B 1.5 Datenschutz

Die Verfassung der Bundesrepublik Deutschland gewährleistet das Recht der Bürgerinnen und Bürger, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen. Aufgabe des Datenschutzes ist es nach § 1 Bundesdatenschutzgesetz (BDSG), "den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird". In den Datenschutzgesetzen der Länder finden sich ähnliche Aufgabenumschreibungen zum Schutz des "Rechts auf informationelle Selbstbestimmung". Das gesamte Datenschutzrecht bezieht sich nur auf personenbezogene Daten. Darunter sind "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" zu verstehen. Juristische Personen werden nicht erfasst.

Rechtliche Rahmenbedingungen bei der Verarbeitung personenbezogener Daten

Die folgenden Ausführungen beziehen sich ausschließlich auf deutsches Recht. Das jeweils im Einzelfall anzuwendende Recht richtet sich danach, ob die Daten verarbeitende Stelle eine öffentliche Stelle des Bundes, eines Landes oder ein privates nicht öffentliches Unternehmen ist. Für öffentliche Stellen des Bundes und für private Unternehmen gilt das Bundesdatenschutzgesetz, für öffentliche Stellen der Länder das jeweilige Landesdatenschutzgesetz. Die Struktur der Datenschutzgesetze ist weitgehend einheitlich, der Regelungsinhalt ist jedoch in einigen Bereichen unterschiedlich. Dies gilt für die Grundbegriffe der Datenverarbeitung, für die Zulässigkeit der Datenverarbeitung aufgrund einer Rechtsvorschrift oder einer Einwilligung und für die Rechte der Bürger. Darüber hinaus gibt es bereichsspezifische Spezialgesetze, die gegenüber den Regelungen der Bundes- und Landesdatenschutzgesetze vorrangig sind (z. B. Sozialgesetzbuch, Straßenverkehrsgesetz, Meldegesetze, Polizeigesetze).

Die folgenden Ausführungen beziehen sich auf die Vorschriften des BDSG und haben daher Geltung für öffentliche Stellen des Bundes und private Unternehmen. Bei öffentlichen Stellen der Länder sind die einzelnen Landesdatenschutzgesetze zu beachten.

Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten, landesspezifische Besonderheiten

Die Erhebung, Verarbeitung und Nutzung personenbezogener (bzw. - beziehbarer) Daten ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Einwilligung ist regelmäßig schriftlich zu erteilen. Zuvor ist der Betroffene auf den Zweck der Verarbeitung hinzuweisen. Bereits als Vorfrage für die Zulässigkeit der Datenverarbeitung ist von Bedeutung, ob überhaupt personenbezogene Daten benötigt werden. Gestaltung und Auswahl von Datenverarbeitungsprogrammen haben sich nämlich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Dabei ist insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen.

Weiterhin sind die Grundsätze der Erforderlichkeit und Zweckbindung der Datenverarbeitung zu berücksichtigen. Danach ist die Datenverarbeitung nur zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist. Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden. Die Verarbeitung darf nur für vorher festgelegte Zwecke erfolgen. Eine Datenerhebung und -speicherung für noch nicht festgelegte Zwecke ist unzulässig. Zweckänderungen sind allein in den im Gesetz genannten Ausnahmefällen möglich.

Generell ist darauf hinzuweisen, dass Landesdatenschutzgesetze in den jeweiligen Zusammenhängen unterschiedliche Abweichungen aufweisen, die im Einzelnen zu berücksichtigen sind.

Datengeheimnis, Verpflichtung auf den Datenschutz, Unterrichtung

Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Bei nicht öffentlichen Stellen sind die Beschäftigten bei Aufnahme ihrer Tätigkeit nach § 5 BDSG auf das Datengeheimnis zu verpflichten. Im öffentlichen Bereich bedarf es beim Bund und in den meisten Ländern keiner förmlichen Verpflichtung mehr. Hier greift eine entsprechende datenschutzrechtliche Unterrichtung. Auf Ausnahmen in den Landesdatenschutzgesetzen ist zu achten.

Technische und organisatorische Maßnahmen

Zum Schutz der personenbezogenen Daten sind von den Daten verarbeitenden Stellen die notwendigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Insbesondere sind dazu die in der Anlage zu § 9 BDSG enthaltenen "Gebote" einzuhalten, die 8 Kontrollziele (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Einhaltung der Zweckbestimmung) vorgeben. Die zu ergreifenden Maßnahmen werden im Gesetz nicht konkret beschrieben, da ihre Eignung vom jeweiligen Anwendungsfall und dem Schutzbedarf der personenbezogenen Daten abhängig ist und die technischen Maßnahmen einem permanenten Wandel unterliegen. Die in den Landesdatenschutzgesetzen enthaltenen Kontrollziele weichen von den Zielen des BDSG teilweise ab, teilweise werden abstraktere Ziele der informationstechnischen Sicherheit benannt und die konkrete Umsetzung in Sicherheitskonzepten verlangt.

Besondere Datenarten, Vorabkontrolle, automatisierte Einzelentscheidungen oder Abrufverfahren

Weist eine Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen auf wie z. B. die Verarbeitung besonderer Datenarten (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) oder soll damit die Persönlichkeit des Betroffenen einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens bewertet werden, ist vor dem Beginn der Verarbeitung eine Vorabkontrolle durchzuführen (§ 4d Abs. 5 BDSG). Eine Vorabkontrolle ist nicht durchzuführen, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. In manchen Landesdatenschutzgesetzen ist eine Vorabkontrolle generell bei allen Verfahren vorgeschrieben, mit denen personenbezogene Daten durch öffentliche Stellen verarbeitet werden. Die Voraussetzungen hierfür können von den beim Bund geltenden Regelungen abweichen.

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen (§ 6a Abs. 1 BDSG).

Besonderer Schutzbedarf besteht auch bei automatisierten Abrufverfahren. Bei diesen Online-Verfahren trägt die empfangende Stelle die Verantwortung für die Zulässigkeit des Abrufs (§ 10 Abs. 4 Satz 1 BDSG). In manchen Landesdatenschutzgesetzen ist die Einrichtung von automatisierten Abrufverfahren an besondere rechtliche Voraussetzungen geknüpft.

Rechte der Betroffenen

Die Betroffenen haben nach dem BDSG und den landesspezifischen Datenschutzgesetzen insbesondere die folgenden Rechte:

- Recht auf Auskunft über die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden und den Zweck der Speicherung.
- Recht auf Berichtigung, wenn unrichtige Daten gespeichert werden.
- Recht auf Sperrung, soweit die Richtigkeit der Daten vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.
- Recht auf Löschung, wenn die Speicherung der Daten unzulässig ist oder die Daten nicht mehr benötigt werden. An die Stelle einer Löschung tritt eine Sperrung, soweit Aufbewahrungsfristen entgegenstehen, der Grund zur Annahme besteht, dass die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigen würde oder die Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohen Aufwand möglich ist.
- Recht auf Widerspruch gegen die Datenverarbeitung wegen der besonderen persönlichen Situation des Betroffenen, sofern die Datenverarbeitung nicht durch eine Rechtsvorschrift verlangt wird.
- Recht auf Schadensersatz wegen einer unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten.

