Bundesministerium
des Innern

DOMEA – Konzept

Erweiterungsmodul zum DOMEA®-Organisationskonzept 2.1

Datenschutz in IT-gestützten Vorgangsbearbeitungssystemen

www.kbst.bund.de

Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung

KBSt

Schriftenreihe der KBSt
ISSN 0179-7263
Band 79
November 2005

Schriftenreihe der KBSt
Band 79
ISSN 0179 - 7263

Interessenten erhalten die derzeit lieferbaren Veröffentlichungen der KBSt und weiterführende Informationen zu den Dokumenten beim

Bundesministerium des Innern
Referat IT 2 (KBSt)
11014 Berlin

Tel.: +49 (0) 1888 681 - 2312
Fax.: +49 (0) 1888 681 - 52312

Homepage der KBSt: www.kbst.bund.de
mailto: Monika.Pfeiffer@bmi.bund.de

Inhalt

Abbildungen

1 Einleitung

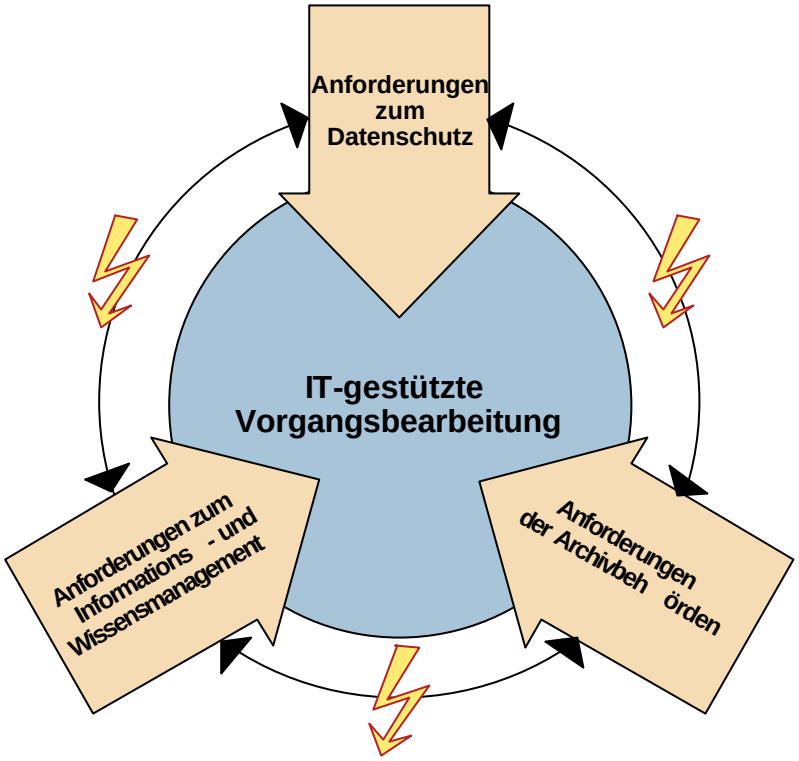
Mit der Einführung der IT-gestützten Vorgangsbearbeitung auf allen Ebenen der öffentlichen Verwaltung vollzieht sich ein grundlegender Wandel in behördlichen Arbeitsabläufen und Verfahrensweisen. Die zunehmende Verdrängung herkömmlicher papiergebundener Informationen durch E-Mails, elektronische Dokumente und schließlich die elektronische Akte führt zur leichteren Verfügbarkeit des gesamten Datenbestandes. Oblag für die papiergebundene, konventionelle Bearbeitung das Ordnen, Aufbewahren und Bereitstellen, und damit auch das Recherchieren, bisher meist ausschließlich den Registratoren, können inzwischen Bearbeiter Recherchen über den Datenbestand selbst ausführen und Schriftgut in kürzester Zeit auf elektronischem Weg behördenintern oder an autorisierte Stellen außerhalb der Behörde weiterleiten.

Die elektronische Verwaltung von Information reduziert die Aufwände bei der Erstellung von Daten. Automatisch werden die Bearbeitungsstationen des elektronischen Geschäftgangs protokolliert und Dokumente können in kürzester Zeit kopiert, verbreitet und überarbeitet werden. Vor dem Hintergrund dieser Veränderungen stellen sich Fragen nach dem Umgang mit personenbezogenen Daten. Je mehr sich die bisher realisierten Lösungen in erster Linie auf die elektronische Bereitstellung, die Performanz des Zugriffs und die permanente Verfügbarkeit von Daten konzentrieren, desto dringlicher wird die Frage nach der Umsetzung datenschutzrechtlicher Aspekte.

Das Recht des Einzelnen auf informationelle Selbstbestimmung verankert den „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner personenbezogenen Daten“ im Gesetz. Dies gilt für die Mitarbeiter einer Behörde ebenso wie für den Bürger.

Geht der gesetzlich verankerte Schutz personenbezogener Daten mit einer entsprechenden Einschränkung der Erfassung und des Zugriffs auf Daten einher, treten Interessenkonflikte hinsichtlich Langzeitarchivierung und Informations- und Wissensmanagement zu Tage. So verlangen die Anforderungen an die Archivierung und Revisionsfestigkeit elektronischer Akten auch eine lückenlose Erfassung der im Bearbeitungsprozess entstandenen Daten (Bearbeitungs- und Protokollinformationen) und Dokumente. Darüber hinaus bestehen im Rahmen der Einführung der elektronischen Akte auch Erwartungen hinsichtlich einer besseren Informationsteilung im Rahmen eines behördlichen Informations- und Wissensmanagements.

Damit wird deutlich, dass zusammen mit den Anforderungen des Datenschutzes zur gleichen Thematik teilweise entgegengesetzte Anforderungen aus den Bereichen Informations- und Wissensmanagement sowie Archivierung auf die IT-gestützte Vorgangsbearbeitung einwirken. Hier wäre eine zu restriktive Auslegung der datenschutzrechtlichen Problematik hinderlich.



Vor diesem Hintergrund verfolgt das vorliegende Dokument das Ziel, Ansätze zur Umsetzung datenschutzrechtlicher Aspekte bei der Nutzung der IT-gestützten Vorgangsbearbeitung darzustellen und in den Zusammenhang mit Anforderungen der Archivbehörden und den Anforderungen an eine Informations- und Wissensmanagement zu stellen.

Auf eine allgemeine Diskussion datenschutzrechtlicher Probleme wird dabei bewusst verzichtet. Hierzu steht umfassende Literatur jedermann zugänglich zur Verfügung. Nach einer kurzen Darstellung des rechtlichen Rahmens, werden stattdessen datenschutzrechtliche Fragestellungen an einzelnen Bearbeitungsschwerpunkten im Geschäftsgang dargestellt. Zu diesen Fragestellungen werden organisatorische und/oder technische Lösungsvorschläge unterbreitet. Dadurch sollen die Behörden für die spezifischen Anforderungen sensibilisiert und gleichzeitig in die Lage versetzt werden, Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen in Abhängigkeit ihrer speziellen Erfordernisse zu beurteilen und zu realisieren.

Technische Lösungsmöglichkeiten und insbesondere funktionale Anforderungen werden in der neuen Version 2.0 des Anforderungskataloges berücksichtigt. Dadurch werden auch die Produkthersteller entsprechender Systeme für die Datenschutzproblematik sensibilisiert und können die grundlegenden Anforderungen in die Entwicklung ihrer Produkte einfließen lassen.

2 Aufbau und Zweck des Dokumentes

Dieses Dokument richtet sich an Behörden, die sich im Rahmen der Einführung IT-gestützter Vorgangsbearbeitung mit der Umsetzung von datenschutzrechtlichen Anforderungen auseinandersetzen. Es werden datenschutzrechtliche Problemstellungen im Geschäftsgang dargestellt und entsprechende Maßnahmen aufgezeigt.

Die Inhalte dieses Dokumentes werden, neben der Einleitung, in fünf Kapiteln dargestellt.

Kapitel 3 „Grundlagen“ nimmt eine Abgrenzung des Themas Datenschutz zu verwandten Themenkomplexen vor und beschäftigt sich mit den rechtlichen Rahmenbedingungen. Dazu werden die Bedeutung der fünf Grundsätze des Datenschutzes für die Einführung IT-gestützter Vorgangsbearbeitung untersucht und weiterhin die Rechte der Betroffenen sowie datenschutzrechtliche Regelungen dargestellt.

Kapitel 4 „Problemfelder des Datenschutzes in der IT-gestützten Vorgangsbearbeitung“ beinhaltet zwei Bereiche der IT-gestützten Vorgangsbearbeitung in denen datenschutzrechtliche Überlegungen zum Tragen kommen: Zum einen den Umgang mit Dokumenten, die personenbezogene Daten enthalten können. Zum anderen den Umgang mit Protokollinformationen, die in IT-gestützten Vorgangsbearbeitungssystemen (teil-) automatisch erstellt werden. Es erfolgt eine Erläuterung der Problemfelder. Entsprechende Lösungswege zur Beachtung des Datenschutzes werden aufgezeigt.

Kapitel 5 „Datenschutzrechtliche Aspekte im Geschäftsgang“ untersucht die konkreten Problematiken, die bei der Einführung IT-gestützter Vorgangsbearbeitung auftreten können. Vor dem Hintergrund eines Mustergeschäftsgangs, unter Berücksichtigung des DOMEA®-Organisationskonzeptes, werden technische und organisatorische Maßnahmen dargestellt, die Behörden zur Umsetzung einer datenschutzgerechten, IT-gestützten Vorgangsbearbeitung ergreifen können.

Kapitel 6 „Umgang mit Rechten der Betroffenen im IT-gestützten Geschäftsgang“ untersucht die Wirksamkeit der dargestellten Maßnahmen im Hinblick auf das Recht des Einzelnen auf informationelle Selbstbestimmung.

Kapitel 7 „Zusammenfassung“ greift die in den Kapiteln 4, 5 und 6 dargestellten Maßnahmen nochmals auf und fasst sie vor dem Hintergrund der in Kapitel 3 dargestellten Grundsätze des Datenschutzes zusammen.

3 Grundlagen

3.1 Definition und Abgrenzung des Begriffs Datenschutz

Das Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983 regelte das „**Recht des Einzelnen auf informationelle Selbstbestimmung**“ (BVerfGE 65, 1).

Es besteht demnach ein "Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner personenbezogenen Daten".

Die Aufgabe des Datenschutzes ist die Gewährleistung der informationellen Selbstbestimmung des Einzelnen

Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in unzulässiger Weise in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig und bedürfen durchweg einer Rechtsgrundlage.

Das Recht auf informationelle Selbstbestimmung verlangt neben dem rechtlichen Schutz der personenbezogenen Daten (Datenschutz) auch eine angemessene Datensicherheit.

Begriffsbestimmung Datensicherheit sowie Abgrenzung gegenüber Datenschutz

Datensicherheit umfasst alle organisatorischen und technischen Maßnahmen für die Sicherstellung der notwendigen Verfügbarkeit und Abschirmung personenbezogener Daten.

Beim Datenschutz steht die Betroffenensicht im Vordergrund. Der Begriff Datensicherheit beschreibt demgegenüber die Anforderungen an den Datenschutz aus Anwendersicht: Verfügbarkeit, Integrität und Vertraulichkeit der Daten müssen gewährleistet sein, um den Benutzer vor Schäden zu bewahren.

Die Anforderungen an den Datenschutz aus Sicht des Anwenders

- **Verfügbarkeit:** Verfügbarkeit bezeichnet die Eigenschaft, bestimmte Datensicherungsleistungen in zugesicherter Form und Qualität in einem zugesicherten Zeitraum erbringen zu können.
- **Integrität**: Informationen dürfen nur von Befugten in beabsichtigter Weise verändert und nicht unzulässig modifiziert werden (Unversehrtheit, aber auch Vollständigkeit, Widerspruchsfreiheit und Korrektheit).
- **Vertraulichkeit:** Die Information darf nur Befugten zugänglich sein, es darf kein unbefugter Informationsgewinn stattfinden.

3.2 Weitere Begriffsbestimmungen

Insbesondere in § 3 BDSG und in den korrespondierenden Normen auf Länderebene (z. B. § 3 DSG NRW, § 2 LDSG Schleswig-Holstein) werden die grundlegenden datenschutzrechtlichen Begriffe definiert. Für die Zwecke der IT-gestützten Vorgangsbearbeitung sind Begrifflichkeiten in folgenden Kategorien besonders relevant:

- Personenbezogene Daten
- Ausprägungen der Verwendung personenbezogener Daten
- Beteiligte sowie deren Rechte

Im Folgenden werden die Begrifflichkeiten näher erläutert.

3.2.1 Personenbezogene Daten

Definition personenbezogene Daten
Definition besondere personenbezogene Daten

Als **personenbezogene Daten** werden einzelne Informationen gewertet, durch die sich Rückschlüsse auf die Identität oder die sachlichen Verhältnisse einer Person ziehen lassen (vgl. § 3 Abs. 1 BDSG). Damit wird deutlich, dass der Schutz ausschließlich für natürliche Personen gilt. Juristische Personen, wie z. B. eine Aktiengesellschaft, werden durch das BDSG nicht geschützt.

Darüber hinaus klassifiziert das Bundesdatenschutzgesetz Angaben über:

- rassische und ethnische Herkunft
- politische Meinung
- religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit
- Sexualleben

als **besondere personenbezogene Daten** (§ 3 Abs. 9 BDSG).

Besondere personenbezogene Daten sind verstärkt schutzwürdig, da sie den Intimbereich des Betroffenen berühren und ein Missbrauch gegebenenfalls schwerwiegende Nachteile für diesen bedeuten könnte.

Für die Bestimmung des Schutzbedarfes innerhalb der öffentlichen Verwaltung, würde eine Kategorisierung in

- Dokumente mit bzw. ohne personenbezogene Daten oder auch
- Dokumente mit personenbezogenen bzw. mit besonderen personenbezogenen Daten

aber zu kurz greifen, da ein Großteil der Dokumente Daten zum Zweck der Kontaktaufnahme, also personenbezogenen Daten nach dem BDSG enthält.

Eine spezielle Schutzwürdigkeit, d.h. Maßnahmen, die über die für die Akten einer Verwaltung sowieso geltenden Schutzmaßnahmen hinausgehen, ist für solche Daten aber nur schwer zu begründen, da ohne de-

ren Erfassung eine Kontaktaufnahme in der behördlichen Arbeit überhaupt nicht möglich ist.

Für die Praxis des Datenschutzes empfiehlt sich deshalb eine weitere Klassifikation der im BDSG nicht als „besonders" bezeichneten personenbezogenen Daten in:

1. Kontaktdaten, im folgenden „**einfache personenbezogene Daten**" und
2. personenbezogenen Daten, die über Kontaktdaten hinausgehen, im folgenden „**sensible personenbezogene Daten**".

Zu den **einfachen personenbezogenen Daten** zählen alle für die Kontaktaufnahme benötigten Informationen, bspw.:

- Name und Vorname
- Titel
- Akademische Grade
- Anschrift
- Kontaktdaten sonstiger Art (E-Mail, Telefon, Fax etc.)
- u. U. auch Berufs- und Funktionsbezeichnung[1]

Sensible personenbezogene Daten sind dann alle personenbezogenen Daten, die über Kontaktinformationen hinausgehen, aber durch das BDSG noch nicht als besonders klassifiziert sind u.a.:

- Staatsangehörigkeit
- Beruf
- Einkommen
- Familienstand

3.2.2 Ausprägungen der Verwendung personenbezogener Daten

Die einzelnen Ausprägungen der Verwendung personenbezogener Daten sind im § 3 Abs. 2-6a BDSG definiert. Die nachfolgenden Begriffsbestimmungen entsprechen den gesetzlichen Definitionen oder sind an diese angelehnt.

Ausprägungen der Verwendung personenbezogener Daten

Erheben ist das Beschaffen von Daten über den Betroffenen durch z. B. Befragung, medizinische Untersuchung und Observierung.

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.

- **Speichern** ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung.

[1] Vgl. dazu auch Informationsfreiheitsgesetze, bspw. § 9 Abs. 3 IFG NRW

- **Verändern** ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten.
- **Übermitteln** ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten.
- **Sperren** ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.
- **Löschen** ist das Unkenntlichmachen gespeicherter personenbezogener Daten.

Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Anonymisieren ist das Verändern personenbezogener Daten derart, dass Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer natürlichen Person zugeordnet werden können.

Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen, zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

3.2.3 Beteiligte

Mögliche Beteiligte im Datenschutz

Betroffener ist eine natürliche Person, von der personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Betroffener kann auch der Mitarbeiter einer Behörde sein, dessen personenbezogene Daten bei der IT-gestützten Vorgangsbearbeitung gespeichert werden.

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Empfänger ist jede Person oder Stelle, die Daten erhält.

Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle außer der Betroffene selbst.

3.3 Grundsätze des Datenschutzrechts

Die Grundsätze des Datenschutzrechts leiten sich aus dem Recht auf informationelle Selbstbestimmung ab

Eine datenschutzrechtskonsistente IT-gestützte Vorgangsbearbeitung hat sich an den - insbesondere im BDSG niedergelegten - Grundsätzen des Datenschutzrechts zu orientieren. Sind diese Grundsätze adäquat berücksichtigt, erfüllt dies die wesentlichen Anforderungen der Vielzahl von Gesetzen, die datenschutzrechtliche Regelungen enthalten. Die Grundsätze, leiten sich direkt oder indirekt aus dem im Volkszählungsurteil des Bundesverfassungsgerichts ergangenem informationellen Selbstbestimmungsrecht ab und sind somit seit 20 Jahren in höchstrichterlicher Rechtsprechung fixiert.

Zu den allgemeinen Grundsätzen des Datenschutzrechts zählen:

Grundsätze des Datenschutzrechts

- Zulässigkeit
- Erforderlichkeit
- Datenvermeidung und Datensparsamkeit
- Zweckbindung
- Transparenz

Die Umsetzung dieser Grundsätze und die davon abgeleiteten Rechte der Beteiligten regelt im Wesentlichen das Bundesdatenschutzgesetz.

3.3.1 Zulässigkeit

Grundsätzlich ist jede Verarbeitung personenbezogener Daten verboten. Ausnahmsweise ist eine Verarbeitung zulässig, wenn

- ein Gesetz oder eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet oder
- der Betroffene eingewilligt hat (vgl. § 4 Absatz 1 BDSG).

3.3.1.1 Zulässigkeit durch Gesetz oder andere Rechtsvorschriften

Die Zulässigkeit der Verwendung personenbezogener Daten regelt im Wesentlichen das BDSG. Demnach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder deren Nutzung für die Geschäftszwecke einer Behörde zulässig, wenn

- sie zur Erfüllung der Fachaufgabe der verantwortlichen Stelle erforderlich sind
- kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung und Nutzung überwiegt.

Andere Rechtsvorschriften, die eine Zulässigkeit der Verwendung personenbezogener Daten regeln sind u. a. Rechtsverordnungen, Richtlinien, Satzungen oder Erlasse.

Die Zulässigkeit der Verwendung personenbezogener Daten ergibt sich aus einer Rechtsnorm oder der Einwilligung des Betroffenen

Beispiel: Eine Meldebehörde benötigt einen bestimmten Satz personenbezogener Daten, um ihre gesetzlich definierten Aufgaben wahrnehmen zu können. Die Erhebung personenbezogener Daten des Betroffenen ist zulässig, da sie auf der Grundlage einer Rechtsnorm (§ 1 Melderechtsrahmengesetz) beruht.

3.3.1.2 Einwilligung des Betroffenen

Eine Einwilligung des Betroffenen zur Verwendung seiner personenbezogenen Daten ist nur wirksam, wenn die folgenden Kriterien erfüllt sind:

- Die Einwilligung ist nur wirksam, wenn sie auf der freiwilligen Entscheidung des Betroffenen beruht (vgl. § 4a Abs. 1 S. 1 BDSG).

- Der Betroffene muss vorab über den Zweck der Speicherung und einer vorgesehenen Übermittlung unterrichtet werden (vgl. § 4a Abs. 1 S. 2 BDSG).
- Die Einwilligung durch den Betroffenen bedarf grundsätzlich der Schriftform (vgl. § 4a Abs. 1 S. 3 BDSG). Die Einwilligung kann auch per E-Mail oder per Erklärung in einem Webformular erfolgen. Sofern im Rahmen einer E-Government-Anwendung die Möglichkeit einer elektronischen Einwilligung angeboten wird, ist § 4 des Gesetzes über den Datenschutz bei Telediensten (TDDSG) zu beachten. § 4 TDDSG schreibt vor, dass die Einwilligungserklärung durch eine eindeutige und bewusste Handlung des Nutzers erfolgen muss, und dass sie protokolliert wird und jederzeit abrufbar sein muss. Das TDDSG korrespondiert mit den Grundsätzen des BDSG. Es regelt den Schutz personenbezogener Daten bei der Nutzung von Telediensten zu nicht dienstlichen oder beruflichen Zwecken (E-Commerce, E-Government).

Beispiel: Ein Katasteramt erhält von einem ortsansässigen Immobilienmakler die Anfrage, personenbezogene Daten über Hauseigentümer im betreffenden Ort zu erhalten, um diese in einer Datenbank anzulegen. Die Übermittlung der Daten bedarf zur Gewährleistung der Zulässigkeit der Einwilligung der Betroffenen (Hauseigentümer).

3.3.2 Erforderlichkeit

Das Speichern, Verändern oder Nutzen personenbezogener Daten ist nur dann zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist (§ 14 Abs.1 BDSG).

Die Verwendung eines Datums ist erforderlich, wenn sie für die Erledigung der jeweiligen Fachaufgabe benötigt wird

Die Erforderlichkeit der Verwendung personenbezogener Daten ergibt sich aus der jeweiligen, per Rechtsnorm übertragenen Fachaufgabe einer Behörde. Unter folgenden Umständen ist die Erforderlichkeit zur Verwendung personenbezogener Daten gegeben:

- Die Fachaufgabe ist ohne die Verwendung der personenbezogenen Daten nicht oder nicht vollständig zu erfüllen.
- Die Fachaufgabe ist ohne die Verwendung der personenbezogenen Daten nur unter großen Schwierigkeiten, mit einem unverhältnismäßig höheren Aufwand oder verspätet zu erfüllen.

Sind einzelne personenbezogene Daten eines Datensatzes für die Erreichung des Verarbeitungszieles überflüssig, gebietet das Prinzip der Erforderlichkeit, dass seitens der verantwortlichen Stelle Maßnahmen zu treffen sind, die gewährleisten, dass nur die zur Erfüllung der konkreten Fachaufgabe erforderlichen Daten verarbeitet werden. In Betracht kommen dabei zum Beispiel die Sperrung, Anonymisierung, Pseudonymisierung oder Löschung von Datenmengen.

Beispiel: Ein Regierungspräsidium hält Einzelbelege über die Gewährung von BAföG-Leistungen vor. Diese enthalten personenbezogene Daten. Bearbeiter des Kultusministeriums, einer dem Regierungspräsidium übergeordneten Behörde, welche zwar die BAföG-Mittel bewirtschaft,

aber für Einzelfallentscheidungen nicht verantwortlich ist, haben nach dem Grundsatz der Erforderlichkeit keinen Zugriff auf diese Einzelbelege. Die personenbezogenen Daten der Einzelbelege werden für die Erfüllung der Aufgaben des Kultusministeriums i.d.R. nicht benötigt.

3.3.3 Datenvermeidung und Datensparsamkeit

Der Grundsatz der Datenvermeidung und Datensparsamkeit besagt, dass sich die Gestaltung und Auswahl elektronischer Dienste an dem Ziel auszurichten hat, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Die Verwaltung hat somit schon im Vorfeld der Entwicklung und Auswahl von Datenverarbeitungssystemen und bei der Ausgestaltung konkreter Datenverarbeitungsprozesse darauf hinzuwirken, dass diese möglichst datensparsam sind.

Datenverarbeitungssysteme und -prozesse sind grundsätzlich datensparsam zu gestalten

Der Grundsatz der Datenvermeidung und Datensparsamkeit ist von dem Prinzip der Erforderlichkeit abzugrenzen. Das Prinzip der Erforderlichkeit bezieht sich auf den konkreten Einzelfall der Datenerhebung, -verarbeitung und –nutzung, das Prinzip der Datenvermeidung und Datensicherheit auf die allgemeine Systematik der Datenverwendung.

3.3.4 Zweckbindung

Der Grundsatz der Zweckbindung besagt, dass personenbezogene Daten ausschließlich für den Zweck verarbeitet werden, für den sie erfasst und gespeichert wurden. Demnach ist z. B. die Erhebung, Verarbeitung und Nutzung beliebiger personenbezogener Daten unzulässig. Eine Datenverarbeitung zu einem anderen als dem ursprünglichen Zweck ist nur zulässig, sofern eine hinreichende Rechtsgrundlage oder eine schriftliche Einwilligung des Betroffenen vorliegt.

Die Verwendung personenbezogener Daten muss zweckgebunden erfolgen

§ 15 und § 16 BDSG treffen Aussagen über die Zulässigkeit der Datenübermittlung an öffentliche bzw. nicht-öffentliche Stellen (vgl. Kap. 4.1.1). Für Spezialfälle sind Datenübermittlungen zwischen Behörden üblicherweise genau geregelt.

Beispiel: Eine Meldebehörde hält Daten über die Adoption eines Kindes vor. Im Rahmen der betreffenden Meldedatenübermittlungsverordnung ist die automatische Übermittlung personenbezogener Daten zwischen Meldebehörden und Polizeidienststelle geregelt. Der auszutauschende Datensatz ist definiert und enthält keine Daten darüber, ob ein Einwohner adoptiert wurde oder nicht. Die Übertragung von Informationen über Adoptionen an eine Polizeidienststelle wäre deshalb ein Verstoß gegen das Prinzip der Zweckbindung.

3.3.5 Transparenz

Das Prinzip der Transparenz gebietet, dass dem Betroffenen Kenntnisnahme über die Struktur der Datenverarbeitung, über die Datenverarbeitungsprozesse, über die eingesetzte Technik und über die Datenströme ermöglicht wird.

Die systematisierte Verarbeitung personenbezogener Daten muss für Betroffene transparent gestaltet werden

3.4 Rechte der Betroffenen

Die Rechte des Betroffenen bei der Verarbeitung seiner personenbezogenen Daten durch eine Behörde

Aus dem Recht des Einzelnen auf **informationelle Selbstbestimmung** und den daraus abgeleiteten **Grundsätzen des Datenschutzrechts** ergeben sich für den Betroffenen insbesondere folgende Rechte:

Recht auf Auskunft: Dem Betroffenen ist auf seinen Antrag hin mitzuteilen, welche personenbezogenen Daten gespeichert sind, woher diese Daten stammen, wohin diese Daten übermittelt wurden oder werden und warum diese Daten gespeichert wurden. Der Anspruch des Betroffenen besteht nicht, wenn die ausführende Behörde durch die Auskunftserteilung bei der Erledigung ihrer Aufgabe beeinträchtigt werden würde oder wenn sie aufgrund gesetzlicher Bestimmungen nicht erteilt werden darf.

Recht auf Berichtigung: Das Recht des Betroffenen auf Berichtigung ist vielmehr eine Pflicht der verarbeitenden Stelle auf Korrektur unrichtiger personenbezogener Daten. Diese besteht für die Behörde unabhängig davon ob der Betroffene seinen Anspruch geltend macht oder nicht.

Recht auf Löschung: Die speichernde Stelle hat die personenbezogenen Daten zu löschen, wenn die Speicherung nicht zulässig. Dabei bedeutet Löschen das unkenntlich machen von gespeicherten personenbezogenen Daten, so dass sie für niemanden mehr zugänglich sind.

Darüber existieren in einigen Fachbereichen gesetzliche Regelungen, die in bestimmten Fällen das Löschen von personenbezogenen Daten vorschreiben (vgl. bspw. § 80 AusIG)

Recht auf Sperrung: Anstelle des Rechts auf Löschung tritt das Recht auf Sperrung von personenbezogenen Daten, wenn Aufbewahrungspflichten auf Seiten der speichernden Stelle bestehen oder wenn anzunehmen ist, dass schutzwürdige Interessen des Betroffenen durch die Löschung beeinträchtigt werden. Anders als bei der Löschung bleiben die Daten bei einer Sperrung physisch erhalten. Die gesperrten Daten werden durch eine mechanische oder technische Vorrichtung vor Zugriffen geschützt. Sie können jedoch, z.B. zur Verwendung bei Gerichtsverfahren, reaktiviert werden.

Recht auf Benachrichtigung: Das Recht auf Benachrichtigung besteht sofern personenbezogene Daten ohne Kenntnis des Betroffenen erhoben werden. Es umfasst Angaben über die Speicherung, die Identität der verarbeitenden Stelle und die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung. Eine Pflicht auf Benachrichtigung von Seiten der jeweiligen verarbeitenden Behörde besteht nicht, sofern die Speicherung oder Übermittlung der Daten durch ein Gesetz ausdrücklich vorgesehen ist.

Schadenersatzanspruch des Betroffenen: Der Betroffene hat nach § 7 BDSG einen Anspruch auf Schadenersatz, wenn er durch die unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden erleidet. Die Ersatzpflicht entfällt, sofern die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

Anrufung des Datenschutzbeauftragten: An den Bundesbeauftragten für den Datenschutz oder die jeweiligen Landesbeauftragten kann sich ein Betroffener wenden, wenn er der Ansicht ist, bei der Erhebung, Ver-

arbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes oder des Landes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

3.5 Datenschutzrechtliche Regelungen und Informationsfreiheit

Informationsfreiheitsgesetze liegen derzeit in den Bundesländern Nordrhein-Westfalen, Schleswig-Holstein, Brandenburg und Berlin vor. Sie gewähren Bürgern das Recht auf Herausgabe von Verwaltungsinformationen. Hintergrund der Einführung dieser Gesetze ist die von weiten Teilen der Bevölkerung bemängelte Transparenz der Verwaltungsprozesse im öffentlichen Dienst. Die vier bisher existierenden Informationsfreiheitsgesetze sind bezogen auf Zweck und Inhalt sehr ähnlich, daher wird im Folgenden auf eine weitergehende Differenzierung verzichtet und die Datenschutzproblematik in diesem Zusammenhang ausschließlich anhand des IFG NRW näher beschrieben.

Verwaltungsinformationen im Sinne des IFG NRW sind alle in Schrift-, Bild-, Ton- oder Datenverarbeitungsform oder auf sonstigen Informationsträgern vorhandenen Informationen, die im dienstlichen Zusammenhang erlangt wurden. Bisher mussten Bürger ein berechtigtes Interesse nachweisen, wenn sie bestimmte Akten einsehen wollen. Dies hat sich nun umgekehrt, die Behörde muss begründen, welche rechtlichen Bedenken gegen eine Herausgabe von Akten sprechen. **Unzulässig** ist z. B. grundsätzlich die **Herausgabe personenbezogener Daten** abgesehen von wenigen Ausnahmetatbeständen, die in § 9 IFG NRW normiert sind. Die Klausel zum Schutz personenbezogener Daten, entspricht diesbezüglich den allgemeinen Grundsätzen des Datenschutzrechts. So ist eine Herausgabe personenbezogener Daten im Rahmen einer Anfrage gestützt auf das IFG zum Beispiel nur zulässig, wenn der Betroffene einwilligt, ein Gesetz die Herausgabe gestattet oder die Offenbarung der Daten erhebliche Nachteile für das Allgemeinwohl verhindern würde.

4 Problemfelder des Datenschutzes in der IT-gestützten Vorgangsbearbeitung

Aus datenschutzrechtlicher Sicht sind in der IT-gestützten Vorgangsbearbeitung zwei Problemfelder zu betrachten:

1. Der Umgang mit den Dokumenten, d.h. die Behandlung von Meta- und Primärinformation von elektronischen Dokumentobjekten.
2. Der Umgang mit Protokollinformationen, die in IT-gestützten Vorgangsbearbeitungssystemen (teil-)automatisch erstellt und zum Dokument bzw. zum Vorgang oder zur Akte hinterlegt werden.

In den folgenden Kapiteln werden diese Problemfelder erläutert und Lösungswege aufgezeigt. Im Anschluss stellt Kapitel 5 die unterschiedlichen Lösungsansätze anhand eines beispielhaften Geschäftsgangs dar.

