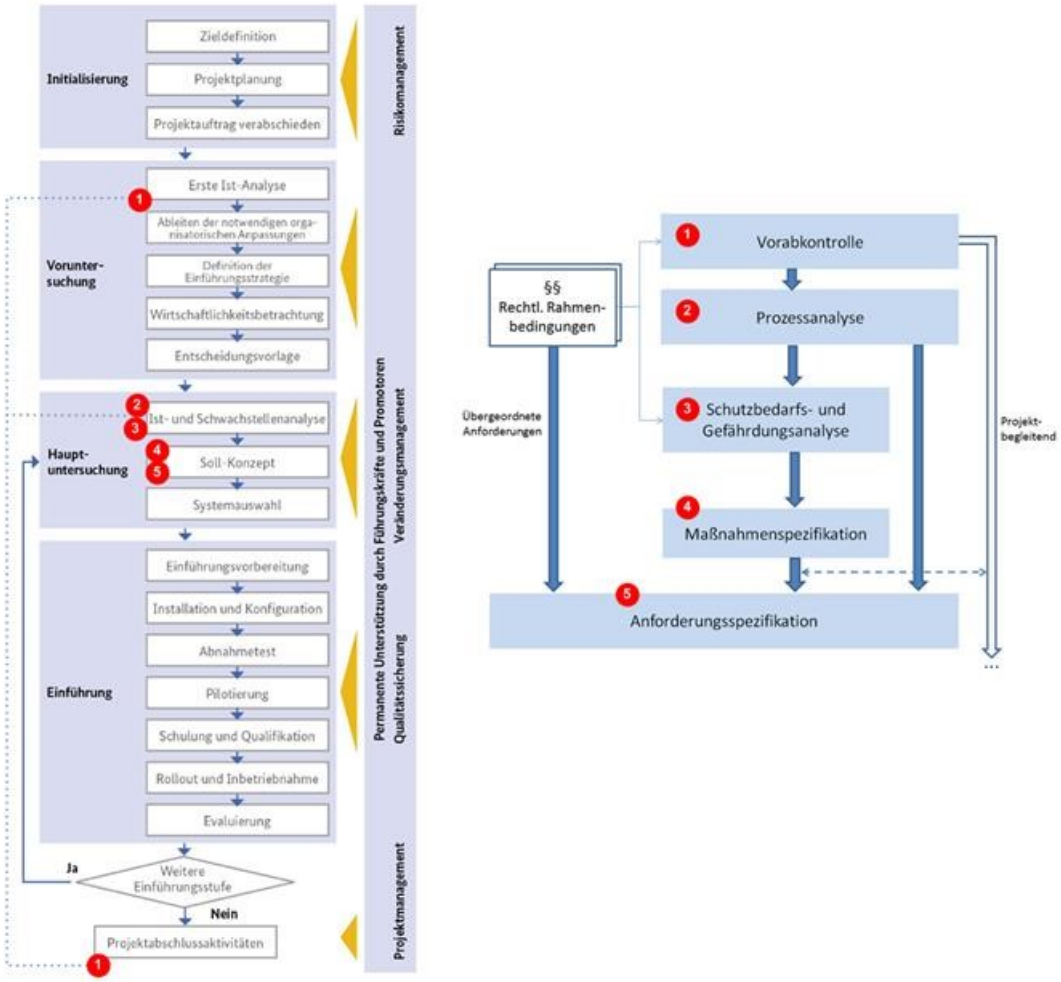

Abbildung 6: Planung und Umsetzung von Datenschutzmaßnahmen in Einführungsprojekten

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 Vorabkontrolle	Dokumentation des Ergebnisses der Prüfung der Rechtsgrundlage der Datenverarbeitung
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 bestimmten 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 organisatorische Regelungen	Übersicht der getroffene Dienstvereinbarungen und -anweisungen zur Umsetzung der organisatorischen Regelungsbedarfe wie bspw. Zweckbindung der Protokollierung, Posteingangsbehandlung etc.
K-08	Wirtschaftlichkeitsbetrachtung	Sofern die eP-Akte als gesondertes Projekt realisiert wird, sind Wirtschaftlichkeitsbetrachtungen zu den einzelnen Phasen der Einführung zu erstellen (S. Kap. 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[71] und kann als Grundlage für die Struktur eines Datenschutzkonzepts dienen.