Diese Rechte können nicht durch Verträge oder sonstige Rechtsgeschäfte ausgeschlossen oder beschränkt werden.

Darüber hinaus kann sich der Betroffene zu Fragen des Datenschutzes auch an den betrieblichen bzw. behördlichen Datenschutzbeauftragten (bDSB) oder die jeweils zuständige Aufsichtsbehörde wenden. Niemand darf benachteiligt oder gemaßregelt werden, weil er sich an den Datenschutzbeauftragten oder die Aufsichtsbehörde gewandt hat. Form- und Fristerfordernisse bestehen nicht.

Ansprechpartner und Kontrollen

Die Einhaltung der datenschutzrechtlichen Bestimmungen wird durch Datenschutz-Kontrollinstanzen überprüft:

Die betrieblichen oder behördlichen Datenschutzbeauftragten sind für die interne Datenschutzkontrolle zuständig. Sie sind der Unternehmens-/Behördenleitung unmittelbar zu unterstellen und bei der Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Die Beauftragten für den Datenschutz wirken auf die Einhaltung der Vorschriften über den Datenschutz hin. Ihnen ist von der verantwortlichen Stelle eine Übersicht über die automatisierten Verfahren im Betrieb/in der Behörde zur Verfügung zu stellen. Den größten Teil dieser Angaben hat der betriebliche Datenschutzbeauftragte jedermann in geeigneter Weise verfügbar zu machen. Der betriebliche/behördliche Datenschutzbeauftragte kann sich in Zweifelsfällen an die für die Datenschutzkontrolle zuständige Behörde wenden.

Der Bundesbeauftragte für den Datenschutz ist für die öffentlichen Stellen im Bundesbereich zuständig. Dazu gehören die Behörden der Bundesverwaltung und die sonstigen öffentlichen Stellen des Bundes, auch die bundesunmittelbaren Körperschaften. Seine Hauptaufgabe besteht darin, diese öffentlichen Stellen zu beraten und zu kontrollieren.

Die Landesbeauftragten für den Datenschutz sind zuständig für die Beratung und Überwachung der Behörden der Landesverwaltung und der sonstigen öffentlichen Stellen des Landes, wozu auch die Kommunalverwaltungen gehören.

Die Datenschutzaufsichtsbehörden für die nicht öffentlichen Stellen übernehmen im Bereich der Wirtschaft die Beratung und Überwachung. In einem Teil der Bundesländer wird diese Aufgabe durch die Landesdatenschutzbeauftragten wahrgenommen. In den anderen Bundesländern ist die Aufgabe bei dem jeweils zuständigen Ministerium, meistens dem Innenministerium, angesiedelt.

Die Anschriften der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzaufsichtsbehörden für die nicht öffentlichen Stellen sind zu finden unter www.datenschutz.de.

Datenschutz in den IT-Grundschutz-Katalogen

Die in den IT-Grundschutz-Katalogen in den anderen Bausteinen enthaltenen Maßnahmen dienen der Informationssicherheit und damit auch dem Schutz von personenbezogenen Daten. Die nachfolgend dargestellten Gefährdungslagen beschränken sich auf zusätzliche Gefährdungen aus Sicht des Datenschutzes. Entsprechende Maßnahmen dazu werden anschließend empfohlen.

Wegen der oft schwierigen Rechtslage bei Datenschutzfragen in allgemeinen oder spezialrechtlichen Regelungen sollte zur Beurteilung der gesetzlichen Anforderungen und der daraus folgenden Maßnahmen für das IT-Sicherheits- und Datenschutzkonzept fachkundige Unterstützung in Anspruch genommen werden.

Gefährdungslage:

Gefährdungen im Umfeld des Datenschutzes können vielfältiger Natur sein. Stellvertretend für diese Vielzahl der Gefährdungen werden in diesem Baustein die folgenden typischen Gefährdungen betrachtet:

- G 6.1 Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten
- G 6.2 Nichteinhaltung der Zweckbindung bei der Verarbeitung personen-bezogener Daten
- G 6.3 Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten
- G 6.4 Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten
- G 6.5 Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten
- G 6.6 Fehlende oder nicht ausreichende Vorabkontrolle
- G 6.7 Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten
- G 6.8 Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten
- G 6.9 Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen
- G 6.10 Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten
- G 6.11 Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland
- G 6.12 Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten
- G 6.13 Fehlende oder unzureichende Datenschutzkontrolle

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen eines Datenschutzmanagements müssen die rechtlichen Rahmenbedingungen beachtet und geeignete technische und organisatorische Maßnahmen getroffen werden, um den Datenschutz sicher zu stellen. Dazu gehören Maßnahmen in der Planungs- und Konzeptionsphase, im Zuge der Umsetzung, sowie beim Betrieb von IT-Systemen und -Verfahren.

Nachfolgend wird das ergänzende Maßnahmenbündel für den Bereich Datenschutz vorgestellt, das für alle IT-Systeme und IT-Verfahren anzuwenden ist, mit deren Hilfe personenbezogene Daten verarbeitet werden:

Planung und Konzeption

- M 7.1 (C) Datenschutzmanagement
- M 7.2 (B) Regelung der Verantwortlichkeiten im Bereich Datenschutz
- M 7.3 (A) Aspekte eines Datenschutzkonzeptes
- M 7.4 (A) Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten
- M 7.5 (A) Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

Umsetzung

- M 7.6 (A) Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezoge ner Daten
- M 7.7 (A) Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten
- M 7.8 (A) Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten
- M 7.9 (C) Datenschutzrechtliche Freigabe
- M 7.10 (A) Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezoge ner Daten
- M 7.11 (A) Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten
- M 7.12 (A) Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung per sonenbezogener Daten

Betrieb

- M 7.13 (Z) Dokumentation der datenschutzrechtlichen Zulässigkeit
- M 7.14 (A) Aufrechterhaltung des Datenschutzes im laufenden Betrieb
- M 2.110 (A) Datenschutzaspekte bei der Protokollierung
- M 7.15 (A) Datenschutzgerechte Löschung/Vernichtung

G 6.1 Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat.

Es besteht die Gefahr, dass personenbezogene Daten rechtswidrig verarbeitet werden, wenn keine ausreichende Rechtsgrundlage (Einwilligung oder gesetzliche Erlaubnis, z. B. durch Datenschutzgesetze, Sozialgesetzbuch, Schulgesetze, Polizeigesetze, Krankenhausgesetze) gegeben ist. Ergänzend wird auch auf die Gefährdung G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen* verwiesen.

Eine Verarbeitung personenbezogene Daten ohne ausreichende Rechtsgrundlage kann eine Geldbuße oder Freiheitsstrafe zur Folge haben bzw. zu dienst- oder arbeitsrechtlichen Konsequenzen führen. Der Betroffene kann ein Recht auf Schadensersatz geltend machen.

G 6.2 Nichteinhaltung der Zweckbindung bei der Verarbeitung personen-bezogener Daten

Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben oder erstmals gespeichert worden sind. Es besteht die Gefahr, dass diese Daten auch für andere Zwecke verarbeitet werden, da damit der Aufwand für eine erneute Erhebung und Information der Betroffenen erspart werden kann.