4.1 Behandlung von Dokumenten

In Hinblick auf den Datenschutz ist nach vier Arten von Dokumenten zu unterscheiden, die im Rahmen des IT-gestützten Geschäftsgangs bearbeitet werden:

Klassifikation von Dokumenten hinsichtlich datenschutzrechtlicher Relevanz

1. **Dokumente ohne Personenbezug:** Diese Dokumente enthalten keinerlei personenbezogene Daten im Sinne des § 3 Abs. 1 bzw. § 3 Abs. 9 BDSG (zur Definition personenbezogener Daten siehe Kapitel 3.2.1). Für diese Dokumente sind datenschutzrechtliche Überlegungen nicht relevant. Für die Behandlung dieser Dokumente gelten die Empfehlungen des DOMEA®-Organisationskonzeptes 2.1 ohne Einschränkung.
2. **Dokumente mit einfachen personenbezogenen Daten:** Diese Dokumente beinhalten hauptsächlich Kontaktinformationen, d.h. Personennamen, Adressdaten, Fax- und Telefonnummern, Titel, akad. Grade u.ä. (vgl. Kapitel 3.2.1).
3. **Dokumente mit sensiblen und besonderen personenbezogenen Daten:** Diese Dokumente beinhalten personenbezogene Daten, anhand derer eine Person umfassender charakterisiert werden kann, z. B. Familienstand, Einkommen, Gesundheitszustand (vgl. Kapitel 3.2.1).

Personalakten werden hier nicht näher untersucht

4. **Personalakten**: Die Personalakte gibt als Sammlung aller Schriftstücke mit Aufzeichnungen über die persönlichen und dienstlichen Verhältnisse der Arbeitnehmer und Beamten ein vollständiges Bild über den Werdegang des einzelnen Beschäftigten. Sie dient dem sachgemäßen Personaleinsatz und der effektiven Personalplanung. Darüber hinaus hat sie auch die Funktion einer zahlungsbegründenden Unterlage.

   Für Personalakten wird eine besondere Schutzwürdigkeit im Sinne des Datenschutzes festgestellt. In den folgenden Ausfüh-

rungen wird von einer Betrachtung des Umgangs mit Personalakten im IT-gestützten Geschäftsgang abgesehen, da von Speziallösungen zum Umgang mit Personalakten ausgegangen wird.

Für Dokumente, die einfache, sensible und/oder besondere personenbezogene Daten enthalten, sind im Rahmen der IT-gestützten Vorgangsbearbeitung u. U. geeignete Vorkehrungen zur Wahrung des Datenschutzes zu treffen. Die prinzipielle Notwendigkeit und die Auswahl der geeigneten Maßnahmen hängen dabei von der Art der personenbezogenen Daten und der Verwendung der Dokumente ab.

4.1.1 Dokumente mit einfachen personenbezogenen Daten

Der überwiegende Teil von Eingängen an eine Behörde beinhaltet lediglich einfache personenbezogene Daten zum Zweck der Kontaktaufnahme, wie z. B. Vor- und Zuname und Adressdaten.

Diese personenbezogenen Daten sind für die Bearbeitung des Vorgangs in der Regel erforderlich, um beispielsweise eine Antwort an den Eingeber/Antragsteller zu senden. Aus diesem Grund ist eine Übernahme dieser Informationen in den Metadatensatz des Vorgangsbearbeitungssystems generell erforderlich.

Maßnahmen zur Wahrung des Datenschutzes dieser einfachen personenbezogenen Daten im Vorgangsbearbeitungssystem sind insbesondere für Fälle zu ergreifen, in denen einfache personenbezogene Daten an Dritte übermittelt werden bzw. durch Dritte im Vorgangsbearbeitungssystem genutzt werden. Dabei ist zu unterscheiden, ob die einfachen personenbezogenen Daten

Je nach Verwendung sind unterschiedliche Schutzmaßnahmen erforderlich

1. innerhalb der Behörde,
2. zwischen Behörden oder
3. an Dritte außerhalb der öffentlichen Verwaltung

übermittelt werden bzw. durch diese genutzt werden.

Im Folgenden werden entsprechende Maßnahmen näher erläutert.

4.1.1.1 Verwendung innerhalb einer Behörde

Die Übermittlung einfacher personenbezogener Daten innerhalb einer Behörde ist nach § 15 Abs. 1 BDSG grundsätzlich zulässig, sofern diese Übermittlung zur Erfüllung der Aufgabe des Dritten innerhalb der Behörde erforderlich ist. Da es sich bei einfachen personenbezogenen Daten um Kontaktdaten handelt, kann im Allgemeinen von einer Zulässigkeit ausgegangen werden.

Technisch-organisatorische Maßnahmen

Im Vorgangsbearbeitungssystem sind technische Maßnahmen zu ergreifen, die eine Übermittlung personenbezogener Daten an Dritte innerhalb einer Behörde ermöglichen. Dazu zählt beispielsweise der Versand dieser personenbezogenen Daten innerhalb der Behörde oder der Zugriff durch Mitarbeiter verschiedener Organisationseinheiten auf diese Daten im Vorgangsbearbeitungssystem. Entsprechende Möglichkeiten sind im DOMEA®-Organisationskonzept bereits beschrieben.

Es sind ggf. behördenspezifische organisatorische Maßnahmen zu ergreifen, die einen Übermittlungs- und Zugriffsschutz auch einfacher personenbezogener Daten innerhalb einer Behörde regeln. Diese Maßnahmen sind insbesondere dann zu ergreifen, wenn bereits durch den Tätigkeitsbereich einer Organisationseinheit weitgehende Rückschlüsse auf die Person getroffen werden können (z. B. personenbezogene Daten in der Strafverfolgung). Funktionalitäten zur Beschränkung von Zugriffsrechten bei der Weiterleitung von Dokumenten sind bereits Bestandteil des DOMEA®-Anforderungskataloges und werden in Kap. 4.1.2.1 nochmals kurz erläutert.

4.1.1.2 Austausch innerhalb der öffentlichen Verwaltung

Die Übermittlung einfacher personenbezogener Daten zwischen Behörden ist nach § 15 Abs. 1 BDSG grundsätzlich zulässig, sofern diese Übermittlung zur Erfüllung der Aufgabe der öffentlichen Stelle erforderlich ist.

Technisch-organisatorische Maßnahmen

Im Vorgangsbearbeitungssystem sind technische Maßnahmen zu ergreifen, die eine Übermittlung personenbezogener Daten an weitere öffentliche Stellen zulässt (vgl. Erweiterungsmodul zum DOMEA®-Organisationskonzept 2.1 „Inner- und interbehördliche Kommunikation“, Band 65, Schriftenreihe der KBSt, November 2005).

Organisatorisch sind behördenspezifische Regelungen zu entwickeln, welche die Mitarbeiter dazu sensibilisieren, personenbezogene Daten nach vorheriger Prüfung an öffentliche Stellen zu übermitteln. Darüber hinaus sind ggf. für einzelne Organisationseinheiten einer Behörde Regelungen zu treffen, ob und an welche öffentlichen Stellen einfache personenbezogene Daten übermittelt werden dürfen.

4.1.1.3 Abgabe an nicht-öffentliche Stellen

Nach § 16 Abs. 1 BDSG ist eine Übermittlung einfacher personenbezogener Daten an nicht-öffentliche Stellen unter folgenden Voraussetzungen zulässig:

- Zur Aufgabenerfüllung der Behörde ist eine Übermittlung der einfachen personenbezogenen Daten an nicht-öffentliche Stellen erforderlich.
- Die nicht-öffentliche Stelle benötigt die einfachen personenbezogenen Daten und kann diesen Bedarf nachweisen.
- Der Betroffene hat kein schutzwürdiges Interesse an dem Ausschluss der personenbezogenen Daten bei der Übermittlung.

Technisch-organisatorische Maßnahmen

Im Vorgangsbearbeitungssystem sind technische Maßnahmen zu ergreifen, die eine Übermittlung personenbezogener Daten an nicht-öffent-

liche Stellen zulassen (vgl. Erweiterungsmodul zum DOMEA®-Organisationskonzept 2.1 „Inner- und interbehördliche Kommunikation“, Band 65, Schriftenreihe der KBSt, November 2001). Darüber hinaus sind technische Maßnahmen zu ergreifen, die eine Dokumentübermittlung ohne jegliche personenbezogene Daten ermöglichen, da ggf. von der Unzulässigkeit der Übermittlung personenbezogener Daten ausgegangen werden muss (zu den Maßnahmen insbesondere Anonymisierung und Pseudonymisierung vgl. Kapitel 4.1.2.2).

Organisatorisch sind behördenspezifische Regelungen zu entwickeln, welche die Mitarbeiter dazu sensibilisieren, einfache personenbezogene Daten nur nach vorheriger Prüfung an nicht-öffentliche Stellen zu übermitteln. Darüber hinaus sind ggf. für einzelne Organisationseinheiten einer Behörde zu regeln, ob und an welche nicht-öffentlichen Stellen eine Übermittlung einfacher personenbezogene Daten zulässig ist.

4.1.2 Dokumente mit sensiblen und besonderen personenbezogenen Daten

Sensible sowie besondere personenbezogene Daten unterliegen einem besonderen Schutzbedarf (vgl. Kapitel 3.2.1). Entsprechende Daten, die in den Meta- und Primärinformationen vorliegen, sind demzufolge im IT-gestützten Geschäftsgang vor einer unzulässigen Verarbeitung und Nutzung zu schützen. Die Einschränkung des Zugriffs auf Primärdatenebene, mit Hinblick auf die heutzutage bestehenden technischen Möglichkeiten, bedeutet immer eine Sperrung des gesamten Dokumentes im System. Dem steht der Anspruch entgegen, den Mitarbeitern einer Behörde Dokumente in Vorgangsbearbeitungssystemen für ein Informations- und Wissensmanagement bereitzustellen. Die erst durch die elektronische Verarbeitung des Schriftguts entstehenden Möglichkeiten zum Aufbau eines behördlichen Informations- und Wissensmanagements wären damit aufgrund datenschutzrechtlicher Probleme sofort wieder zunichte gemacht.

Eine Möglichkeit diesen Interessenkonflikt zu vermeiden, wäre die Übernahme der personenbezogenen Daten in die Metadaten eines Dokumentes, da hier mit DOMEA®-konzeptkonformen Vorgangsbearbeitungssystemen Funktionalitäten vorhanden sind, um den Zugriff auf einzelne Datenfelder zu beschränken und nicht besonders schützenswerte Informationen von dieser Beschränkung auszunehmen. Diese Möglichkeit besteht i. A. allerdings nur, wenn die personenbezogenen Daten strukturiert übergeben werden, bspw. in einem Antragsverfahren bei der Verwendung elektronischer Formulare.

Häufig treten die personenbezogenen Daten jedoch in den Primärinformationen auf. Aus diesem Grund sind in Vorgangsbearbeitungssystemen Maßnahmen zu ergreifen, die besonders schutzwürdige personenbezogene Daten in Primärinformationen schützen.

Technisch-organisatorisch kann die Anforderung des besonderen Schutzes personenbezogener Daten in den Primärinformationen in zwei Alternativen gelöst werden:

- Alternative 1: Durch die Vergabe von Zugriffsrechten auf Dokumente werden personenbezogene Daten vor einer unzulässigen Verarbeitung und Nutzung geschützt.
- Alternative 2: Personenbezogene Daten werden in den Primärdaten anonymisiert bzw. pseudonymisiert.

Beide Alternativen sind aus Sicht des Datenschutzes gleichwertig. Aus Sicht eines behördeninternen Informations- und Wissensmanagement ist Alternative 2) zu bevorzugen, da Alternative 1) den Zugriff auf das gesamte Dokument sperrt, auch wenn nur ein geringer Teil der Primärinformationen datenschutzrechtlichen Schutzbedarf nach sich zieht. Eine so strikte Auslegung der Anforderungen zum Datenschutz kann den Bearbeiter, der für die Erfüllung seiner Aufgaben auf die Informationen im Aktenbestand angewiesen ist u. U. behindern. Andererseits stellt Alternative 2) erhöhte technische Anforderungen an das System. Im Folgenden sollen deshalb beide Varianten erläutert werden, so dass in Abhängigkeit von den behördenspezifischen Anforderungen die am besten geeignete Alternative ausgewählt werden kann.

4.1.2.1 Umsetzung des Schutzbedarfs unter Verwendung von Zugriffsrechten

In DOMEA®-konzeptkonformen Vorgangsbearbeitungssystemen können Zugriffsrechte auf Dokumente üblicherweise nach der Art des Zugriffs (Suchen, Lesen, Erstellen, Ändern, Löschen) und darüber hinaus auch auf Teile des Dokumentobjektes (einzelne Metadaten, alle Metadaten, Primärdaten – aber nicht für Teile der Primärdaten) für einzelne Benutzer differenziert vergeben werden. Darüber hinaus ist es weiterhin möglich, einem Benutzer der keinen Zugriff auf ein bestimmtes Dokument besitzt, die erforderlichen Rechte durch Weiterleitung des entsprechenden Dokuments temporär zu übertragen (vgl. DOMEA®-Anforderungskatalog).

Mit diesen Funktionalitäten lässt sich der Schutzbedarf personenbezogener Daten in Primärinformationen umsetzen, da vom System sichergestellt ist, dass ein Zugriff ohne die entsprechenden Zugriffsrechte nicht möglich ist (vgl. DOMEA®-Anforderungskatalog).

Durch eine entsprechende Konfiguration der Zugriffsrechte auf Grundlage eines Zugriffsrechtekonzeptes könnte somit der Zugriff auf ein Dokument auf den federführenden Bearbeiter und seine Vorgesetzten beschränkt werden. Selbst wenn im Verlauf der Bearbeitung die Beteiligung weiterer Stellen notwendig sein sollte, kann diesen der Zugriff durch die Weiterleitung des Dokumentes durch den federführenden Bearbeiter automatisch erteilt werden. Nach Rückgabe des Dokumentes an den federführenden Bearbeiter wäre der beteiligten Stelle der Zugriff auf das Dokument wieder automatisch entzogen.

4.1.2.2 Umsetzung des Schutzbedarfs bei Beachtung von IWM-Anforderungen

Recherche und Schutz personenbezogener Daten schließen sich nicht aus

Wie bereits erwähnt, besteht der Nachteil der im vorigen Abschnitt dargestellten Variante zur Umsetzung des Schutzbedarfs in der Tatsache, dass durch die Einschränkung des Zugriffs auf die Primärinformationen auch ein Großteil nicht schützenswerter Daten dem Zugriff für die Bear-

beitung entzogen wird. Für ein möglichst umfassendes Informations- und Wissensmanagement besteht aber vielmehr der Anspruch, nur den wirklich schützenswerten Datenbestand zu schützen und Informationen ohne besonderen Schutzbedarf einem möglichst breiten Bearbeiterkreis der Behörde zur Verfügung zu stellen.

Maßnahmen, die darauf abzielen, den verfügbaren Informationsbestand unter Beachtung der besonderen Schutzwürdigkeit personenbezogener Daten zugänglich zu machen, erfordern erhebliche technische sowie organisatorische Anforderungen, die im Folgenden dargestellt werden:

Identifiziert ein Bearbeiter personenbezogene Daten eines Eingangs als nicht-erforderlich bzw. besonders schutzwürdig, so sind im Sinne des Datenschutzrechts folgende Maßnahmen zu ergreifen:

- Anonymisieren oder
- Pseudonymisieren[2] der nicht-erforderlichen bzw. besonders schutzwürdigen personenbezogenen Daten.

Je nachdem ob die Primärinformationen im NCI- oder CI-Format vorliegen, bestehen unterschiedliche Möglichkeiten der Unkenntlichmachung nicht-erforderlicher personenbezogener Daten[3]:

1. Primärinformationen im NCI-Format:

Schwärzung in NCI-Daten

Bei Primärinformationen im NCI-Format (z. B. Image eines Schriftstücks) wird eine Schicht (sog. Layer) über die Primärinformation gelegt, welche die Ansicht des Eingangs verändert. Diese Schicht ermöglicht das Anonymisieren der nicht-erforderlichen personenbezogenen Daten (z. B. durch Einfügen einer Schwärzung an den entsprechenden Stellen) (siehe folgende Abbildung).

Bei der Anonymisierung personenbezogener Daten in den Primärinformationen ist zu gewährleisten, dass im Vorgangsbearbeitungssystem von nun an nur noch die anonymisierte Version zur Verfügung steht. Die nicht-anonymisierte Primärinformation steht zur Ansicht und Bearbeitung nicht mehr zur Verfügung (doppelte Speicherung), wird aber aus Gründen der Revisionssicherheit und auch mit Hinblick auf die evtl. erforderliche Abgabe an die zuständige Archivbehörde weiter elektronisch vorgehalten (siehe Kapitel 5.1.2.3 für Revisionssicherheit bzw. 5.3.3 für Übergabe von Altakten an die Archivbehörde).