Inhaltsverzeichnis

[71] 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 Vorabkontrolle bei der Verarbeitung personenbezogener Daten	• Wird vor der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten geprüft, ob dies erforderlich und rechtlich zulässig ist? • Wird bei allen Geschäftsprozessen und Verfahren darauf geachtet, dass personenbezogene Daten angemessen geschützt sind?
Verpflichtung/ Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten (S. Kap. 3.4.1)	• Werden alle Mitarbeiter bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet bzw. darüber unterrichtet? • Werden die Mitarbeiter regelmäßig für die Belange des Datenschutzes sensibilisiert?
Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten	• Wird bei der Einrichtung von Abrufverfahren geprüft, dass alle datenschutzrechtlichen Rahmenbedingungen eingehalten sind?
Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten	• Wurden bei der Vertragsgestaltung zur Auftragsdatenverarbeitung, bei der personenbezogene Daten verarbeitet werden, alle relevanten Datenschutz-Aspekte berücksichtigt? • Ist sichergestellt, dass externe Dienstleister die Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeiten? • Wurden auch beim Auftragnehmer alle Mitarbeiter bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet?
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? • Wird vor Verarbeitung personenbezogener Daten die datenschutzrechtliche Unbedenklichkeit geprüft?
Datenschutzaspekte bei der Protokollierung	• Wurde ein Konzept erstellt, das den Zweck der Protokollierung, deren Kontrollen sowie Schutzmechanismen für die Rechte der betroffenen Personen beschreibt? • Wird die Zweckbindung der Protokolldaten beachtet, insbesondere bei den Zugriffsregelungen? • Lässt die Form der Protokollierung effektive Auswertungsmöglichkeiten zu? • Wurden die Auswertungsmöglichkeiten mit dem Daten-

	schutzbeauftragten und der Personalvertretung abgestimmt?
Aufrechterhaltung des Datenschutzes im laufenden Betrieb	• Wird die Einhaltung der datenschutzrechtlichen Anforderungen regelmäßig überprüft? • Sind die Zuständigkeiten und Kompetenzen von IT-Revision und Datenschutzkontrolle abgestimmt?
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[72]	**Prüffragen**
Einbeziehung des Datenschutzbeauftragten und Vorabkontrolle	• Wird der Datenschutzbeauftragte vor den Software-Tests mit Daten, die Personenbezug haben könnten, informiert? • Wird vor der Freigabe von IT-Verfahren, die personenbezogene Daten verarbeiten, eine datenschutzrechtliche Prüfung durchgeführt?

Tabelle 8: Prüffragen zu möglichen Datenschutzmaßnahmen

[72] 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 nachfolgende, 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.

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

Die Schnittstellen werden in diesem Beispiel als bidirektionale Software- und Datenschnittstellen vorausgesetzt (bspw. in Form eines Nachrichtentauschs über XDOMEA[73]) und bezeichnen aus organisatorischer Sicht den Übergang der übermittelten Daten von einem Zuständigkeitsbereich zum anderen.