Werden personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der IT-Sicherheit oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert wurden, zu anderen Zwecken genutzt, so ist dies unzulässig.

Eine Gefahr, dass die Zweckbindung missachtet wird, besteht insbesondere bei automatisierten Abrufverfahren und sonstigen Übermittlungen sowie bei Verknüpfungen bzw. Auswertungen von Datenbeständen.

Eine Verarbeitung personenbezogene Daten unter Missachtung der Zweckbindung kann eine Geldbuße oder Freiheitsstrafe zur Folge haben bzw. zu dienst- oder arbeitsrechtlichen Konsequenzen führen. Der Betroffene kann ein Recht auf Schadensersatz geltend machen.

Beispiele:

- Die Zweckbindung wird verletzt, wenn eine Betriebsleitung Protokolldateien, in denen die An- und Abmeldung von Benutzern an IT-Systemen aus Gründen der IT-Sicherheit und des Datenschutzes festgehalten werden, zur Anwesenheits- und Verhaltenskontrolle nutzt.
- In einem Schreibbüro wird die Anzahl der Anschläge bei der Erstellung von Dokumenten für Zwecke der Kostenrechnung protokolliert. Zusätzlich soll dies unzulässigerweise dazu genutzt werden, die Anschlagsleistung der Mitarbeiter festzustellen.
- In der Kantine eines Unternehmens wird das Essen über eine kombinierte Mitarbeiter- und Kantinenkarte bezahlt. Die Kantinen-Abrechnungsdaten werden zur Erarbeitung individueller Gesundheitsvorsorgeprogramme genutzt, ohne dass die Mitarbeiter hierzu ihre Zustimmung gegeben haben.

G 6.3 Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten

Personenbezogene Daten dürfen nur verarbeitet werden, wenn dies zur Erfüllung der rechtmäßigen Aufgaben der dafür zuständigen datenverarbeitenden Stelle erforderlich ist.

Bei der Datenverarbeitung muss im Interesse des Betroffenen die sein Persönlichkeitsrecht am wenigsten beeinträchtigende Verarbeitung gewählt werden (Verhältnismäßigkeit).

Der Erforderlichkeitsgrundsatz ist immer dann verletzt, wenn Bearbeiter Zugriffsbefugnisse auf komplette Datenbestände erhalten, obwohl sie diese weit reichenden Zugriffsmöglichkeiten für ihre Aufgabenerfüllung nicht brauchen.

Ein sehr kritischer Punkt sind auch die weit reichenden Zugriffsrechte der Systemverwalter und Netzadministratoren. Gängige Betriebssysteme, insbesondere PC- und Netz-Betriebssysteme lassen noch immer allumfassende Zugriffsberechtigungen zu, die es erlauben, beliebige Dateien zu lesen, zu schreiben und insbesondere Protokolldateien, die eigentlich zur datenschutzrechtlichen Kontrolle und Revision der Datenverarbeitung gedacht sind, zu manipulieren oder sogar zu löschen. Somit können mögliche Spuren unerkannt beseitigt werden.

Auch eine fehlende Funktionstrennung zwischen Systemtechnik, Programmierung, Anwendung und Kontrolle und eine fehlende Abschottung von Programmen und Datenbeständen kann eine Überschreitung des Erforderlichkeitsgrundsatzes begünstigen.

Beispiele:

- Ein Versicherungssachbearbeiter ist ausschließlich zuständig für Versicherte mit den Anfangsbuchstaben A bis G, kann aber auf die Daten aller Versicherten zugreifen.
- Zugriffsrechte werden entsprechend der Hierarchie der datenverarbeitenden Stelle nach oben durchgereicht, so dass letztendlich der Leiter der Stelle Kraft seines Amtes alle Daten lesen und verändern kann.

G 6.4 Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten

Datenvermeidung und Datensparsamkeit sind Grundanforderungen, die bei der Bestimmung der zu erhebenden, verarbeitenden oder zu nutzenden Daten nach Art, Umfang und Dauer zu beachten sind. Sie sind gleichzeitig auch Vorgaben für die technische Gestaltung und ihre Auswahl. Eine Verletzung diese Grundsatzes kann unter Anderem eintreten durch:

- Erhebung von mehr Daten, als für den Verarbeitungszweck benötigt werden (z.B. mehr als zwei Kommunikationsadressen wie postalische Adresse, Telefonnummer und E-Mailadresse für Vertragszwecke).
- Verarbeitung von Daten in größerer Detaillierung als benötigt (z.B. Verarbeitung von Geburtsdatum oder Kreditkartennummer, wenn nur die Bestätigung eines Alters von mehr als 18 Jahren benötigt wird).
- Verarbeitung und Speicherung von personenbezogenen Daten über einen längeren Zeitraum als dies für den Verwendungszweck notwendig ist (z.B. Sicherheitsanalysen von Protokolldateien einer Firewall).

Von den Möglichkeiten der Anonymisierung und Pseudonymisierung ist wann immer möglich Gebrauch zu machen.

G 6.5 Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten

Das Datengeheimnis, d. h. der Schutz personenbezogener Daten, wird verletzt, wenn Personen, die Zugriff auf personenbezogene Daten haben, solche Daten unbefugt verarbeiten. Die Pflicht zur Wahrung des Datengeheimnisses gilt auch nach Beendigung der Tätigkeit. Ursache für solche Verletzungen sind oft eine Unkenntnis der Bearbeiter über die geltenden datenschutzrechtlichen Bestimmungen, die bei Aufnahme ihrer Tätigkeiten nicht entsprechend unterrichtet oder nicht auf den Datenschutz verpflichtet wurden.

Das Datengeheimnis kann verletzt werden durch das Nichtlöschen oder Verfälschen von gespeicherten personenbezogenen Daten, die Weitergabe von Adressdateien an Werbeunternehmen, die Weitergabe von personenbezogenen Daten innerhalb der Behörde oder des Unternehmens ohne dienstlichen Anlass, die unbefugte Einsichtnahme in Personaldaten, das Erstellen unzulässiger Auswertungen, die Nutzung dienstlicher Daten für private Zwecke (z. B. Weitergabe von Bonitätsdaten eines Nachbarn durch einen Mitarbeiter einer Bank im privaten Kreis).

Beispiele:

- Ein Mitarbeiter eines TK-Unternehmens benutzt seine dienstliche Berechtigung zur Abklärung der Bonität von Kunden dazu, Daten der Schufa oder anderer Wirtschaftsauskunfteien über einen missliebigen Nachbarn abzurufen und diese an Verwandte oder Bekannte weiterzugeben.
- Ein Mitarbeiter am Empfang eines Hotels gibt Anmeldedaten berühmter Gäste an die Presse, um sich damit ein Zubrot zu verdienen.
- Ein Administrator einer Stadtverwaltung hat bei seinen Arbeiten mit den Melderegister-Dateien zufällig die geheimgehaltene Anschrift einer alleinerziehenden Mutter gesehen und gibt diese an einen Bekannten im Sportverband weiter, dem das Sorgerecht wegen Bedrohung der Mutter und des Kindes entzogen und eine Kontaktaufnahme verboten worden war.