[2] Zur Definition der Begrifflichkeiten siehe Kapitel 3.2.2.

[3] Zu den Formaten NCI (Non Coded Information) und CI (Coded Information) siehe Organisationskonzept 2.0 Kap. 4.1.4.

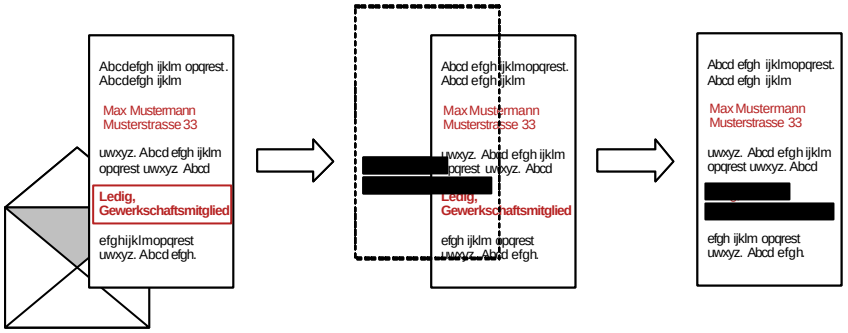


Abbildung 1: Behandlung nicht-erforderlicher personenbezogener Daten in Primärinformationen im NCI-Format (Beispiel)

2. Primärinformationen im CI-Format:

Pseudonymisierung in CI-Daten

Nicht-erforderliche personenbezogene Daten in Primärinformationen im CI-Format können durch Pseudonymisieren unkenntlich gemacht werden. Dabei werden die vorhandenen personenbezogenen Daten durch Einsetzen anderer Daten ersetzt (z. B. Vergabe eines neuen Namens) (siehe Abbildung). Es ist zu gewährleisten, dass über das Pseudonym kein Rückschluss auf das dahinter liegende personenbezogene Datum getroffen werden kann.

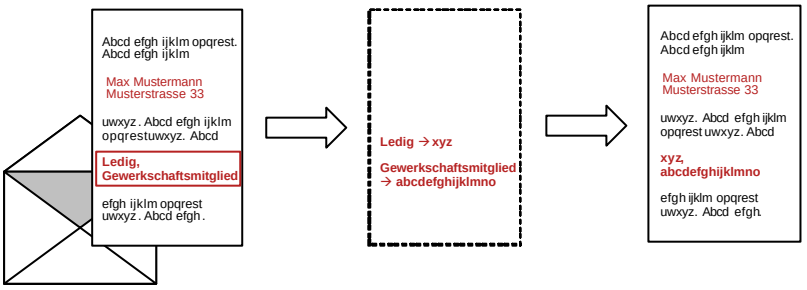


Abbildung 2: Behandlung nicht-erforderlicher personenbezogener Daten in Primärinformationen im CI-Format (Beispiele)

Die technische Unterstützung der Pseudonymisierung ist üblicherweise keine Standardfunktionalität von Vorgangsbearbeitungssystemen, sondern ist projektspezifisch umzusetzen. Insbesondere die Erstellung und Verwaltung eineindeutiger Pseudonyme[4] stellt dabei einen nicht unerheblichen Mehraufwand bei der Anpassung eines Vorgangsbearbeitungssystems dar. Darüber hinaus ist mit Hinblick auf die Anforderungen aus den Archivgesetzen auch hier eine Umkehrbarkeit der Pseudonymisierung sicherzustellen ist (siehe Kapitel 5.1.2.3 für Revisionssicherheit bzw. 5.3.3 für Übergabe von Altakten an die Archivbehörde).

Aus diesem Grund sollte vor der Umsetzung geprüft werden, ob eine einfache Anonymisierung der entsprechenden Daten nicht aus-

[4] Ein eineindeutiges Pseudonym ist nur einem einzigen personenbezogenen Datum zugeordnet (Beispiel: Hinter dem Pseudonym d7h89s verbirgt sich der Familienstand von Herrn Max Mustermann).

reichend ist. Datenschutzrechtlich ist der Schutzeffekt der Anonymisierung mit dem der Pseudonymisierung identisch.

In Kapitel 5 wird am Beispiel eines IT-gestützten Geschäftsgangs dargestellt, wie Dokumente, die besonders schutzwürdige personenbezogene Daten enthalten, unter Gesichtspunkten des Datenschutzes bearbeitet werden können.

4.2 Behandlung von Protokoll- und Bearbeitungsinformationen

Bei der Arbeit mit Vorgangsbearbeitungssystem werden sowohl in der strukturierten als auch in der unstrukturierten Vorgangsbearbeitung verschiedenste Aktivitäten am System automatisch mitprotokolliert.

Notwendigkeit der Protokollierung

Die automatische Protokollierung der Bearbeitung ist vom Prinzip auch durchaus sinnvoll, schreibt doch die GGO für den gesamten Bearbeitungsprozess die Nachvollziehbarkeit eines Sachstands auf Basis der elektronischen Akte vor (vgl. § 12 Abs. 3 GGO). Dies umfasst nicht nur die Dokumente einer Akte, sondern nach § 6 Abs. 4 RegR ausdrücklich auch die Historie einer Bearbeitung, d. h. insbesondere die Geschäftsgangvermerke, Verfügungen und Beteiligungen. Durch die automatische Erfassung wird der Bearbeiter somit von notwendigen Arbeitsschritten entlastet und potenzielle Fehler durch manuelle Erfassung können weitestgehend vermieden werden.

Möglichkeiten des Missbrauchs der Protokollinformationen

Problematisch ist jedoch die Tatsache, dass die automatische Protokollierung von Arbeitsschritten häufig über das notwendige Maß hinausgeht. DOMEA®-konzeptkonforme Vorgangsbearbeitungssysteme ermöglichen beispielsweise auch die automatische Protokollierung der Anzeige von Dokumenten, die An- und Abmeldung am System, die Verwendung unterschiedlicher Werkzeuge etc. Darüber hinaus ist der Zugriff auf die gesammelten Protokolldaten in vielen Fällen nicht geregelt, so dass über die Auswertung der Protokollinformationen ein umfassendes Profil für den Systembenutzer erstellt werden könnte. Dies beinhaltet die Gefahr eines Protokolldatenmissbrauchs, beispielsweise durch Verwendung der Protokolldaten zu Zwecken der Verhaltens- und Leistungskontrolle.

Protokollierung ist kein Selbstzweck, sondern nur dann sinnvoll und auch datenschutzrechtlich zu vertreten, wenn sie genau definierten Anforderungen genügt und potenziellen Missbrauch weitestgehend unterbindet. Dem Missbrauch von Protokollinformationen kann dabei an drei Stellen entgegengewirkt werden:

1. **Bei der Erfassung** von Protokollinformationen, durch die Beschränkung auf die minimal notwendigen Daten.
2. **Bei der Auswertung**, durch eine konsequente Beschränkung des Zugriffs auf die Protokollinformationen.
3. **Bei der Aufbewahrung** von Protokollinformationen, durch die rechtzeitige Vernichtung von Protokolldaten.

4.2.1 Erfassung von Protokollinformationen

Anforderungen der GGO an die Protokollierung

§ 12 Abs. 3 GGO schreibt die Nachvollziehbarkeit eines Sachstands auf Basis der elektronischen Akte vor. Dies umfasst nicht nur die Dokumente einer Akte, sondern nach § 6 Abs. 4 RegR ausdrücklich auch die Historie einer Bearbeitung, d. h. insbesondere die Geschäftsgangvermerke, Verfügungen und Beteiligungen. Die entsprechende Protokollierung sollte weitestgehend automatisch erfolgen, um Fehler bei der manuellen Erfassung zu vermeiden. Im Folgenden wird der Umfang der automatisch zu erfassenden Protokollinformation fallspezifisch untersucht. Die Angaben zum Umfang sind dabei gleichzeitig Minimum – mit Hinblick auf die Nachvollziehbarkeit – und Maximum – mit Hinblick auf den Datenschutz – dessen, was zu erfassen ist.

Protokollierung von Geschäftsgangvermerken

Nach Nummer II Anlage 2 zu § 13 Abs. 2 GGO und § 8 Abs. 3 RegR bestehen für die Protokollierung von Geschäftsgangvermerken folgende Mindestanforderungen:

- Variante 1: Elektronische Abbildung der hierarchieabhängigen papiergebundenen farblichen Vermerke nach Nummer I Anlage 2 zu § 13 Abs. 2 GGO.
- Variante 2: Neben dem Geschäftsgangvermerk wird der Name oder das Namenszeichen des Bearbeiters und das aktuelle Datum protokolliert, z. B. „Kenntnis genommen, Karl König, 22.11.2004“.

Protokollierung von Verfügungen

Förmliche Verfügungen regeln die Einleitung, Fortführung und den Abschluss eines Geschäftsgangs und sind für die Nachvollziehbarkeit unabdingbar. Für die elektronische Vorgangsbearbeitung ist die Protokollierung von Verfügung, Urheberschaft (d. h. Name oder Namenszeichen) und Datum deshalb erforderlich (vgl. auch § 9 RegR).

Protokollierung von Beteiligungen

§ 15 Abs. 5 GGO schreibt die Ersichtlichkeit der Beteiligung anderer Organisationseinheiten an der Bearbeitung eines Vorgangs vor. Für die Beteiligung durch förmliche Verfügungen, wie Mitzeichnungen oder Kenntnisnahmen, wurde die Notwendigkeit der Protokollierung bereits oben dargestellt. An dieser Stelle ist deshalb nur die formlose Beteiligung relevant. Diese erfolgt i.a. mündlich oder schriftlich mit und ohne Beteiligung des Vorgangsbearbeitungssystems. Eine automatische Protokollierung der Weiterleitung ist aus datenschutzrechtlichen Aspekten deshalb auch nicht erforderlich. Der Bearbeiter entscheidet hier über die Aktenrelevanz der Beteiligung.

Protokollierung von Versionen

Die Anforderungen an die Nachvollziehbarkeit nach der GGO beziehen sich auch auf die im Laufe der Bearbeitung durch den Federführenden oder die Beteiligten erstellten Entwurfsversionen. Auch hier ist die Protokollierung von Urheberschaft, Datum der Versionserstellung und Versionsnummer ausreichend.

Protokollierung von Löschung und Änderungen

Darüber hinaus sind alle Änderungen am Aktenbestand, d. h. insbesondere die Löschung, nachvollziehbar, d. h. mit Aktion, Urheberschaft und Datum der Aktion, zu protokollieren.

Protokollierung sonstiger Aktionen

Die Protokollierung lesender Zugriffe ist i. a. nicht erforderlich, datenschutzrechtlich nicht vertretbar und deshalb abzustellen. Ausnahmen, wie z. B. VS-Regelungen sind möglich, werden aber an dieser Stelle nicht erörtert. Sie sind fallspezifisch zu prüfen.

4.2.2 Auswertung von Protokollinformationen

Einschränkung des Zugriffs auf die Protokollinformationen

Durch die elektronische Erfassung ermöglicht die IT-gestützte Vorgangsbearbeitung im Unterschied zur konventionellen Vorgangsbearbeitung, trotz Einschränkung der zu protokollierenden Daten, vielfältige Auswertungen in zu konventioneller Vorgangsbearbeitung nicht vergleichbarer Qualität. Um den möglichen Missbrauch der notwendigen Protokollierung zu verhindern, ist der Lesezugriff, d. h. die Auswertung der Protokollinformation einzuschränken und jegliche Manipulationsmöglichkeit zu unterbinden.

Technisch-organisatorische Maßnahmen

Die Verhinderung von Manipulationen ist bereits Bestandteil des DOMEA®-Anforderungskataloges Version 1.2 (siehe „Zertifizierung nach dem Konzept „Papierarmes Büro (DOMEA®-Konzept)“, Band 53, Schriftenreihe der KBSt). Die Einschränkung des Zugriffs wird in der neuen Version des Anforderungskataloges an Bedeutung gewinnen, so dass auch hier die technischen Voraussetzungen gegeben sein sollten. Aufgabe der Behörde ist aber nach wie vor die Definition eines geeigneten Zugriffsrechtekonzeptes, das auch den Zugriff auf die Protokoll- und Bearbeitungsinformationen regelt.

Im Allgemeinen ist ein Vollzugriff auf die für eine Bearbeitung erfassten Protokoll- und Bearbeitungsinformationen nur für den Bearbeiter selbst und für alle seine Vorgesetzten nötig. Eine pauschale Verfügbarkeit der Protokoll- und Bearbeitungsinformationen auch innerhalb der Organisationseinheit ist nicht sinnvoll (im Unterschied zu den Primär- und Metainformationen, wo der Zugriff mit Hinblick auf ein Informations- und Wissensmanagement mindestens innerhalb der eigenen Organisationseinheit sinnvoll ist).

Ein wirkungsvoller Zugriffsschutz ist dabei nur möglich, wenn Protokollinformationen von übrigen Daten systemtechnisch getrennt vorgehalten und angezeigt werden. Die Trennung sollte derart realisiert sein, dass der Zugriff auf die Protokollinformationen unabhängig vom Zugriff auf sonstige Daten und idealerweise auch weitestgehend unabhängig von allgemeinen Administrationsrechten vergeben werden kann. Zu berücksichtigen ist allerdings, dass der Zusammenhang zwischen Protokollinformation und Primär- bzw. Metadaten selbstverständlich trotz systemtechnischer Trennung erhalten bleiben muss, da nicht nur für die Auswertung, sondern auch für die Aussonderung Protokollinformation sowie Primär- bzw. Metadaten eine zusammenhängende Einheit darstellen. Diese Forderung schränkt die Möglichkeiten der systemtechnischen Trennung ein.

Denkbar wäre aber bspw. die Speicherung in eigenen Datenbanktabellen oder auch in logisch getrennten Speicherbereichen, so dass Administrationsrechte für die Administration der Protokolldaten von anderen Administrationsrechten getrennt werden können.

Hinsichtlich der Auswertung sind neben den Protokolldaten auch insbesondere die Werkzeuge, die das System zur Sichtung und Auswertung von Protokollinformationen zur Verfügung stellt, vor unbefugtem Zugriff zu schützen.

Information der Mitarbeiter darüber, was protokolliert wird

Darüber hinaus sind die betroffenen Bearbeiter über Umfang und Inhalt der automatischen Protokollierung und die Auswertung der Protokollinformationen zu informieren. Dies kann beispielsweise in Zusammenarbeit mit der Personalvertretung oder dem Datenschutzbeauftragten einer Behörde geschehen und sollte in einer Dienstvereinbarung festgehalten werden.

Für die Auswertung der Protokollinformationen durch Berechtigte sind schriftliche Arbeitsanweisungen vorzusehen. Konsequenzen bei Verstößen sind ebenfalls zu regeln.

4.2.3 Aufbewahrung von Protokollinformationen

Löschung der Protokollinformationen kann erst nach Ablauf der Aufbewahrungsfrist erfolgen.

Wie bereits erläutert, ist die Erforderlichkeit der Aufgabenerfüllung Maßstab für die Aufbewahrung von Protokollinformationen. Im Gegenzug besteht nach § 20 Abs. 2 BDSG die Pflicht zur Löschung von Protokollinformationen, wenn für die Aufbewahrung die Erforderlichkeit entfällt. Nach Abschluss der Bearbeitung, d. h. üblicherweise mit der z. d. A. Verfügung, ist Schriftgut für den in der Aufbewahrungsfrist zur Akte oder zum Vorgang definierten Zeitraum in der Behörde für den erneuten Bearbeitungszugriff vollständig vorzuhalten (vgl. §19 Abs. 1 RegR). Dies umfasst auch die Aufbewahrung von Protokollinformationen.

Technisch-organisatorische Maßnahmen

Schutzmaßnahmen bei der Sicherung von Protokollinformationen

Für die langfristige Aufbewahrung von Protokollinformationen ist die Sicherung genau wie für Primär- und Metainformationen unumgänglich. Aufgrund der Missbrauchsmöglichkeiten besteht auch hier ein besonderer Schutzbedarf dieser Informationen, so dass insbesondere bei der Sicherung auf Wechseldatenträgern über Maßnahmen wie Verschlüsselung oder Aufbewahrung in besonders geschützten Bereichen nachgedacht werden sollte.