Hinweis

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

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

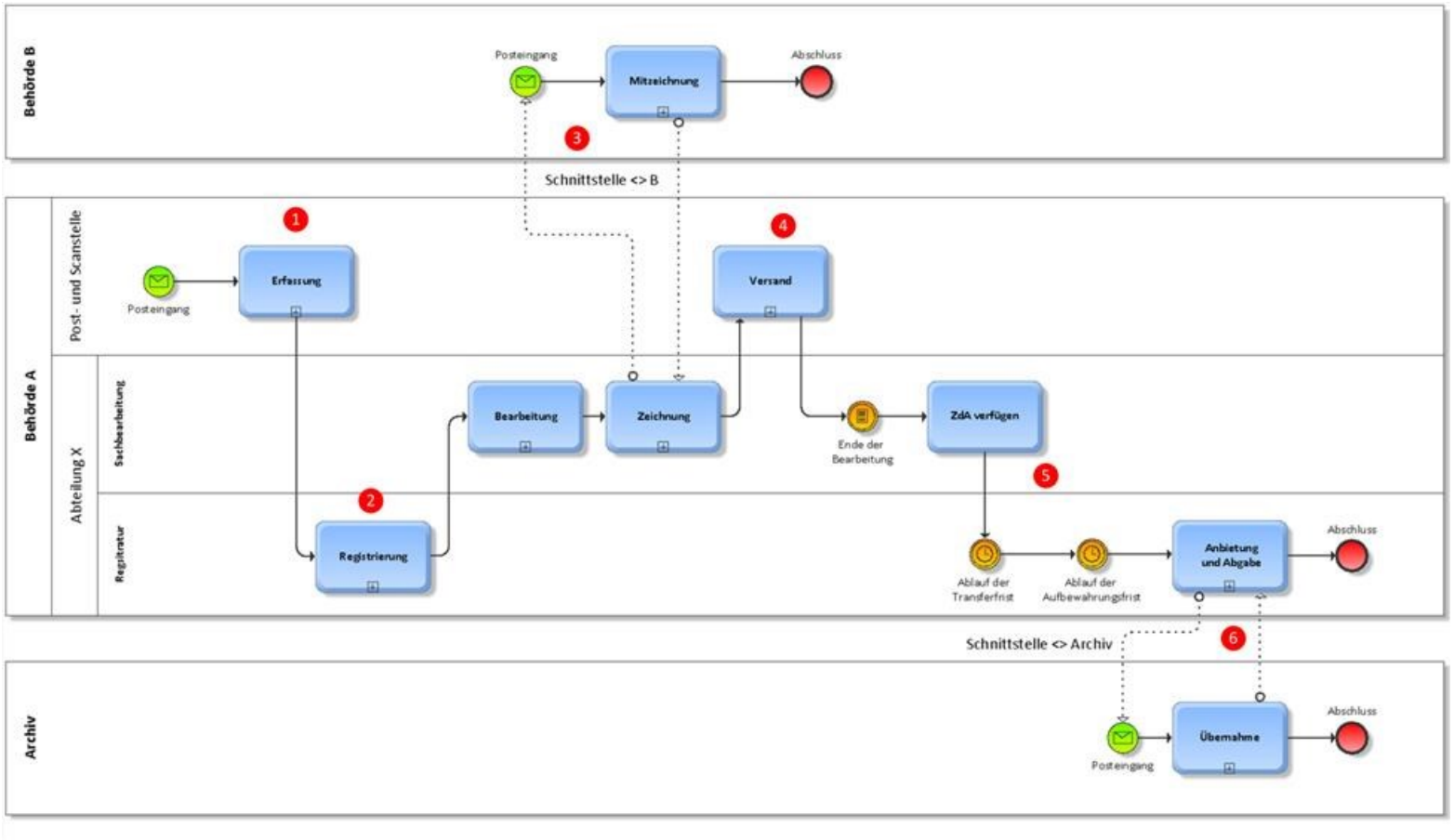

Abbildung 7: Beispiel eines Sollprozesses in BPMN 2.0

Folgende Fragestellungen und Anforderungen lassen sich mit Bezug auf den Datenschutz 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	Wurden organisatorische Maßnahmen getroffen, um zu vermeiden, dass Schriftgut digitalisiert und in das E-Akte-System überführt wird, das nicht in elektronischer Form bearbeitet werden darf?	
1.2	Wurden technische und organisatorische Maßnahmen getroffen, um zu gewährleiten, dass der Beweiswert der Dokumente bei Übernahme erhalten bleibt? Wurden für das beweiswerterhaltende Scannen Aufbewahrungsfristen der Papieroriginale definiert?	
1.3	Wurden organisatorische Maßnahmen zur Vermeidung personenbezogener Informationen mit besonderem Schutzbedarf in Metadaten getroffen?	
1.4	Wurden die entsprechenden technischen und organisatorischen Maßnahmen getroffen, um Fehlleitungen aus der zentralen Post- und Scanstelle zu vermeiden.	
2	Registrierung durch die Abteilungsregistratur	
2.1	Wurden die entsprechenden technischen und organisatorischen Maßnahmen getroffen, um Fehler bei der Zuordnung des Posteingangs zu einem Aktenzeichen und Vorgang zu vermeiden?	
2.2	Wurden organisatorische Maßnahmen zur Vermeidung personenbezogener Informationen mit besonderem Schutzbedarf in Metadaten getroffen?	
3	Mitzeichnungsverfahren, Beteiligung einer anderen Behörde	
3.1	Erfolgt die Beteiligung externer Stellen über ein standardisiertes Austauschformat (bspw. XDOMEA)?	
3.2	Wurde definiert, welche Metadaten an externe Stellen übertragen werden sollen?	
3.3	Wurde das Primärdokument in einem unveränderlichen Format wie bspw. PDF/A übertragen?	
3.4	Wie werden die Informationen über die Mitzeichnung zur mitgezeichneten Version des Dokuments abgelegt und nachvollziehbar gehalten?	
4	Versand des schlussgezeichneten Dokuments	
4.1	Kann der Versand in elektronischer Form erfolgen? Besteht für den Postausgang die 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

Glossar der Begriffe im Kontext Datenschutz (nach §3 BDSG)

Anonymisieren	Verändern personenbezogener Daten derart, dass 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 zugeordnet werden können
Authentizität (von Daten)	Bezeichnet die 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
Besondere Arten personenbezogener Daten	Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben
BDSG	Bundesdatenschutzgesetz
Betroffener	natürliche Person, über die personenbezogene Daten anfallen
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	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