G 6.6 Fehlende oder nicht ausreichende Vorabkontrolle

Weist eine Verarbeitung personenbezogener Daten besondere Risiken für die Rechte und Freiheiten der Betroffenen auf wie z. B. die Verarbeitung besonderer Datenarten (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) oder soll damit die Persönlichkeit des Betroffenen einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens bewertet werden, ist vor dem Beginn der Verarbeitung eine Vorabkontrolle durchzuführen (§ 4d Abs. 5 BDSG). Dies gilt allerdings nicht, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. In manchen Landesdatenschutzgesetzen ist eine Vorabkontrolle generell bei allen Verfahren vorgeschrieben, mit denen personenbezogene Daten durch öffentliche Stellen verarbeitet werden. Die Voraussetzungen hierfür können von den beim Bund geltenden Regelungen abweichen.

Wird eine vorgeschriebene Vorabkontrolle nicht oder nur unzureichend durchgeführt, können sich Gefahren für das informationelle Selbstbestimmungsrecht ergeben.

Beispiele:

- Wenn Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet werden, von Unbefugten genutzt werden können, beispielsweise weil sie sich auf Grund unzureichender Sicherungsmaßnahmen Zutritt oder Zugang verschaffen können und dabei Kenntnis von Daten erhalten, kann dies besondere Risiken für die Rechte und Freiheiten der Betroffenen zur Folge haben.
- Die Vertraulichkeit und Integrität der Daten kann bei der Verarbeitung bzw. während einer Datenübermittlung verletzt werden, wenn diese nicht ausreichend geschützt werden (z. B. durch Verschlüsselung).
- Personenbezogene Daten, die im Auftrag verarbeitet werden, können durch den Auftragnehmer weit reichender als vertraglich geregelt zum Schaden der Betroffenen verarbeitet werden.
- Personenbezogene Daten können unter Umgehung der Zweckbindung verarbeitet und unzulässigerweise miteinander zum Nachteil der Betroffenen verknüpft werden.

G 6.7 Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten

Die Ausübung der aus dem Datenschutz herrührenden Rechte der Betroffenen (z. B. das Recht auf Auskunft, Berichtigung, Sperrung, Löschung) können diesen von der datenverarbeitenden Stelle aus technischen oder organisatorischen Gründen in unzulässiger Weise verwehrt werden. Die Betroffenen können ihre Rechte auch nicht ausüben, wenn Informationen unvollständig angegeben werden.

Beispiele:

- Ein Kunde wünscht Berichtigung der über ihn gespeicherten Daten. Die zuständige Stelle gibt vor, der Aufwand sei zu groß oder die technischen Möglichkeiten fehlten.
- Die Stelle erteilt eine unvollständige oder nicht aktuelle Auskunft über die gespeicherten Daten des Betroffenen.

G 6.8 Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten

Die Vergabe von Tätigkeiten der Datenverarbeitung nach Außen im Wege einer Auftragsdatenverarbeitung ist unter der Voraussetzung zulässig, dass der Auftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich ist. Die Vergabe des Auftrags hat unter besonderer Berücksichtigung der technischen und organisatorischen Eignung des Auftragnehmers zu erfolgen. Der Auftrag hat schriftlich zu erfolgen, wobei die Datenverarbeitung selber sowie die zugehörigen technischen und organisatorischen Maßnahmen zu beschreiben sind. Zu diesen Maßnahmen gehört insbesondere auch die Gewährleistung der Auftragskontrolle. Der Auftragnehmer bleibt bezogen auf die Datenverarbeitung weisungsgebunden.

Diese Bestimmungen gelten auch für die Prüfung und Wartung von technischen Anlagen, die der automatisierten Verarbeitung personenbezogener Daten dienen (Fernwartung).

Beispiele:

- Ein Unternehmen möchte die technische Abwicklung der Lohnbuchhaltung im Rahmen eines Application-Services an einen Dienstleister auslagern. Die Datenverarbeitung findet so statt, dass Mitarbeiter des Dienstleisters im Zuge der Administration und Datensicherung auch Zugriff auf die Lohndaten nehmen können. Die vertraglichen Vereinbarungen regeln lediglich die Verfügbarkeit und das Wiederanlaufen des Dienstes der Lohnbuchhaltung. Aus ungeklärter Ursache kommen Lohndaten von Mitarbeitern des Auftraggebers in die Öffentlichkeit. Sie werden zur Anprangerung der Einkommen der Mitarbeiter benutzt. Konkurrierende Unternehmen versuchen Mitarbeiter mit besseren Angeboten abzuwerben und den Konkurrenten damit zu schädigen. Betroffene Mitarbeiter beschweren sich bei der zuständigen Aufsichtsbehörde.
- Im Zuge der Überprüfung der Datenverarbeitung des Auftraggebers stellt die Aufsichtsbehörde fehlende Regelungen der Auftragsdatenverarbeitung fest, da wesentliche vertragliche Vereinbarungen zur Sicherstellung der datenschutzrechtlichen Bestimmungen (hier insbesondere bezogen auf die Umsetzung der Sicherheitsziele des Datenschutzrechtes, Überprüfung der Umsetzung beim Dienstleister und Vereinbarungen für den Fall der mangelhaften Umsetzung) fehlen. Die Aufsichtsbehörde muss dies beanstanden und fordert dazu auf, die Mängel kurzfristig abzustellen.

G 6.9 Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen

Werden personenbezogene Daten erhoben, ohne dass der Betroffene über die vorgesehene Verarbeitung und die Rechtsgrundlage unterrichtet wird, ist die Transparenz in Frage gestellt.

Sie ist auch in Frage gestellt, wenn ihm Angaben über die Herkunft und den Empfänger dieser Daten sowie Löschungsfristen vorenthalten werden.

Werden die Datenschutz-Kontrollinstanzen nicht rechtzeitig vor

- der Einführung neuer Verfahren,

- der Freigabe von Verfahren,

- dem Erlass von Verwaltungsvorschriften,

- der Einrichtung von automatisierten Abrufverfahren oder

- einer Vergabe von Datenverarbeitung im Auftrag

informiert, werden sie daran gehindert, Vorschläge zur Verbesserung des Datenschutzes so rechtzeitig zu unterbreiten, dass noch eine Berücksichtigung bei der Verfahrensentwicklung möglich ist. Die Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen verbleibt auch bei Einbeziehung der Datenschutz-Kontrollinstanzen bei der datenverarbeitenden Stelle.

Durch fehlende oder mangelhafte Protokollierung und Dokumentation bei der Verarbeitung personenbezogener Daten und durch fehlende Aktualisierung bei Verfahrensänderungen wird die Arbeit der Kontrollinstanzen beeinträchtigt. Eine effektive Kontrolle kann auch durch unvollständige oder nicht aktualisierte Verzeichnisse der eingesetzten IT-Systeme, mangelhafte Konfigurationsübersichten und fehlende Verkabelungspläne gefährdet sein.