Nach Ablauf der Aufbewahrungsfrist ist das Schriftgut gemäß den Regelungen des Archivgesetzes der zuständigen Archivbehörde anzubieten und bei Bedarf zu übergeben. In der Behörde wird, nach Prüfung durch die zuständige Archivbehörde und mit schriftlicher Zustimmung der zuständige Archivbehörde, das nicht zu übernehmende Schriftgut vernichtet (vgl. § 22 Abs. 2 RegR und Erweiterungsmodul zum DOMEA®-Organisationskonzept 2.1 „Aussonderung und Archivierung elektronischer Akten“, Schriftenreihe der KBSt, Band 66, Oktober 2004). Die Feststellung, dass die Aufbewahrung von Protokollinformationen nicht mehr erforderlich ist, kann deshalb nur nach Ende dieses Aufbewahrungszeitraums erfolgen. Bei der Löschung ist sicherzustellen, dass sich die Vernichtung auf die entsprechenden Akten, Vorgänge und Dokumente inkl.

der im System bis zu diesem Zeitpunkt vorgehaltenen Protokollinformationen erstreckt.

5 Datenschutzrechtliche Aspekte im IT-gestützten Geschäftsgang

Relevante datenschutzrechtliche Problematiken, die im Zusammenhang mit der Nutzung der IT-gestützten Vorgangsbearbeitung auftreten, werden im Folgenden anhand des Geschäftsgangs beleuchtet. Zu den Problematiken werden die technisch-organisatorische Maßnahmen aufgezeigt, die als Lösungsansätze in Betracht kommen.

Die Phasen des Geschäftsgangs von der Eingangsphase bis zur Archivierung/Aussonderung wurden in Anlehnung an das DOMEA®-Organisationskonzept gewählt und stellen einen typischen Ablauf in der Ministerialverwaltung dar.

5.1 Eingangsphase

In der Eingangsphase werden die Zuständigkeit ermittelt und vorbereitende Tätigkeiten für die Bearbeitung des Geschäftsgangs durchgeführt (z. B. Registrieren von Eingängen).

5.1.1 Empfang externer Eingänge

Unterschiedliche Eingangskanäle beim Empfang externer Eingänge

Außer auf Papier können Eingänge an eine Behörde auf verschiedenen elektronischen Wegen, z. B. über E-Mail oder Web-Formulare, eingehen. Werden die Eingänge einer zentralen Organisationseinheit zugeleitet, d. h. entweder an eine herkömmliche Posteingangsstelle bei papiergebundenen Eingängen oder an ein zentrales E-Mail Postfach bei elektronischen Eingängen, erfolgt dort üblicherweise eine Ersterfassung vor der inhaltlichen Registrierung. Bei einem dezentralen Empfang der elektronischen Eingänge obliegt die Erfassung und Registrierung der Eingänge der Verantwortung des Bearbeiters, der den elektronischen Eingang empfängt bzw. ihn aus einem der Organisationspostkörbe entnimmt (vgl. Organisationskonzept 2.0 Kap. 4.1.12).

In jedem Eingang können personenbezogene Daten enthalten sein (siehe Abbildung):

Behandlung personenbezogener Daten in Eingängen

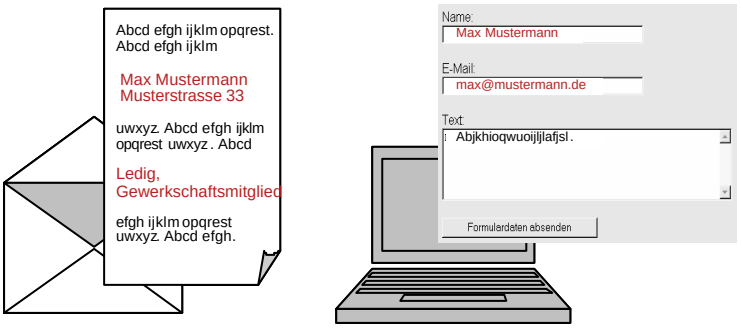


Abbildung 3: Eingang personenbezogener Daten (Beispiele)

Damit besteht bereits beim Empfang externer Eingänge die Gefahr, Grundsätze des Datenschutzes auf verschiedene Weise zu missachten.

5.1.1.1 Datenschutzrechtliche Problematik: Prüfung der Zulässigkeit/Erforderlichkeit in der Eingangsphase

Zulässigkeit der automatischen Erfassung

Werden Eingänge in einer zentralen Posteingangsstelle ersterfasst und ggf. digitalisiert, so werden personenbezogene Daten für die elektronische Weiterverarbeitung aufgenommen, unabhängig davon, ob diese Daten für den Geschäftsgang zulässig und erforderlich sind.

Zulässigkeitsprüfung bei strukturierten Prozessen

Bei strukturierten Vorgängen ist die Problematik der Zulässigkeits- und Erforderlichkeitsprüfung in der Eingangsphase gering einzuschätzen. Denn Behörden sind bei der Bereitstellung eines Formulars angehalten, dezidiert zu prüfen, welche personenbezogenen Daten zur Aufgabenerledigung tatsächlich benötigt werden. Darüber hinaus sollten Behörden auch die bereit gestellten Formulare unter den genannten Aspekten einer datenschutzrechtlichen Würdigung unterziehen. In den nachfolgenden Ausführungen wird davon ausgegangen, dass bei strukturierten Prozessen vor der Entscheidung, personenbezogene Daten in einem Formular zu erheben, bereits eine Prüfung auf Zulässigkeit und Erforderlichkeit erfolgte und somit nur die erforderlichen personenbezogenen Daten enthalten sind und übernommen werden.

Darüber hinaus besteht bei strukturierten Eingängen die Möglichkeit, eine Einverständniserklärung zur zweckgebundenen Erfassung personenbezogener Daten abzufragen. Die Überprüfung dieser im Formular enthaltenen Einverständniserklärung ist auch im Rahmen der Eingangsbehandlung leicht umzusetzen.

Insbesondere bei unstrukturierten Prozessen ist die Zulässigkeitsprüfung kritisch

Die Problematik der Prüfung der Zulässigkeit und Erforderlichkeit in der Posteingangsstelle tritt demnach insbesondere bei Eingängen im Rahmen unstrukturierter Vorgänge auf. Denn im Gegensatz zu strukturierten, d.h. in der Regel formularbasierten Eingängen im Rahmen von Antragsverfahren, ist nicht von vorneherein ersichtlich, welche im Eingang enthaltenen personenbezogenen Daten benötigt werden.

Technisch-Organisatorische Maßnahmen

Zulässigkeitsprüfung kann nur durch den zuständigen Bearbeiter erfolgen

Die Prüfung der in den Eingängen ggf. enthaltenen personenbezogenen Daten auf Zulässigkeit und Erforderlichkeit in der Verarbeitung sollte erst durch den Bearbeiter erfolgen, der über den entsprechenden Sachverstand für die Bearbeitung verfügt. Da der externe Eingang u. U. erst an den entsprechenden Bearbeiter geleitet werden muss, ist es als unverhältnismäßig zu erachten, bereits in der Phase des Empfangs externer Eingänge (unstrukturierte Prozesse) eine sofortige Prüfung der Zulässigkeit und Erforderlichkeit, z. B. im Bereich der zentralen Posteingangsstelle, zu fordern (bzgl. Verhältnismäßigkeit vgl. auch § 9 BDSG).

Folgende technisch-organisatorische Maßnahmen können dazu beitragen, dem missbräuchlichen Umgang mit personenbezogenen Daten in der Eingangsphase entgegenzuwirken:

- Papiergebundene Eingänge werden digitalisiert und an den Empfänger weitergeleitet. Papiergebundene Originale, die Urkunden-

charakter besitzen, werden aufbewahrt. Die Entscheidung ob alle anderen Papieroriginale nach einer Übergangsfrist vernichtet werden oder eine längerfristige Aufbewahrung erfolgen soll, ist behördenspezifisch zu treffen. Überlegungen zur Aufbewahrungen und Vernichtung von Papieroriginalen werden im Erweiterungsmodul zum DOMEA®-Organisationskonzept 2.0 „Scan-Prozesse“, Schriftenreihe der KBSt, Band 64, erörtert.

- Elektronische Eingänge werden direkt an den festgelegten Eingangsempfänger weitergeleitet. Neben einer Person kann dies auch der elektronische Eingangspostkorb einer Organisationseinheit sein. Hierbei ist jedoch zu bedenken, dass die Zugriffsmöglichkeit mehrerer Bearbeiter auf personenbezogene Daten eingeschränkt werden sollte. Möglich wäre in diesem Fall zum Beispiel, dass der Zugriff auf die personenbezogenen Daten erst mit Übernahme in die Bearbeitung, also zu dem Zeitpunkt, wenn ein Bearbeiter einen Eingang aus dem Postkorb der Organisationseinheit entnimmt, freigegeben wird. Vorgangsbearbeitungssysteme bieten dazu die Möglichkeit, Zugriffsrechte im Arbeitsprozess zu ändern.
- Persönlich adressierte, papiergebundene Eingänge werden ungeöffnet und papiergebunden an den Empfänger geleitet. Eine Digitalisierung erfolgt zu einem späteren Zeitpunkt - bei der Bearbeitung durch den Eingangsempfänger.
- Persönlich adressierte, elektronische Eingänge werden direkt an den intendierten Empfänger geleitet.

Die Mitarbeiter in der zentralen Posteingangsstelle werden von Aufgaben im Zusammenhang mit der Wahrung des Datenschutzes durch die o. g. technisch-organisatorischen Maßnahmen entlastet.

Für den Bearbeiter erhöht sich durch die genannten technisch-organisatorischen Maßnahmen die Verantwortung im Umgang mit personenbezogenen Daten. Er entscheidet dagegen im Rahmen der Eingangsbehandlung, welche der vorliegenden personenbezogenen Daten in die IT-gestützte Vorgangsbearbeitung übernommen werden müssen.

5.1.1.2 Datenschutzrechtliche Problematik: Sicherstellung der Zweckbindung personenbezogener Daten

Die schnelle Verbreitung von und der erleichterte Zugriff auf personenbezogene Daten erfordern Maßnahmen zur Sicherstellung der Zweckbindung

Durch das Vorliegen von Eingängen in elektronischer Form bzw. deren Umwandlung in diese Form kann der Grundsatz der Zweckbindung der in den Eingängen enthaltenden personenbezogenen Daten gefährdet sein. So besteht ggf. die Möglichkeit, über eine Recherche in den digitalisierten Papiereingängen, Erhebungen zu generieren, die mit dem einzelnen Geschäftsvorfall an sich in keiner Verbindung stehen (Beispiel: Erhebung der Zahl der Eingänge einer bestimmten Person).

Technisch-organisatorische Maßnahmen

Die nach dem DOMEA®-Konzept zertifizierten Systeme der IT-gestützten Vorgangsbearbeitung sollen informationstechnische Möglichkeiten

bieten, um im Bereich des Empfangs externer Eingänge datenschutzrechtliche Regelungen einzuhalten.

Mit Hinblick auf die Grundsätze Datenvermeidung und Datensparsamkeit kann eine sparsame Erfassung bereits durch einen Verzicht unnötiger Pflichtfelder in den Erfassungsmasken unterstützt werden. Dies bedeutet, dass bei der Konfiguration des Systems, die Definition von Metadaten grundsätzlich unter Berücksichtigung der spezifischen behördlichen Gegebenheiten erfolgen sollte. Die Behörde sollte dabei von den in DOMEA®-zertifizierten Systemen bestehenden Möglichkeiten zur Anpassung der Metadatenfelder auch Gebrauch machen.

Grundsatz der Datensparsamkeit bei der Erfassung

Weitere technisch-organisatorische Maßnahmen zur Wahrung der Zweckbindung bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten unterscheiden sich, je nachdem, ob der Eingang die Behörde über eine zentrale Posteingangsstelle erreicht oder direkt bei einem Bearbeiter eingeht.

Technisch-organisatorische Maßnahmen beim Empfang personenbezogener Daten in einer Posteingangsstelle

Bei einem Eingang über eine Posteingangsstelle (z. B. behördliche Poststelle, zentrale E-Mail-Adresse, E-Mail-Postkorb der Organisationseinheit, zentraler Informationsservice) können folgende Maßnahmen zur Wahrung der Zweckbindung ergriffen werden:

Nachweisführung in zentralen Posteingangsstellen

1. Für die Nachweisführung des Eingangs in der Posteingangsstelle gilt der Grundsatz der Datenvermeidung und Datensparsamkeit. Es werden nur diejenigen personenbezogenen Daten als Metadaten gespeichert, die für eine Nachweisführung unbedingt notwendig sind, so z. B. Name und Anschrift des Absenders (vgl. Organisationskonzept 2.0 Kap. 4.1.3.3).

2. Die elektronische Speicherung der Eingänge als Metadaten in der Posteingangsstelle erfolgt nur so lange, bis der Bearbeiter seine Kenntnisnahme elektronisch bestätigt. Mit der elektronischen Empfangsbestätigung verliert die Posteingangsstelle die Zugriffsrechte auf den Eingang.

3. Die Recherchefunktionalitäten innerhalb der Metadaten in der Posteingangsstelle sind einzuschränken. Über die Recherche nach dem Kriterium eines personenbezogenen Datums (z. B. Vorname, Zuname) ist keine Auswertung quantitativer Art möglich. Dazu zählt zum Beispiel eine Recherche, bei der Informationen darüber gewonnen werden können, wie viele Eingaben eine bestimmte Person an die Behörde gerichtet hat.

Technisch-organisatorische Maßnahmen beim Empfang personenbezogener Daten durch einen Bearbeiter

Bei einem direkten Eingangsempfang durch einen Bearbeiter wird die zentrale Posteingangsstelle übersprungen. Die Problematik der Zweckbindung bei der Erhebung der personenbezogenen Daten stellt sich in diesem Fall nur insofern, als dass der Bearbeiter dafür sensibilisiert sein

Sensibilisierung der Bearbeiter für datenschutzrechtliche Problematik erforderlich

muss, eine Ersterfassung der personenbezogenen Daten als Metadaten ausschließlich für den Zweck der weiteren Verarbeitung durchzuführen.

Eine Sensibilisierung des Bearbeiters für die Wahrung datenschutzrechtlicher Anforderungen kann in Form von Schulungen erfolgen. Insofern empfiehlt es sich, unter Mitwirkung des behördlichen Datenschutzbeauftragten für die entsprechende Fachaufgabe Checklisten zu erstellen, anhand derer der Bearbeiter eine Entscheidung über die Erhebung und Speicherung personenbezogener Daten zum Zweck der weiteren Bearbeitung des Vorgangs trifft.

5.1.2 Eingangsbehandlung

Ziel der Eingangsbehandlung ist die Festlegung der Zuständigkeit für den durch den Eingang angestoßenen Geschäftsgang. Der Eingangsempfänger vermerkt die Kenntnisnahme und prüft die Zuständigkeit. Bei Nichtzuständigkeit wird der Eingang an die zuständige Stelle weitergeleitet.

Nach Prüfung der Zuständigkeit übernimmt der Federführende die Verantwortung für die Durchführung der Bearbeitung. In einem ersten Schritt erfolgt mit der inhaltlichen Sichtung die Überprüfung daraufhin, ob personenbezogene Daten im Eingang enthalten sind. Trifft dies zu, erfolgt eine Prüfung der Zulässigkeit und Erforderlichkeit der Verarbeitung dieser Daten (vgl. Organisationskonzept Kap. 3.2.1).

5.1.2.1 Datenschutzrechtliche Problematik: Trennung der erforderlichen von den nicht-erforderlichen personenbezogenen Daten

Frühzeitige Vernichtung nicht-erforderlicher Daten wird bereits unterstützt

Generell ist eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die für die Bearbeitung einer behördlichen Aufgabe nicht erforderlich sind, nicht zulässig (siehe Kapitel 3.3.2). § 15 Abs. 5 und 6 BDSG bestimmen, dass jedoch auch eine Übermittlung nicht-erforderlicher personenbezogener Daten an öffentliche Stellen zulässig ist, wenn deren Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist (siehe Abbildung).