Empfänger	jede Person oder Stelle, die Daten erhält
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)	Bezeichnet die 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	Verfahren sind so zu gestalten, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen.
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)	bedeutet, dass die Erhebung, Verarbeitung und Übermittlung der Daten nachvollzogen werden können
Nichtabstreitbarkeit	Bei der Nichtabstreitbarkeit[74] liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen: Nichtabstreitbarkeit der Herkunft: Es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten. Nichtabstreitbarkeit des Erhalts: Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten.
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)
OE	Organisationseinheit
OCR	Optische Zeichenerkennung (Optical Character Recognition – OCR) bezeichnet eine Komponente der Scansoftware, die aus einem Scanprodukt (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
Pseudonymisieren	Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren
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	Erhebung, Verarbeitung und Nutzung personenbezogener Daten müssen mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden 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 (perso-	Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass der Dritte zur

[74] S. BSI, IT-Grundschutz Kataloge

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/glossar/04.html

nenbezogener Daten)	Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.
Verändern (personenbezogener Daten)	das inhaltliche Umgestalten gespeicherter personenbezogener Daten
Verantwortliche Stelle	jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt
Verarbeiten (von Daten)	das Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten
Verfügbarkeit (von Daten)	Bezeichnet die Verfügbarkeit 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)	Die Vertraulichkeit gilt prinzipiell für alle Daten und Informationen im elektronischen Geschäftsgang. Daten dürfen im Zuge der Bearbeitung und der Übermittlung nicht in unbefugte Hände geraten. In Bezug auf die Befugnis gilt der Grundsatz der Erforderlichkeit.
VPS	Die Virtuelle Poststelle ist eine technische Komponente zur Sicherstellung von Authentizität, Integrität und Nichtabstreitbarkeit des Empfangs elektronisch übermittelter Dokumente zwischen registrierten Kommunikationspartnern.[75]

[75] Für weitere Informationen siehe auch: https://www.bsi.bund.de/DE/Themen/weitereThemen/VirtuellePoststelle/Grundlagen/DieVirtuellePoststelle/dievirtuellepoststelle_node.html