Fehlende oder unvollständige Meldungen zu den internen Verzeichnissen und, soweit gesetzlich vorgeschrieben, zu den öffentlichen Verzeichnissen gefährden die Transparenz der Datenverarbeitung für den Betroffenen und die Kontrollinstanzen.

Beispiele:

- Einem Betroffenen ist durch eine unzulässige automatisierte Datenverarbeitung einer öffentlichen Stelle Schaden entstanden. Ein Versuch, durch Einsicht in das Verfahrensverzeichnis (soweit ein solches vorhanden ist) beim zuständigen Landesbeauftragten für den Datenschutz nähere Informationen zu erhalten, kann daran scheitern, dass dort keine Meldungen vorliegen oder dass in der Meldung, obwohl vorgeschrieben, die Partner durchgeführter Übermittlungen nicht genannt sind.
- Wegen fehlender Verfahrensbeschreibungen weiß niemand in einer öffentlichen Stelle, welche Dateien von welchen Ämtern über welchen Bediensteten geführt werden.

G 6.10 Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten

Durch unzureichende technische und organisatorische Maßnahmen bei der Verarbeitung personenbezogener Daten besteht vor allem die Gefahr, dass

- Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten können,
- Datenverarbeitungssysteme durch Unbefugte benutzt werden können,
- Berechtigte auf Daten außerhalb ihrer Zugriffsberechtigungen zugreifen können,
- personenbezogene Daten unbefugt gelesen, kopiert, verändert oder entfernt werden können,
- personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können,
- nicht überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist,
- nicht nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind,
- personenbezogene Daten, die im Auftrag verarbeitet werden, entgegen den Weisungen des Auftraggebers verarbeitet werden können,
- personenbezogene Daten nicht gegen zufällige Zerstörung oder Verlust geschützt sind,
- das nicht gewährleistet ist, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können und insgesamt

Beispiele:

- Beispielsweise glauben viele IT-Betreuer, dass es bei einzelstehenden PCs, die auch nur durch eine Person mit einer Anwendung genutzt werden, ausreichen würde, den PC durch ein individuelles BIOS-Passwort zu schützen. Dabei wird übersehen, dass der BIOS-Passwortschutz in vielen Fällen mit einfachen Mitteln und in kurzer Zeit zu umgehen ist, so dass personenbezogene Daten unbemerkt zur Kenntnis genommen oder gar verfälscht werden können. Dazu gehört auch, dass PCs, insbesondere tragbare Geräte, sehr leicht gestohlen werden können und dann die Daten, wenn sie nicht verschlüsselt sind, mit Programmen des Betriebssystems von jedem Kundigen ausgelesen und missbräuchlich verwendet werden können.
- Ein bei Kontrollen immer wieder aufgedecktes Problem besteht darin, dass bei IT-Systemen zwar der Zugriff auf die Programme und Datenbestände durch eine Benutzeridentifikation (Benutzerkennung und Passwort) und eine gezielte Benutzerführung (Menüsystem, benutzerspezifische Oberfläche) abgesichert ist, aber es z. B., obwohl gesetzlich vorgeschrieben, nachträglich nicht mehr feststellbar ist, welche Daten in

Datenverarbeitungssysteme eingegeben wurden, da man es bei der Konzipierung der Systeme versäumt hat, auch eine ausreichende Protokollierung zu integrieren.

- Ausgelöst durch Diskussionen um eine Reduzierung der Personalkosten und der Kosten der Datenverarbeitung glauben viele Anwender, die vorhandenen Probleme durch eine Verlagerung der Datenverarbeitung außer Haus zu lösen und damit die Verpflichtung zum Datenschutz auf den Auftragnehmer verlagern zu können. Dabei werden oft die in den Datenschutzgesetzen enthaltenen Bestimmungen im Rahmen der Datenverarbeitung im Auftrag übersehen, die eine klare vertragliche Regelung verlangen und die Verantwortung einschließlich einer Kontrolle der technischen und organisatorischen Maßnahmen weiterhin beim Auftraggeber belassen.

G 6.11 Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland

Bei der Übermittlung personenbezogener Daten ins Ausland sind besondere gesetzliche Bestimmungen zu beachten. Personenbezogene Daten dürfen in die Mitgliedstaaten der Europäischen Union unter den gleichen Voraussetzungen übermittelt werden wie innerhalb der Bundesrepublik Deutschland. An Stellen in so genannte Drittländer dürfen personenbezogene Daten nur übermittelt werden, wenn dort ein angemessenes Datenschutzniveau (vergleiche § 4b Abs. 3 BDSG) gewährleistet ist, die im Gesetz genannten Ausnahmen vorliegen (§ 4c Abs. 1 BDSG) oder die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist (§ 4 c Abs. 2 BDSG). Im letzteren Fall bedürfen die Übermittlungen einer Genehmigung durch die Aufsichtsbehörden.

Beispiel:

- Ein deutsches Unternehmen, das zu einem international agierenden Konzern gehört, möchte seine bisherige nationale Zugangs- und Zugriffsverwaltung auf einen Verzeichnisdienst (Directory Service) umstellen, der in Japan durch eine andere Konzerntochter zentral betrieben werden soll.
- Japan hat (noch) kein angemessenes Datenschutzniveau. Die Weitergabe von personenbezogenen Daten an einen japanischen Auftraggeber ist daher nur zulässig, wenn durch geeignete Maßnahmen ein angemessenes Datenschutzniveau gewährleistet wird. Dies kann durch Unterzeichnung der so genannten Standardvertragklauseln zwischen dem deutschen Auftraggeber und dem japanischen Auftragnehmer erfolgen.

G 6.12 Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten

Niemand darf einer automatisierten Entscheidung unterworfen werden, die für ihn eine negative rechtliche Folge nach sich zieht oder ihn erheblich beeinträchtigt. Voraussetzung dieses Verbotes ist, dass sich die Entscheidung ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten stützt, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Das Verbot gilt nicht, wenn dem Begehren des Betroffenen stattgegeben wurde. Eine Ausnahme gilt auch, wenn der Betroffene über die automatisierte Einzelfallentscheidung unterrichtet wurde und seine schutzwürdigen Interessen durch geeignete Maßnahmen gewährleistet werden. Hierzu zählt die Möglichkeit, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist dann verpflichtet, ihre Entscheidung erneut zu überprüfen.

Der Betroffene ist in jedem Fall über die Verarbeitung seiner Daten, die der automatisierten Einzelfallentscheidung zugrunde gelegt werden, den Verwendungszweck und die Kategorien der Empfänger zu unterrichten. Um seinen Standpunkt geltend machen zu können, muss er zudem über die Folgen der Verarbeitung und über die Funktionsweise des konkreten Verfahrens (logischer Aufbau) informiert werden.