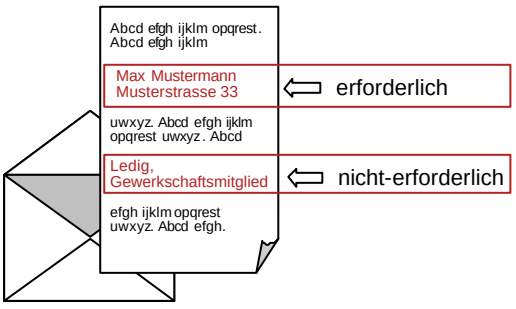


Abbildung 4: Erforderliche und nicht-erforderliche personenbezogene Daten in einem Eingang (Beispiel)

Technisch-organisatorische Maßnahmen

Möglichkeiten zur frühzeitigen Vernichtung nicht-erforderlicher Primärdaten sind durch die Unterstützung des elektronischen Weglegens bereits vorhanden (vgl. DOMEA®-Organisationskonzept).

Die nach dem DOMEA®-Konzept zertifizierten IT-gestützten Vorgangsbearbeitungssysteme bieten einige technisch-organisatorischen Möglichkeiten, um die oben genannte Problematik zu bewältigen:

Entfernung der schützenswerten Daten aus den Primärdaten

Erforderliche personenbezogene Daten werden als Metadaten im Vorgangsbearbeitungssystem erfasst. Es erfolgt eine Kennzeichnung, dass es sich bei diesen Metadaten um personenbezogene Daten handelt (siehe Abbildung). Nicht-erforderliche personenbezogene Daten werden nicht als Metadaten erfasst.

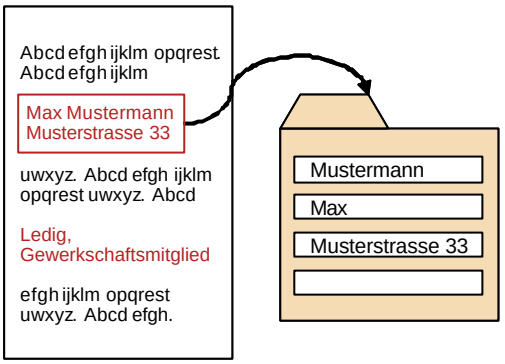


Abbildung 5: Übertrag erforderlicher personenbezogener Daten in den Metadatensatz

Diese Metadaten werden je nach Fall bzw. Ermessen des Bearbeiters dem Dokument, dem Vorgang oder der Akte zugeordnet. Eine gesonderte, zentrale Speicherung der personenbezogenen Daten erfolgt nicht.

5.1.2.2 Datenschutzrechtliche Problematik: Schutz sensibler und besonderer personenbezogener Daten vor der Nutzung und Verarbeitung in Primärinformationen

Da ein Eingang verschiedene personenbezogene Daten enthalten kann, sind im Rahmen der Eingangsbehandlung Maßnahmen zu ergreifen, die auf den Schutz sensibler und besonderer personenbezogener Daten in den Primärinformationen abzielen.

Technisch-organisatorische Maßnahmen

Wie in Kapitel 4.1 beschrieben, werden Dokumente, die besonders schutzwürdige personenbezogenen Daten enthalten, vor einer unzulässigen Nutzung und Verarbeitung durch Dritte geschützt. Es ist behördenspezifisch festzulegen, auf welche Weise dieser Schutz gewährleistet wird.

5.1.2.3 Datenschutzrechtliche Problematik: Revisionssicherheit der behandelten Primärinformationen

Nur reversible Anonymisierung / Pseudonymisierung genügt den Anforderungen an die Revisionsfestigkeit des Schriftguts

Trotz des Grundsatzes, nicht-erforderliche personenbezogene Daten in den Primärinformationen zu anonymisieren oder zu pseudonymisieren, ist von einer generellen und irreversiblen Unkenntlichmachung abzusehen. Denn Primärinformationen müssen ggf. vor Gericht oder bei der Abgabe an das zuständige Archiv im ursprünglichen Zustand vorgelegt werden. Eine Wiederherstellung unterliegt jedoch dem Grundsatz der Zweckbindung und kann daher nur dann ausgeführt werden, wenn ein bestimmter Zweck dies erfordert.

Technisch-organisatorischen Maßnahmen

Systemtechnisch können Anonymisierungen/Pseudonymisierungen in Primärinformationen im Vorgangsbearbeitungssystem revidiert werden.

Die Wiederherstellung kann beispielsweise über einen passwortgeschützten Zugang auf die Primärinformation erfolgen (siehe Abbildung).

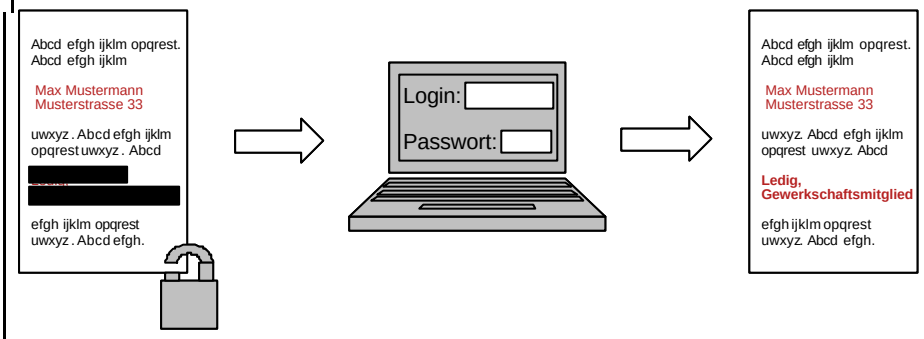


Abbildung 6: Revision anonymisierter personenbezogener Daten in einer Primärinformation

Zur Wahrung der Zweckbindung ist die Wiederherstellung des Originalzustands einer Primärinformationen nur festgelegten Personen zu gewähren (z. B. Datenschutzbeauftragten). Ein Zugriffsrechtekonzept regelt behördenspezifisch die organisatorischen Maßnahmen bei einer notwendigen Einsicht.

Wird eine Anonymisierung/Pseudonymisierung personenbezogener Daten in den Primärinformationen revidiert, so ist zu gewährleisten, dass nur diejenigen personenbezogenen Daten freigegeben werden, die für den auftretenden Zweck erforderlich sind (siehe Abbildung)[5].

[5] Zur Revision von anonymisierten/pseudonymisierten personenbezogener Daten bei der Abgabe an Archive siehe Kapitel 5.3.

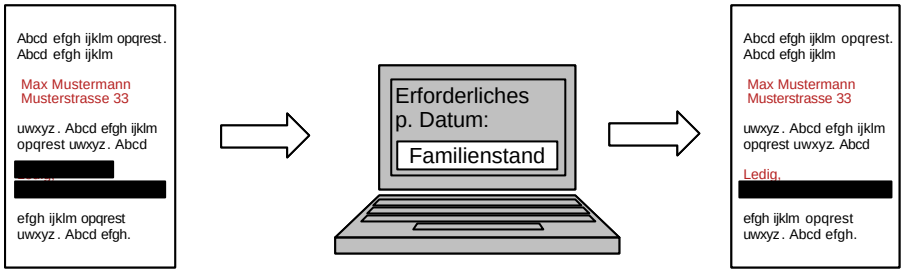


Abbildung 7: Wahrung des Grundsatzes der Erforderlichkeit bei Revision anonymisierter/pseudonymisierter personenbezogener Daten in Primärinformationen

Daher ist es sinnvoll, jedem nicht-erforderlichen Datum bei der Anonymisierung/Pseudonymisierung ein Attribut zu verleihen (z. B. Familienstand). Dieses Attribut sagt etwas über den Charakter des anonymisierten/pseudynomisierten personenbezogenen Datums aus, ohne den Inhalt an sich Preis zu geben. Über eine Eingabemaske kann nach dem Attribut gesucht werden (siehe Abbildung). Bei Vorhandensein des erforderlichen personenbezogenen Datums wird eine Revision durchgeführt. Alle anderen nicht-erforderlichen personenbezogenen Daten bleiben unkenntlich.

5.2 Bearbeitung

Es ist die Aufgabe der federführenden Stelle, zusammen mit evtl. zu beteiligenden Organisationseinheiten und unter Verwendung des verfügbaren Schriftguts, einen Entwurf für einen Entscheidungsvorschlag zu erarbeiten (vgl. DOMEA®-Organisationskonzept Kap. 4.2).

5.2.1 Entwurfserstellung und –abstimmung

Die Bearbeitung erfolgt nach dem Grundsatz der Nachvollziehbarkeit

Die Erstellung eines Entscheidungsentwurfs geschieht unter Beteiligung der nach der Natur der Sache in Betracht kommenden weiteren Stellen bzw. Organisationseinheiten. Für den gesamten Bearbeitungsprozess aus Entwurfserstellung und Abstimmung schreibt § 12 Abs. 3 GGO die Nachvollziehbarkeit eines Sachstands auf Basis der elektronischen Akte vor. Dies umfasst nicht nur die Dokumente einer Akte, sondern nach § 6 Abs. 4 RegR ausdrücklich auch die Historie einer Bearbeitung, d. h. insbesondere die Geschäftsgangvermerke, Verfügungen und Beteiligungen. Die entsprechende Protokollierung erfolgt dabei systemtechnisch weitestgehend automatisch, um Fehler bei der manuellen Erfassung zu vermeiden (vgl. Abschnitt 4.2).

5.2.1.1 Datenschutzrechtliche Problematik: Unbefugte Weitergabe

Die Übermittlung einfacher personenbezogener Daten innerhalb einer Behörde ist nach § 15 Abs. 1 BDSG grundsätzlich zulässig, sofern diese Übermittlung zur Erfüllung der Aufgabe des Dritten erforderlich ist (vgl. Kap. 4.1.1). Sind mit der Weitergabe der erforderlichen personenbezogenen Daten weitere personenbezogenen Daten verbunden, so ist nach §

15 Abs. 5 und 6 BDSG auch deren Übermittlung zulässig, sofern eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Unbefugte Weitergabe personenbezogener Daten erfolgt meist ohne Vorsatz, d. h. Schutzbedarf muss erkennbar sein

Eine unbefugte Weitergabe ist jedoch insbesondere dann festzustellen, wenn bspw. durch die Weitergabe der personenbezogenen Daten das Recht des Betroffenen auf informationelle Selbstbestimmung eingeschränkt wird (vgl. § 15 Abs. 5 BDSG). Üblicherweise erfolgt die unbefugte Weitergabe dabei durchaus ohne Vorsatz, da die Auskunft erteilende Stelle häufig den Schutzbedarf der personenbezogenen Daten nur unzureichend oder gar nicht beurteilen kann. Die Auskunft erteilende Stelle muss deshalb in die Lage versetzt werden

- zu erkennen, ob ein Dokument, ein Vorgang oder eine Akte schützenswerte personenbezogene Daten enthält.
- den Zweck zu dem evtl. vorhandene personenbezogene Daten erfasst wurden, zu ermitteln.
- bei der Notwendigkeit zur Weitergabe von Dokumenten mit schützenswerten personenbezogenen Daten, diese zu anonymisieren bzw. zu entfernen.

Vorgangsbearbeitungssysteme ermöglichen technisch eine Trennung der erforderlichen von den nicht-erforderlichen personenbezogenen Daten vor einer Weitergabe an Dritte.

Technische Maßnahmen zur Sicherstellung der Zweckbindung

Durch die Übernahme der personenbezogenen Daten aus den Primärdaten in spezielle Metadatenfelder kann der Bearbeiter bereits erkennen, ob eine Akte schützenswerte personenbezogene Daten enthält (vgl. Kap. 5.1.2.1). Auch die Anonymisierung bzw. Pseudonymisierung entsprechender Daten wurde bereits behandelt (vgl. Kap. 4.1.2).

In Erweiterung zu den bisher genannten Maßnahmen ist deshalb an dieser Stelle die Erfassung des Zwecks, zu dem personenbezogene Daten gespeichert wurden, erforderlich. Die Zweckerfassung ist dabei so zu gestalten, dass der Zweck, zu dem personenbezogene Daten erfasst wurden, für jedes einzelne Datum zurückverfolgt werden kann. Als Erweiterung der Metadatenfelder für die Erfassung personenbezogener Daten ist deshalb ein Feld für die Erfassung des Zweckes vorzusehen. Dieses kann als Freitext gestaltet werden. Alternativ kann je nach Behörde diskutiert werden, ob statt der Freitexterfassung die Zweckbindung durch einen Verweis auf die entsprechende Stelle des Aktenplans festgehalten wird, welche die der Erfassung zugrunde liegende Aufgabe der Behörde definiert.

5.2.2 Recherche

Recherche ist einer der zentralen Vorteile IT-gestützter Vorgangsbearbeitung

Neben der Beteiligung weiterer Stellen stützt sich die federführende Stelle bei der Entwurfserstellung auf bereits vorhandene Daten. Nach § 15 Abs. 1 RegR ist das für die Arbeit erforderliche Schriftgut dem Bearbeiter bereitzustellen. Insbesondere bei der elektronischen Vorgangsbearbeitung erfolgt die Bereitstellung aber nicht durch die Schriftgutverwaltung, sondern der Bearbeiter selbst führt eine Recherche im Aktenbestand durch. Dafür wird er durch ein DOMEA®-konzeptkonformes Vor-

gangsbearbeitungssystem üblicherweise mit einer Vielzahl von Suchmöglichkeiten unterstützt, mit denen Daten im Aktenbestand effizient und in kürzester Zeit aufgefunden werden können. Die Suchmechanismen berücksichtigen dabei auch die Zugriffsrechte auf den Aktenbestand, so dass Objekte nur dann gefunden werden können, wenn der Bearbeiter auch Leserechte bzw. die in einigen Systemen zur weiteren Differenzierung auch vorhandenen Finderechte auf das Objekte besitzt. Jedoch erweist sich dieses Vorgehen aus datenschutzrechtlicher Sicht als nicht differenziert genug, da eine Kennzeichnung besonders schützenswerter personenbezogener Daten bisher nicht erfolgt, so dass ein Bearbeiter im Rahmen der Recherche darauf unbefugt Zugriff nehmen kann. Dieser unbefugte Zugriff erfolgt dabei ohne Vorsatz, da der Bearbeiter die Existenz schützenswerte Daten vor dem Zugriff nicht absehen kann.

5.2.2.1 Datenschutzrechtliche Problematik: Unbefugter Zugriff auf personenbezogene Daten

Der besondere Schutz personenbezogener Daten erfordert eine strikte Beschränkung möglicher Zugriffe auf diese Daten. Nur wenn Erforderlichkeit und Zulässigkeit der Verarbeitung sichergestellt sind, ist der Zugriff gestattet. Auf der anderen Seite ist der Bearbeiter für die Erfüllung seiner Aufgaben auf die Informationen im Aktenbestand angewiesen. Darüber hinaus ist die Bewertung der Erforderlichkeit oder Zulässigkeit für den Bearbeiter ohne direkten Zugriff nur durch zeitintensive Abstimmungsprozesse möglich. In heutigen Systemen können Zugriffsrechte für Primärdaten nur für das gesamte Dokument vergeben werden. Eine pauschale Sperrung eines Dokumentes ist aber gerade mit Hinblick auf die Anforderungen an ein behördliches Informations- und Wissensmanagement, bei dem die Bereitstellung, der Austausch und damit der Nutzen von Informationen verbessert werden sollen, kontraproduktiv. Eine Beschränkung der Zugriffsrechte zum Schutz personenbezogener Daten muss deshalb möglichst feingranular erfolgen. Dies bedeutet, dass die Sperrung schützenswerter Daten so zu erfolgen hat, dass auch nur die direkt zu schützenden Daten gesperrt werden, ohne das unnötige Einschränkungen beim Zugriff auf nicht schützenswerte Daten bestehen. Dies bezieht sich insbesondere auch auf die Fälle, bei denen schützenswerte und nicht schützenswerte Daten in einem Dokument vorliegen und der Anteil nicht schützenswerter Daten besonders hoch ist (vgl. folgende Abbildung).