Beispiele:

- Eine Stelle prognostiziert mit Hilfe eines Scoringsystems die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit oder das zukünftige Verhalten einer Person. Unabhängig vom Ergebnis des Verfahrens hat die verantwortliche Stelle gegenüber dem Betroffenen Informationspflichten. Werden diese vernachlässigt, wird gegen geltende Gesetze verstoßen.
- Wird mit Hilfe des Scoringsystems eine für den Betroffenen nachteilige Entscheidung gefällt, so muss die Daten verarbeitende Stelle durch geeignete Maßnahmen dafür Sorge tragen, dass die berechtigten Interessen der Betroffenen gewahrt bleiben. Hierzu bedarf es nicht nur der Transparenz gegenüber dem Betroffenen, sondern insbesondere auch der Möglichkeit, seinen Standpunkt gegenüber der Stelle geltend zu machen, so dass die Entscheidung einer erneuten Überprüfung unterzogen wird. Werden die Interessen des Betroffenen verletzt oder eine erneute Überprüfung unterlassen, kann sich der Betroffene an die zuständige Datenschutzaufsicht wenden.

G 6.13 Fehlende oder unzureichende Datenschutzkontrolle

Die Kontrolle der Einhaltung der geltenden Datenschutz-Bestimmungen, vor allem die Kontrolle der technischen und organisatorischen Maßnahmen wird oft unzureichend bleiben, wenn in ihr zu Unrecht nur ein unproduktiver Kostenfaktor gesehen wird. Die datenschutzrechtliche Kontrolle kann auch dadurch sehr erschwert werden, wenn versäumt wird, ihre Anforderungen schon bei der Entwicklung und Erprobung von Verfahren einzubeziehen.

Eine effektive Arbeit für eine Datenschutzkontrolle ist in aller Regel nicht gesichert, wenn in einem Unternehmen oder einer Behörde kein Datenschutzbeauftragter bestellt ist oder wenn der vorhandene Datenschutzbeauftragte nicht ausreichend qualifiziert oder geschult ist, oder wenn er nicht ausreichend unterstützt und nicht rechtzeitig informiert wird (unzureichende Personal- und Sachmittel).

Beispiele:

- Der Leiter des Rechenzentrums wird zum internen Datenschutzbeauftragten bestellt, da dieser für das Amt die besten Fachkenntnisse mitbringt. Dabei wird die entstehende Interessenkollision übersehen. Dazu gehört beispielsweise, dass er Sicherheitsvorgaben, die er für den Betrieb von IT-Verfahren gemacht hat oder Protokolldaten, die zur Missbraucherkennung gespeichert wurden, als Datenschutzbeauftragter kontrollieren müsste.
- Es wird eine interne Datenschutzrichtlinie erlassen, nach der jährlich ein Bericht des Datenschutzbeauftragten vorzulegen ist. Der bestellte Datenschutzbeauftragte ist aber schon seit 2 Jahren dauerhaft krank und ein Vertreter wurde nicht ernannt, so dass kein Bericht erstellt wird.

M 2.110 Datenschutzaspekte bei der Protokollierung

Verantwortlich für Initiierung: Leiter IT, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Administrator, Datenschutzbeauftragter

Unter Protokollierung beim Betrieb von IT-Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: "Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: "Wer hatte von wann bis wann welche Zugriffsrechte?"

Art und Umfang von Protokollierungen hängen vom allgemeinen Datenschutzrecht und auch von bereichsspezifischen Regelungen ab.

Die Protokollierung der Administrationsaktivitäten entspricht einer Systemüberwachung, während die Protokollierung der Benutzeraktivitäten im wesentlichen der Verfahrensüberwachung dient. Dementsprechend finden sich die Anforderungen an die Art und den Umfang der systemorientierten Protokollierung überwiegend im allgemeinen Datenschutzrecht, während die verfahrensorientierte Protokollierung oft durch bereichsspezifische Regelungen definiert wird. Beispiele für verfahrensorientierte Protokollierung sind u. a. Meldegesetze, Polizeigesetze, Verfassungsschutzgesetze.

Mindestanforderungen an die Protokollierung

Bei der Administration von IT-Systemen sind die folgenden Aktivitäten vollständig zu protokollieren:

- **Systemgenerierung und Modifikation von Systemparametern**

  Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.

- **Einrichten von Benutzern**

  Wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen, ist vollständig zu protokollieren. Für diese Protokolle sollten längerfristige Aufbewahrungszeiträume vorgesehen werden, da sie Grundlage praktisch jeder Revisionsmaßnahme sind.

- **Erstellung von Rechteprofilen**

  Im Rahmen der Protokollierung der Benutzerverwaltung kommt es insbesondere auch darauf an aufzuzeichnen, wer die Anweisung zur Einrichtung bestimmter Benutzerrechte erteilt hat (siehe auch M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile).

- **Einspielen und Änderung von Anwendungssoftware**

  Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.

- **Änderungen an der Dateiorganisation**

  Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der "Standard-Dateiverwaltungssysteme" ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu (siehe z. B. Datenbankmanagement).

- **Durchführung von Datensicherungsmaßnahmen**

  Da derartige Maßnahmen (Backup, Restore) mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in "Ausnahmesituationen" durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.

- **Sonstiger Aufruf von Administrations-Tools**

  Die Benutzung aller Administrations-Tools ist zu protokollieren, um feststellen zu können, ob Unbefugte sich Systemadministrator-Rechte erschlichen haben.

- **Versuche unbefugten Einloggens und Überschreitung von Befugnissen**

  Geht man von einer wirksamen Authentisierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller "auffälligen Abnormalitäten" beim Einloggen und der Benutzung von Hard- und Software-Komponenten eine zentrale Bedeutung zu. Benutzer in diesem Sinne ist auch der Systemadministrator.

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

- **Eingabe von Daten**

  Die so genannte Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, dass Befugnisüberschreitungen anderweitig protokolliert werden, dürfte eine vollständige Protokollierung von Dateneingaben als Regelfall angesehen werden müssen.

- **Datenübermittlungen**

  Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, kann eine selektive Protokollierung als ausreichend angesehen werden.

- **Benutzung von automatisierten Abrufverfahren**

  In der Regel dürfte eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich sein, um unbefugte Kenntnisnahme im Rahmen der grundsätzlich eingeräumten Zugriffsrechte aufdecken zu können.

- **Löschung von Daten**

  Die Durchführung der Löschung ist zu protokollieren.

- **Aufruf von Programmen**

  Dies kann erforderlich sein bei besonders "sensiblen" Programmen, die z. B. nur zu bestimmten Zeiten oder Anlässen benutzt werden dürfen. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

Zweckbindung bei der Nutzung von Protokolldaten

Protokolldaten unterliegen aufgrund der nahezu übereinstimmenden Regelungen im Datenschutzrecht des Bundes und der Länder einer besonderen engen Zweckbindung (z. B. § 14 Abs. 4 und § 31 BDSG, § 13 Abs. 5 HDSG). Sie dürfen nur zu den Zwecken genutzt werden, die Anlass für ihre Speicherung waren. Dies sind in der Regel die in einem Sicherheitskonzept festgelegten allgemeinen Kontrollen, die in den meisten Datenschutzgesetzen geforderte "Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden " (siehe z. B. § 18 Abs. 2 BDSG, § 8 Abs. 3 LDSG-SH) und die Kontrollen durch interne oder externe Datenschutzbeauftragte. Nur in Ausnahmefällen lassen die bereichsspezifischen Regelungen die Nutzung dieser Daten für andere Zwecke, z. B. zur Strafverfolgung, zu.

Aufbewahrungsdauer

Soweit nicht bereichsspezifische Regelungen etwas anderes vorsehen, richtet sich die Aufbewahrungsdauer der Protokolle nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Maßstab ist die "Erforderlichkeit zur Aufgabenerfüllung". Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht (siehe z. B. § 20 Abs. 2 BDSG).

Als Anhaltspunkte können dienen:

- die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) offenbar werden können und
- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden.

Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, kommen kürzere Speicherungsfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle aus. Auch hier sind die bereichsspezifischen Vorschriften zu beachten.

Technische und organisatorische Rahmenbedingungen

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

- Es sollte ein Revisionskonzept erstellt werden, das den Zweck der Protokolle und deren Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert.
- Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muss ebenso gewährleistet werden wie die Manipulationssicherheit der Einträge in Protokolldateien.
- Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden.
- Die Protokolle müssen so gestaltet sein, dass eine effektive Überprüfung möglich ist. Dazu gehört auch eine IT-Unterstützung der Auswertung.
- Die Auswertungsmöglichkeiten sollten vorab abgestimmt und festgelegt sein.
- Kontrollen sollten so zeitnah durchgeführt werden, dass bei aufgedeckten Verstößen noch Schäden abgewendet sowie Konsequenzen gezogen werden können. Kontrollen müssen rechtzeitig vor dem Ablauf von Löschungsfristen von Protokolldateien stattfinden.
- Kontrollen sollten nach dem 4-Augen-Prinzip erfolgen.
- Es sollte vorab definiert werden, welche Konsequenzen sich aus Verstößen ergeben, die durch die Kontrolle von Protokollen aufgedeckt werden.
- Die Mitarbeiter sollten darüber informiert sein, dass Kontrollen durchgeführt werden, ggf. auch unangekündigt.
- Für Routinekontrollen sollten automatisierte Verfahren (z. B. watch dogs) verwendet werden.
- Personal- bzw. Betriebsräte sollten bei der Erarbeitung des Revisionskonzeptes und bei der Festlegung der Auswertungsmöglichkeiten der Protokolle beteiligt werden.

M 7.1 Datenschutzmanagement

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Datenschutzbeauftragter

Mit Datenschutzmanagement werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen. Datenschutzmanagement ist die übergeordnete Umsetzung des Datenschutzes in einer Organisation oder bei Großverfahren. Nachfolgend wird ein Musterprozess für das Datenschutzmanagement beschrieben, der als Beispielprozess und Vorschlag zu sehen ist. Der Prozess orientiert sich an den BSI-Standards 100-1 und 100-2 und ist als integrativer Bestandteil des IT-Sicherheitsprozesses nach IT-Grundschutz anzusehen, kann aber auch als eigenständiger Prozess behandelt werden, wenn vorrangig der Datenschutzaspekt behandelt werden soll. Sinnvollerweise wird dieser Prozess nicht für einzelne Verfahren eingerichtet und betrieben, sondern für die gesamte Organisation und alle Verfahren, in denen personenbezogene Daten verarbeitet werden.

Der Datenschutzprozess

Herzstück des Datenschutzmanagements ist der Datenschutzprozess. Er ist wie der IT-Sicherheitsprozess als zyklischer Prozess ausgelegt, um bei geändertem Umfeld die Einhaltung geltenden Datenschutzrechtes kontinuierlich sicherstellen zu können. Er deckt die Aufgaben in einer Organisation ab, die sich auf strategischer, taktischer oder operativer Ebene ergeben. Der Prozess bedient sich dabei einzelner Maßnahmen, die im Folgenden beschrieben sind. Er ist so ausgelegt, dass er die Errichtung eines Datenschutzmanagements auch in Organisationen ermöglicht, die noch über keine Strukturen zur Umsetzung des Datenschutzes verfügen. Die folgende Abbildung stellt den Prozess dar:

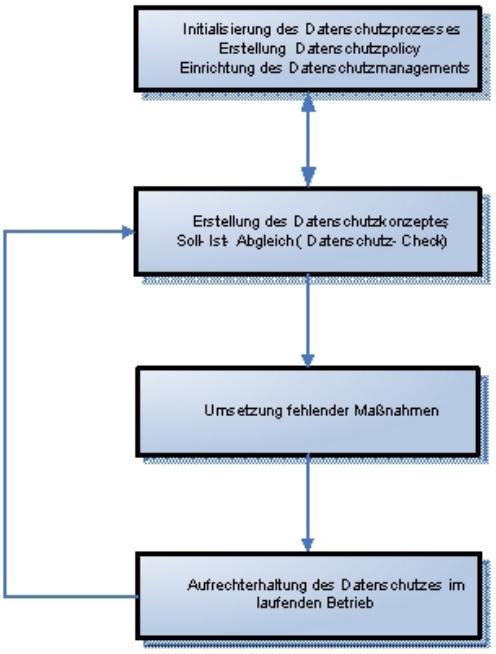

Abbildung 1: Datenschutzprozess

Im Folgenden werden die nun die einzelnen Prozessschritte bzw. Teilprozesse erläutert.

Initialisierung des Datenschutzprozesses

In diesem Prozessschritt sind die Maßnahmen angesiedelt, die eine strategische Zielstellung (Geltungsdauer bis zu fünf Jahren) haben. Sie beinhalten:

Erarbeitung einer Datenschutz-Richtlinie, in der Regel im Rahmen einer behörden- oder unternehmensweiten Sicherheitsrichtlinie: Diese kann als Zielstellungen unter anderem formulieren:

- Regelkonformität ("Compliance") mit minimalen Aufwand oder
- Datenschutz als Wettbewerbsvorteil ("USP": Unique Selling Proposition)

Einrichtung eines Datenschutzmanagements, in der Regel innerhalb des IT-Sicherheitsmanagements. Wichtige Teilaspekte sind die Regelung der Zuständigkeiten (Rolle und Funktion des Datenschutzbeauftragten in Abgrenzung zu und Zusammenarbeit mit den Datensicherheitsbeauftragten), Prozessdefinitionen und Bereitstellung von Ressourcen (Personalkapazitäten).

Erstellung eines Datenschutzkonzepts

Das Datenschutzkonzept ist das Pendant zum IT-Sicherheitskonzept (Geltungsdauer ein bis drei Jahre). Für den Inhalt wird auf Maßnahme M 7.3 *Aspekte eines Datenschutzkonzeptes* verwiesen.

Umsetzung der erforderlichen Maßnahmen

Dieser Prozessschritt beinhaltet die Umsetzung der im Datenschutzkonzept festgelegten, bislang noch nicht umgesetzten Maßnahmen. Die Umsetzung erfolgt im Rahmen eines klassischen Projektmanagements mit einem Projekt- und Arbeitsplan.

Aufrechterhaltung des Datenschutzes im laufenden Betrieb

Die Aufgabe dieses Teilprozesses ist es, auf Änderungen und Störungen im laufenden Betrieb der Verfahren zu reagieren, in denen personenbezogener Daten verarbeitet werden. Dies sind vor allem:

- Änderungen im Datenschutzrecht
- Änderungen in den (IT-)Verfahren
- Störungen in den operativen Betriebsabläufen, die als IT-Sicherheitsvorfall zu klassifizieren sind
- Technischer Fortschritt und reduzierter Aufwand für bisher nicht realisierte Maßnahmen.