Recherche und Schutz personenbezogener Daten schließen sich nicht aus

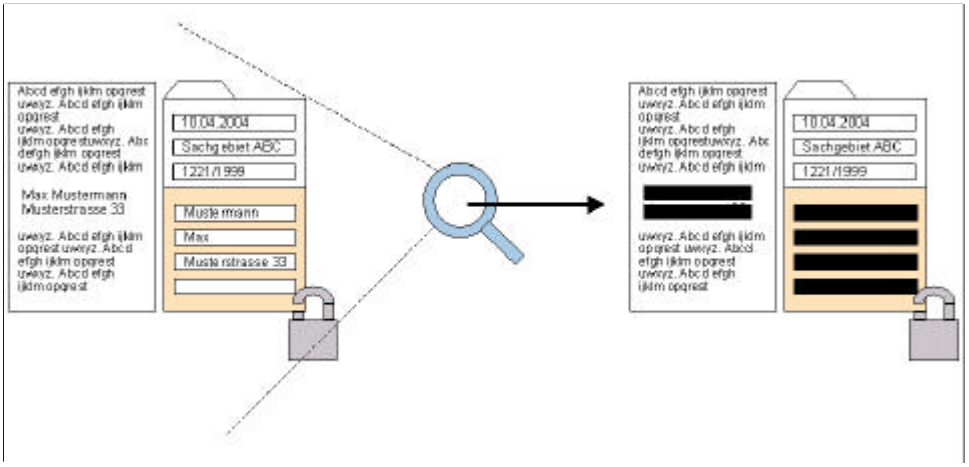


Abbildung 8: Recherche geschützter Daten

Technisch-organisatorische Maßnahmen

Die Umsetzung entsprechend differenzierbarer Zugriffsrechte wurde bereits in Abschnitt 5.1.2.1 und 5.1.2.2 dargestellt. Die Entfernung der personenbezogenen Daten aus den Primärdaten und die systemtechnisch getrennte Aufbewahrung von Primärdaten und personenbezogenen Daten sichert gerade mit Hinblick auf die Recherche einen effizienten Zugriffsschutz, ohne dass der Zugriff auf Primärinformationen unnötig beschränkt werden muss.

Darüber hinaus sind für die erfassten Metadaten Zugriffsrechte feldspezifisch festzulegen. So können schützenswerte und nicht schützenswerte Felder differenziert werden.

5.3 Archivierung

5.3.1 Transferfrist

Zum Zeitpunkt der z.d.A.-Verfügung eines Vorgangs beginnt die Transferfrist. Die Transferfrist beschreibt die Periode, in der z.d.A.-verfügte Objekte direkt wieder in Bearbeitung genommen werden können bzw. im aktiven Dokumentenbestand des Vorgangsbearbeitungssystems vorgehalten werden. Erst nach Ablauf der Transferfrist (vgl. Erweiterungsmodul zum DOMEA®-Organisationskonzept 2.0 „Aussonderung und Archivierung elektronischer Akten“, Schriftenreihe der KBSt, Band 66), die jeweils erneuert wird, sofern der Vorgang während dieser Frist in Bearbeitung genommen wurde (z. B. durch Hinzufügen weiterer Dokumente zum Vorgang), erfolgt die Auslagerung in die elektronische Altregistratur. Die Transferfrist sollte so bemessen sein, dass nach deren Beendigung und der Auslagerung der Akten in die Altregistratur, eine Nutzung der ausgelagerten Akten unwahrscheinlich erscheint. Entsprechend reduziert sind die Anforderungen hinsichtlich der Verfügbarkeit der Akten in der Altregistratur.

Die Dauer der Transferfrist ist behördenspezifisch in einem Metadatenfeld festzulegen und wird der Gesamtaufbewahrungsfrist angerechnet.

5.3.1.1 Datenschutzrechtliche Problematik: Unbefugter Zugriff auf personenbezogene Daten

Sowohl während der Transferfrist als auch nach Auslagerung der Akten in die Altregistratur gelten die gleichen datenschutzrechtlichen Bestimmungen wie bei einer aktiven Akte. Datenschutzrechtliche Probleme, die durch einen unbefugten Zugriff auf die Akte entstehen sowie organisatorische und technische Maßnahmen, um dies zu unterbinden, wurden bereits beschrieben (vgl. Kap. 5.2.2.1).

Bis zur Aussonderung gelten die gleichen Anforderungen wie an in Bearbeitung befindliches Schriftgut

5.3.2 Gesamtaufbewahrungsfrist von Akten

Die Gesamtaufbewahrungsfrist von Akten und Vorgängen ist für die Behörden der Bundesverwaltung aus der „Registraturrichtlinie für das Bear-

Die Festlegung der Aufbewahrungsdauer erfolgt in der Registratur

beiten und Verwalten von Schriftgut in Bundesministerien“[6] abzuleiten. Diese bestimmt sich nach dem Bearbeitungsinteresse und der Wirtschaftlichkeit und ist entsprechend so kurz wie fachlich vertretbar zu bemessen.

Die Gesamtaufbewahrungsfrist von Akten und Vorgängen ist vom zuständigen Registrator bereits beim Anlegen der Akte festzulegen und wird für den Vorgang regelmäßig übernommen. Darüber hinaus sollte zu diesem Zeitpunkt bereits die Transferfrist der Akte bzw. des Vorgangs festgelegt werden (vgl. Kap. 5.3.1). Es sollte im System hinterlegt werden, ob eine Akte bzw. ein Vorgang der zuständigen Archivbehörde anzubieten ist oder direkt vernichtet werden kann (vgl. Kap. 5.3.3).

Die entsprechenden Angaben sind vom Registrator, wie bereits im Erweiterungsmodul zum DOMEA®-Organisationskonzept 2.0 „Aussonderung und Archivierung elektronischer Akten“, Schriftenreihe der KBSt, Band 66, beschrieben, als Metadaten im System zu hinterlegen.

Der Aussonderungsprozess kann auf diese Weise durch die im Vorgangsbearbeitungssystem hinterlegten Daten automatisch angestoßen werden.

5.3.2.1 Datenschutzrechtliche Problematik: Festlegung der Aufbewahrungsdauer

Die Festlegung der Aufbewahrungsdauer berücksichtigt z. Zt. keine datenschutzrechtlichen Aspekte

Die in der Registraturrichtlinie beschriebenen Gesichtspunkte für die Fristbemessung der Aufbewahrung von Akten beziehen sich ausschließlich auf das

- Bearbeitungsinteresse der Behörde („Grad der Zuständigkeit“, „Vorbereitung von Vorschriften oder Verwaltungsvollzug“, „Sicherung von Rechten und Pflichten“, „Bedeutung für die weitere behördliche Arbeit, Art des Schriftguts“) sowie
- Wirtschaftlichkeitsaspekte,

durch welche die Aufbewahrungsfrist so kurz wie zeitlich vertretbar bemessen werden sollte (vgl. RegR Anlage 5).

Die Berücksichtigung datenschutzrechtlicher Aspekte bei der Frage nach der Aufbewahrung behördlichen Schriftguts erfolgt häufig nicht. Auch Hinweise auf die datenschutzrechtlichen Erfordernisse wie die Zweckbindung werden in der Registraturrichtlinie kaum behandelt.

Technisch-organisatorische Maßnahmen

Vorschlag für die Erweiterung der Registraturrichtlinie

Eine Überarbeitung der Registraturrichtlinie unter Berücksichtigung datenschutzrechtlicher Anforderungen ist anzustreben. Damit würde eine wichtige Grundlage für die erforderliche Sensibilisierung der Bearbeiter hinsichtlich datenschutzrechtlicher Probleme erfolgen. Zum einen beinhaltet das die Erweiterung der allgemeinen Bestimmungen um Hinweise, wonach personenbezogene Daten nur entsprechend der zeitlichen Erforderlichkeit und der Zweckbindung vorgehalten werden dürfen. Zum anderen sind auch die in der Registraturrichtlinie getätigten Aussagen über

[6] Auf Länderebene existieren größtenteils eigene Richtlinien für die Aufbewahrung von Schriftgut.

Veränderung der Zweckbindung bei Folgeaspekten der Aktenbearbeitung

die zeitliche Bemessung der Aufbewahrungsdauer dahingehend zu ergänzen, dass die Berücksichtigung datenschutzrechtlicher Anforderungen bei der Frage nach der Aufbewahrung behördlichen Schriftguts überhaupt gestellt wird.

Die Zweckbindung einer Akte ergibt sich neben dem eigentlichen Bearbeitungszweck (z. B. der Antragsbearbeitung und Erstellung eines Genehmigungsbescheides) auch aus Folgeaspekten der Aktenbearbeitung, wie z. B. einer möglichen gerichtlichen Beweisführung eines Antragsverfahrens, das bis zur Verjährungsfrist eines Verfahrens in Kraft treten kann. Diese über die eigentliche Aktenbearbeitung hinausgehende Zweckbindung der Speicherung personenbezogener Daten ist bei der Festlegung der Aufbewahrungsfrist zu berücksichtigen.

Schulung der Bearbeiter zur Sensibilisierung für datenschutzrechtliche Belange

Eine weitere Sensibilisierung des Bearbeiters für die Wahrung datenschutzrechtlicher Anforderungen kann in Form von Schulungen erfolgen. Denkbar wäre es auch, unter Mitwirkung des behördlichen Datenschutzbeauftragten für die entsprechende Fachaufgabe Checklisten zu erstellen, anhand derer der Bearbeiter eine Entscheidung über die Erhebung und Speicherung personenbezogener Daten zum Zweck der weiteren Bearbeitung des Vorgangs trifft.

Darüber hinaus sind die Bearbeiter auf die datenschutzrechtlichen Bestimmungen bei der Aufbewahrung personenbezogener Daten hinzuweisen. Wie oben, beschrieben ist die Sensibilisierung des Bearbeiters für die Wahrung datenschutzrechtlicher Anforderungen, z. B. in Form von Schulungen, erforderlich (vgl. Kap. 4.1.1.2).

Unterstützung bei der Bewertung der datenschutzrechtlichen Relevanz erforderlich

Zusätzlich können im Vorgangsbearbeitungssystem Hinweise zur datenschutzrechtlichen Relevanz der Aufbewahrungsdauer hinterlegt werden. Beispielsweise kann bei einem Eintrag in das Metadatum „Aufbewahrungsdauer“ ein Hinweis aktiviert werden, in dem der Bearbeiter unter Bezugnahme auf datenschutzrechtliche Aspekte darauf hingewiesen wird, dass Akten (und somit deren personenbezogenen Daten) nur so lange aufbewahrt werden dürfen, wie eine Zweckbindung vorhanden bzw. dies fachlich und ggf. rechtlich notwendig ist.

5.3.3 Übergabe der Altakten an die zuständige Archivbehörde sowie Vernichtung von Altakten

In den Archiven werden jene Unterlagen, denen bleibender Wert zukommt, auf Dauer, d. h. auf unbegrenzte Zeit, aufbewahrt. Nach Ablauf der Gesamtaufbewahrungsfrist sind Akten der Behörden den Archiven anzubieten und diesen bei Bedarf auszuhändigen. Akten, die von den Archiven nicht angenommen werden, sind von der Behörde zu vernichten.

Abgabe der originalen Eingänge an die Archivbehörde

Die Übernahme von Schriftgut, welches personenbezogene Daten enthält, durch die Archivbehörde bedeutet dabei, dass die entsprechenden Unterlagen aufgrund des rechtlichen, politischen, wirtschaftlichen, sozialen oder kulturellen Wertes als besondere Quelle für die Erforschung und das Verständnis von Geschichte und Gegenwart dienen. Diese Tatsache entbindet die Behörde von der besonderen datenschutzrechtlichen Schutzverpflichtung und erfordert die vollständige Abgabe des betreffenden Schriftgutes. Entsprechende Regelungen finden sich dabei in den

spezifischen Archivgesetzen. Stellvertretend sei an dieser Stelle auf das Thüringer Archivgesetz § 11 Abs. 2 ThürArchivG verwiesen: „*Anzubieten sind auch Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder über den Datenschutz unterworfen sind. Unberührt bleiben gesetzliche Vorschriften über die Löschung oder Vernichtung unzulässig erhobener oder verarbeiteter Daten oder Unterlagen*."

Grundsätze des Datenschutzes sind auch nach der Abgabe an die Archivbehörde gültig

Die besondere Schutzverpflichtung personenbezogener Daten besteht dabei weiterhin, ist allerdings nach Abgabe nun im Verantwortungsbereich der Archivbehörde.

Nach Übergabe der Daten in die Archivbehörde gelten die datenschutzrechtlichen Aspekte des Bundesarchivgesetzes bzw. die entsprechenden Regelungen der Länder, welche die Rechte Betroffener weitestgehend unberührt lassen. Insbesondere das Recht auf

- Auskunft (vgl. § 4 Abs. 2 BArchG),
- Berichtigung (vgl. § 4 Abs. 3 BArchG),
- Löschung (vgl. § 4 Abs. 1 BArchG),

gilt hier unverändert.

Darüber hinaus sind die Archivbehörden durch das Bundesarchivgesetz zur Prüfung der Erforderlichkeit der Übernahme personenbezogener Daten verpflichtet (vgl. §2 Abs. 4 BArchG). Die Auskunft über personenbezogene Daten ist im Bundesarchivgesetz durch die Sperrfristen (vgl. § 5 BArchG) entsprechend geregelt.

Die Regelungen des Bundesarchivgesetzes wirken sich auf den Umgang mit personenbezogenen Daten in der Behörde aus. Die Altregistratur hat die Akten der zuständigen Archivbehörde in nicht-anonymisierter bzw. -pseudonymisierter Form anzubieten und bei Archivwürdigkeit entsprechend in nicht-anonymisierter bzw. -pseudonymisierter Form abzugeben. Dies bedeutet, dass alle vorgenommenen Anonymisierungen bzw. Pseudonymisierungen personenbezogener Meta- oder Primärdaten (vgl. Kap. 4.1.2.1) reversibel vorgenommen und im Rahmen der Übergabe an das Archiv wieder entfernt werden müssen.

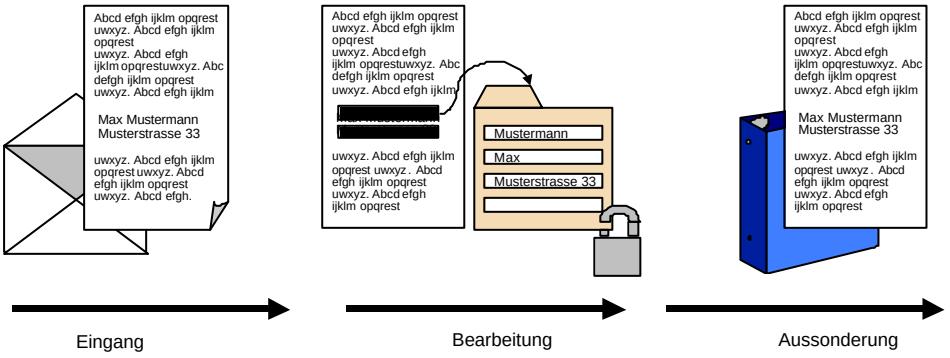


Abbildung 9: Umkehrung der Anonymisierung personenbezogener Daten

Die Aufhebung der Anonymisierung bzw. Pseudonymisierung bedarf in diesem Fall keiner gesonderten organisatorischen Maßnahmen (vgl. Kap.

5.1.2.2), wie beispielsweise einem Vier-Augen-Prinzip. Es muss jedoch nach Aufhebung der Anonymisierung bzw. Pseudonymisierung sowohl durch organisatorische als auch technische Maßnahmen nach wie vor gewährleistet sein, dass Unbefugte keinen Zugriff auf die entsprechenden Daten erlangen. Dies ist i. a. nur dann zu gewährleisten, wenn:

1. die Aufhebung der Anonymisierung bzw. Pseudonymisierung unmittelbar vor der Abgabe an die Archivbehörde erfolgt, d. h. nur die übermittelten und nicht die für die Bearbeitung in der Behörde vorgehaltenen Daten in nicht-anonymisierter bzw. -pseudonymisierter Form vorliegen.
2. die Übermittlung der Daten an die Archivbehörde entsprechend hohen Sicherheitsanforderungen genügt (vgl. Erweiterungsmodul zum DOMEA®-Organisationskonzept 2.1 „Inner- und Interbehördliche Kommunikation“, Schriftenreihe der KBSt, Band 65, November 2005).

5.3.3.1 Datenschutzrechtliche Problematik: Archivierung personenbezogener Daten

Langfristige Aufbewahrung personenbezogener Daten

Der Zweck und damit die Zulässigkeit der Speicherung personenbezogener Daten endet, wie bereits erwähnt, wenn die gesetzliche Frist zur Aufbewahrung der jeweiligen Akte ausläuft. Bekundet die Archivbehörde nach Ablauf der Aufbewahrungsfrist Interesse an der Akte, hat die speichernde Stelle ihrer gesetzlichen Pflicht entsprechend die Unterlagen an das Archiv zu übermitteln. Aus datenschutzrechtlicher Sicht ist es problematisch, dass sowohl die Übermittlung als auch die anschließende Archivierung mit dem Recht auf informationelle Selbstbestimmung (vgl. Kap. 3.4) des Betroffenen kollidieren. Besteht jedoch ein erhebliches Allgemeininteresse an der Akte zu Zwecken der Forschung, Bildung oder Rechtssicherheit, ist dies dem Interesse an der informationellen Selbstbestimmung des Einzelnen aus Sicht des Gesetzgebers vorzuziehen. Aus diesem Grund sind die Archive – wie bereits in Kapitel 5.3.3 erwähnt – bei der Verarbeitung, Nutzung und Übermittlung von Daten ebenfalls an die Grundsätze des Datenschutzes gemäß Bundesarchivgesetz gebunden.

5.3.3.2 Datenschutzrechtliche Problematik: Physische Löschung der personenbezogenen Daten

Löschung aller Daten nach Abgabe bzw. Aussonderung

Nachdem die Akten an die zuständige Archivbehörde übergeben wurden, sind alle personenbezogenen Daten inkl. der Protokollinformationen der Akten in der aktenführenden Behörde irreversibel zu löschen. Dies bedeutet, dass die Daten nicht nur logisch, sondern auch physisch vom Datenträger gelöscht werden müssen. Diese Vorgabe stellt insbesondere bei ReadOnly-Medien ein grundsätzliches Problem dar, da auf diesen Speichermedien die physische Löschung ausgewählter Datensätze nicht möglich ist. Vielmehr ist bei der Archivierung der Daten dafür Sorge zu tragen, dass die Datensätze nach entsprechend definierten Kriterien (z. B. „Aussonderungsart“ oder „Aufbewahrungsdauer“) sortiert, jeweils auf einem Datenträger gespeichert werden. Nach Ablauf der Aufbewahrungsdauer kann dann der gesamte Datenträger vernichtet werden (vgl. Erweiterungsmodul zum DOMEA®-Organisationskonzept 2.0 „Aussonde-

rung und Archivierung elektronischer Akten“, Schriftenreihe der KBSt, Band 66, und „Technische Aspekte der Archivierung elektronischer Akten“, Schriftenreihen der KBSt, Band 67).

Werden diese organisatorischen Anforderungen an die Speicherung von Altakten nicht eingehalten, so ergibt sich das Problem, dass sobald die Aufbewahrungsdauer einer Altakte erreicht wird, alle weiteren auf dem Datenträger gespeicherten Daten auf einen neuen Datenträger zu kopieren sind (Reorganisation), bevor der ursprüngliche Datenträger entsprechend vernichtet werden kann.

6 Umgang mit Rechten der Betroffenen im IT-gestützten Geschäftsgang

Der Betroffene, dessen personenbezogene Daten im Geschäftsgang erhoben werden, kann verschiedene Rechte bezüglich der Erhebung, Verarbeitung und Nutzung dieser Daten in Anspruch nehmen (vgl. Kap. 3.4).

Im Folgenden wird erläutert, wie Vorgangsbearbeitungssysteme eine technisch-organisatorische Unterstützung für die Wahrung von Rechten der Betroffenen leisten können.

6.1 Recht auf Auskunft

Das Bundesdatenschutzgesetz bestimmt, dass Betroffene auf Antrag Information über ihre gespeicherten und verarbeiteten personenbezogenen Daten erhalten können (vgl. Kap. 3.4). Dabei ist der Antragsteller verpflichtet, die Art der personenbezogenen Daten, über die Auskunft erteilt werden sollen, näher zu spezifizieren (z. B. Auskunft über die Speicherung des Familienstandes) (vgl. § 19 Abs. 1 BDSG).

Das Auskunftsrecht macht eine IT-Unterstützung notwendig. Denn auf konventionellem Wege ist eine umfassende Auskunftserteilung über die in der Behörde vorgehaltenen personenbezogenen Daten einer Person kaum möglich.

Effektive Umsetzung des Auskunftsrecht erfordert IT-Unterstützung

Vorgangsbearbeitungssysteme ermöglichen über Suchfunktionalitäten technisch eine Auskunftserteilung.

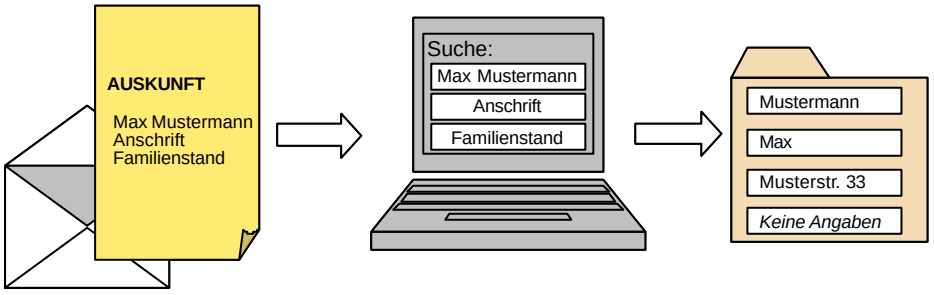


Abbildung 10: Suche nach personenbezogenen Daten für die Auskunftserteilung

Die Suchfunktionalitäten beschränken sich auf den Bereich der Metadaten, da für diese Daten ein Zweck und eine Erforderlichkeit der Speicherung nachgewiesen werden kann. Eine Auskunftserteilung über personenbezogene Daten, die lediglich in den Primärinformationen vorliegen, weil sie im Rahmen der Eingangsbehandlung als nicht-erforderlich eingestuft wurden, ist nach § 19 Abs. 2 BDSG nicht notwendig. Daher sind Suchfunktionalitäten für den Bereich der Primärinformationen nicht erforderlich.

Die Suchfunktionalitäten sind im Sinne des Datenschutzrechts so aufzubauen, dass bei der Suche Ergebnisse erzielt werden, die ausschließlich der auskunftssuchenden Person zugerechnet werden können. Eine Suche anhand eines personenbezogenen Datums, z. B. Nachname, greift daher zu kurz. Es würden u. U. Suchergebnisse auftreten, die unterschiedlichen Personen zugeordnet werden können. Die Suchfunktion muss daher die Eingabe von mindestens zwei Suchbegriffen verlangen.

Da der Auskunftssuchende verpflichtet ist, die Art der von ihm gespeicherten personenbezogenen Daten anzugeben, erstreckt sich die Auskunftserteilung ausschließlich auf diese Daten. Für die Suche folgt daraus, dass lediglich diejenigen personenbezogenen Daten in den Suchergebnissen angezeigt werden dürfen, die erfragt werden.

Das Verlangen einer Auskunftserteilung kann sich auch auf den Ursprung der personenbezogenen Daten, den Zweck der Speicherung sowie die behördlichen Empfänger erstrecken. Dies bedingt eine technische Verknüpfbarkeit der gespeicherten personenbezogenen Daten mit dem damit verbundenen Geschäftsgang. Erfolgt die Speicherung der personenbezogenen Daten als Metadaten zum Vorgang, stellt dies aber kein technisches Hindernis dar.

Die Auskunftserteilung über gespeicherte personenbezogene Daten ist organisatorisch so zu gestalten, dass lediglich ein festgelegter Personenkreis innerhalb der Behörde eine Suche innerhalb der Metadaten durchführen darf (z. B. Datenschutzbeauftragten). Ein Zugriffsrechtekonzept regelt behördenspezifisch die organisatorischen Maßnahmen der Auskunftserteilung.

6.2 Recht auf Benachrichtigung

Werden Daten ohne Kenntnis des Betroffenen und ohne gesetzliche Notwendigkeit erhoben, besteht die Pflicht zur Benachrichtigung der Betroffenen durch die datenerhebende Stelle. Für eine Behörde ist dieser Fall i. a. zu vernachlässigen, da eine Erhebung im Rahmen einer behördlichen Fachaufgabe üblicherweise durch gesetzliche Vorgaben geregelt ist oder eben mit Kenntnis des Betroffenen, d. h. durch Übermittlung der Daten an die Behörde, erfolgt.

Löschung aller Daten nach Abgabe bzw. Aussonderung

Ist im Sonderfall eine Behörde trotzdem dazu verpflichtet, einen Betroffenen über die Erhebung, Speicherung und Verarbeitung seiner personenbezogenen Daten zu unterrichten, kann eine Nachweisführung erfolgen, zu welchen personenbezogenen Daten der Betroffene benachrichtigt wurde.

6.3 Recht auf Berichtigung

Eine Behörde ist u. U. dazu verpflichtet, personenbezogene Daten zu berichtigen (vgl. Kap. 3.4).

Eine Berichtigung unrichtiger personenbezogener Daten ist in Vorgangsbearbeitungssystemen technisch möglich. Die in den Metadaten gespeicherten personenbezogenen Daten werden über das

Vorgangsbearbeitungssystem berichtigt. Dabei kann es erforderlich sein, die unrichtigen personenbezogenen Daten über eine Suche aufzurufen (siehe Abbildung). Die notwendigen Funktionalitäten zur Suche personenbezogener Daten wurden in Kapitel 6.1 erläutert.

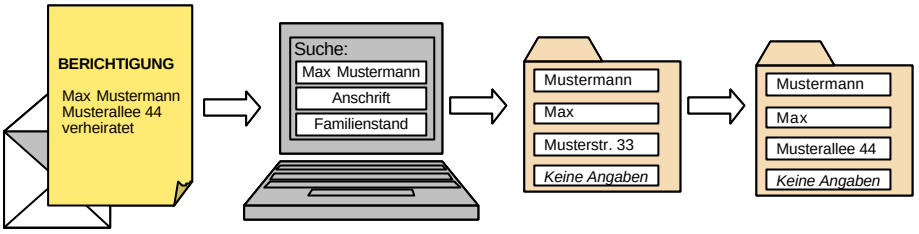


Abbildung 11: Berichtigung personenbezogener Daten in den Metadaten im Vorgangsbearbeitungssystem

Die Berichtigung personenbezogener Daten ist organisatorisch so zu gestalten, dass lediglich ein festgelegter Personenkreis innerhalb der Behörde dies durchführen darf (z. B. Datenschutzbeauftragte). Das Zugriffsrechtekonzept regelt behördenspezifisch die organisatorischen Maßnahmen der Berichtigung. Für den elektronischen Vermerk gelten dabei die gleichen Anforderungen hinsichtlich Zugriffsbeschränkungen etc., wie für das betreffende personenbezogene Datum.

Nachweis der Unrichtigkeit als Vermerk

Eine Berichtigung der Eingänge ist nicht möglich. Hier erfolgt nach § 20 Abs. 1 S. 2 BDSG die Festhaltung der Unrichtigkeit. Diese Nachweisführung kann durch das Anbringen eines elektronischen Vermerks in den Primärinformationen erfolgen (siehe Abbildung).

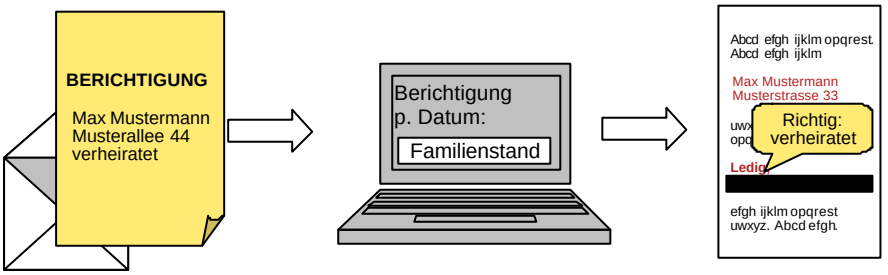


Abbildung 12: Berichtigung personenbezogener Daten in den Primärinformationen

Je nach Auswirkung auf die Interessen des Betroffen kann darüber hinaus eine Sperrung der Eingänge gemäß § 20 Abs. 6 BDSG notwendig sein. In diesem Fall ist mit den in Vorgangsbearbeitungssystemen bereits vorhanden Möglichkeiten die Zugriffsberechtigung, d. h. insbesondere auch der Lesezugriff für den Bearbeiter, auf entsprechende Daten einzuschränken.

6.4 Recht auf Löschung und Sperrung

Technisch-organisatorische Maßnahmen zur Wahrung des Rechts auf Löschung und Sperrung personenbezogener Daten wurden in Kapitel 5.2.1.1 erläutert.

7 Zusammenfassung

In den vorangegangenen Kapiteln wurden verschiedene Maßnahmen zur Bewältigung datenschutzrechtlicher Anforderungen vorgestellt. Dabei wurde auch deutlich, dass spezielle datenschutzrechlich begründete Maßnahmen nur für einen kleinen Teil des Datenbestandes einer Behörde erforderlich sind. Der Großteil der Dokumente, nämlich die ohne personenbezogene Daten und die mit einfachen personenbezogenen Daten, ist durch die Möglichkeiten der Zugriffsbeschränkung in Vorgangsbearbeitungssystemen bereits hinreichend geschützt. Selbst für Dokumente mit sensiblen und besonderen personenbezogenen Daten können hinreichende Schutzmaßnahmen durch restriktive Beschränkung des Zugriffs in Vorgangsbearbeitungssysteme erreicht werden. Lediglich mit Hinblick auf die Erfordernisse eines Informations- und Wissensmanagements sind für die feingranulare Zugriffsbeschränkung weiterführende Maßnahmen erforderlich.

Die Darstellung der Maßnahmen aus dem Geschäftsgang heraus diente dabei der Verdeutlichung der unterschiedlichen Problemstellungen in Bezug auf die IT-gestützte Vorgangsbearbeitung. Da jedoch der dargestellte Geschäftsgang nur i. S. eines Musterprozesses gesehen werden kann, der je nach Behörde in unterschiedlicher Art und Weise Anwendung findet, werden die vorgestellten Maßnahmen im Folgenden nochmals gelistet und statt im Kontext des Mustergeschäftsgang, den in Kapitel 3 dargestellten Grundsätzen des Datenschutzes zugeordnet. Auf diese Weise soll das Potenzial der dargestellten Maßnahmen zur Bewältigung datenschutzrechtlicher Anforderungen verdeutlicht werden.

	Maßnahme	Org./ Tech.	vgl. Kap.
Sicherstellung der Zulässigkeit			
	Prüfung der Zulässigkeit durch den Bearbeiter	O	5.1.1
	Sensibilisierung der Bearbeiter durch Schulungen	O	5.1.1
	Frühzeitiges Löschen bzw. Weglegen	O / T	5.1.2
	Regelungen für die Beschränkung der automatischen Protokollierung und Beschränkung der Auswertung der Protokolldaten mit Hinblick auf unbedingte Notwendigkeiten	O / T	4.2.1
Sicherstellung der Erforderlichkeit			
	Prüfung der Erforderlichkeit durch den Bearbeiter	O	5.1.1
	Sensibilisierung der Bearbeiter durch Schulungen	O	5.1.1

	Arbeitsanweisungen für die Auswertung der Protokolldaten	O	4.2.2
	Berücksichtigung des Datenschutzes bei der Festlegung von Aufbewahrungsfristen und entsprechende Überarbeitung der RegR	O	5.3.2
Sicherstellung Datenvermeidung und -sparsamkeit			
	Anpassung der Erfassungsmasken an den konkreten Bedarf	T	5.1.1
	Frühzeitiges Löschen bzw. Weglegen	O / T	5.1.2
	Regelungen für die Beschränkung der automatischen Protokollierung mit Hinblick auf unbedingte Notwendigkeiten	O	4.2.1
Sicherstellung der Zweckbindung			
	Verschiedene Maßnahmen zur direkten Übernahme der Eingänge durch den Bearbeiter	O	5.1.1
	Einschränkung der Nachweisführung in der Eingangsbehandlung auf das unbedingt Nötige	O / T	5.1.1
	Trennung personenbezogene Daten / nicht-personenbezogene Daten und entsprechende Einschränkung/Parametrisierung der Recherche	T	5.1.2
	(Reversible) Anonymisierung / Pseudonymisierung personenbezogener Daten	T	5.3.3
	Erfassung und Darstellung des Zweckes zu dem personenbezogene Daten gespeichert wurden	T	5.2.1
Sicherstellung der Transparenz			
	Information des Bearbeiters über den Umfang der Protokollierung	O	4.2.2
	Trennung personenbezogene Daten / nicht-personenbezogene Daten und entsprechende Einschränkung/Parametrisierung der Recherche	T	5.2.2
Sonstiges			
	Trennung Protokolldaten / Primär- u. Metadaten	T	4.2.2

	Verschlüsselung von zu sichernden Protokolldaten	T	4.2.3
	Getrennte Speicherung der unmodifizierten Originalinformation	T	5.1.2