Zu diesem Zweck wird begleitend zum IT-Sicherheitsprozess eine Reihe von Sub-Prozessen benötigt, die Änderungen und Störungen aus Datenschutzsicht eigenständig bearbeiten bzw. lösen. Die Ergebnisse können gegebenenfalls auch Strukturänderung im Datenschutzmanagement oder Aktualisierungen des Datenschutzkonzeptes (Aktualisierung) zur Folge haben.

Die folgende Abbildung stellt die Sub-Prozesse in einer Übersicht dar:

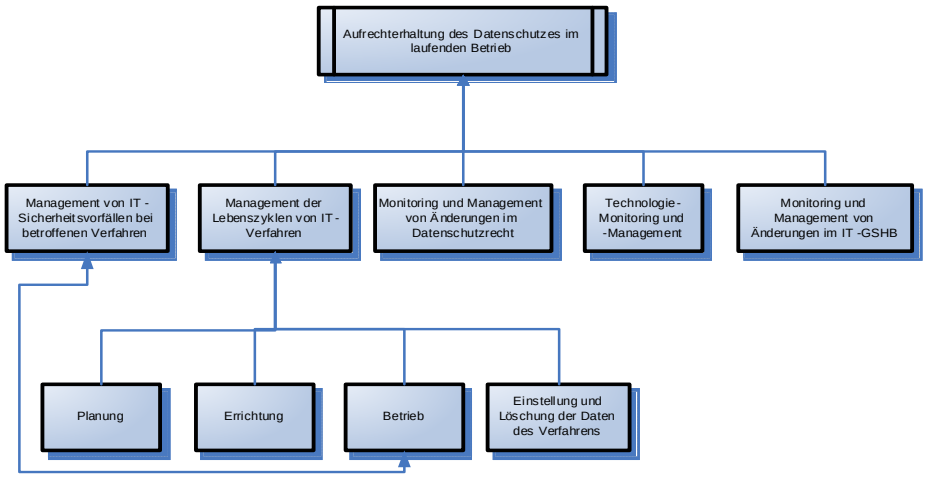

Abbildung 2: Teilprozesse der Aufrechterhaltung des Datenschutzes im laufenden Betrieb

Management von IT-Sicherheitsvorfällen

Das Management von IT-Sicherheitsvorfällen bei IT-Verfahren im laufenden Betrieb muss auch gegebenenfalls die Vorfälle und ihre Folgen unter dem Gesichtspunkt des geltenden Datenschutzrechtes behandeln. Dies geschieht zweckmäßigerweise in Zusammenarbeit mit dem IT-Sicherheitsbeauftragten, der das IT-Sicherheitsvorfall-Team leitet. Aufgaben des begleitenden Datenschutzmanagements können hier sein:

- Priorisierung von technischen und organisatorischen Maßnahmen zur Problemanalyse und Problemlösung bzw. Beweissicherung unter Datenschutzgesichtspunkten
- Behandlung juristischer Aspekte unter dem Gesichtspunkt des Datenschutzrechtes.

Unter dem Gesichtspunkt der Prozessintegration ist es sinnvoll, dass der IT-Sicherheitsprozess das entsprechende Datenschutzmanagement auslöst bzw. den entsprechenden Sub-Prozess aufruft. In der Praxis kann dies beispielsweise bedeuten, dass bei IT-Sicherheitsvorfällen, die Verfahren betreffen, in denen personenbezogene Daten verarbeitet werden, der Datenschutzbeauftragte automatisch Mitglied des IT-Sicherheitsvorfall-Teams wird. Er kann so in die Informationen und Prozessabläufe optimal eingebunden werden. Unter diesem Management ist auch eine Beschreibung zu verstehen, wo bzw. von wem im Unternehmen oder der Behörde Datenschutzvorfälle gemanagt werden.

Management der Lebenszyklen von IT-Verfahren unter Datenschutzgesichtspunkten

Beim Management der Lebenszyklen von IT-Produkten und -Verfahren kommt ein Lebenszyklusmodell zur Anwendung, das sich am allgemeinen Lebenszyklusmodell der BSI-Standards und der IT-Grundschutz-Kataloge orientiert.

Innerhalb der jeweiligen Phasen ist eine Reihe von Maßnahmen aus dem Baustein B 1.5 *Datenschutz* zu berücksichtigen. Dies umfasst:

- In der Planung und Konzeption die Maßnahmen: M 7.1 bis M 7.5
- Bei der Umsetzung der Planung und Konzeption bis hin zum laufenden Betrieb die Maßnahmen: M 7.6 bis M 7.12
- Im laufenden Betrieb die Maßnahmen: M 7.13 bis M 7.15
- Nach Einstellung bis zur endgültigen Löschung des Verfahrens und aller zugehörigen Daten die Maßnahmen: M 7.8, M 2.110 und M 7.15

Darüber hinaus sollte bei der Planung und Konzeption von neuen IT-Verfahren geprüft werden, ob Privacy Enhancing Technologies (PETs) eingesetzt werden können. PETs unterstützen technisch die Umsetzung von Datenschutzgrundsätzen wie Datensparsamkeit, Zweckbindung oder das Transparenzgebot. Beispiele für PETs sind Protokolle wie P3P (Platform for Privacy Preferences) und Verfahren zur Anonymisierung und Pseudonymisierung von Daten beim Netzwerktransfer, der Datenhaltung in Datenbanken oder dem

Data-Mining (Privacy Preserving Data Mining, PPDM). Aber auch Wiedervorlagefunktionen in Programmen, die die Einhaltung von Löschfristen bei der Speicherung von personenbezogenen Daten unterstützen, zählen dazu.

Management von Änderungen im Datenschutzrecht

Änderungen im Datenschutzrecht sind zu verfolgen und hinsichtlich ihrer Auswirkungen auf die Verfahren, in denen personenbezogene Daten verarbeitet werden, zu beurteilen. Dieser Sub-Prozess lässt sich auch in das behörder- oder unternehmensweite Monitoring von Änderungen in relevanter Gesetzgebung integrieren.

Technologie-Monitoring

Das Technologie-Monitoring verfolgt gemeinsam mit dem IT-Sicherheits-Management den "Stand der Technik" bezogen auf IT-Sicherheit und Datenschutz. Unter Maßgabe der einschlägigen Datenschutzgesetzgebung und deren Anwendung gibt dieser Sub-Prozess Impulse für die Weiterentwicklung von Datenschutz- und IT-Sicherheitskonzept.

Monitoring und Management von Änderungen in den IT-Grundschutz-Katalogen

Beim allgemeinen Monitoring sind auch Aktualisierungen der BSI-Standards und der IT-Grundschutz-Kataloge, insbesondere des Datenschutzbausteins zu berücksichtigen. Neben Impulsen für die Weiterentwicklung von Datenschutz- und IT-Sicherheitskonzept sind auch die Schnittstellen zu IT-Sicherheitsmanagement zu überprüfen und gegebenenfalls anzupassen.

Zusammenfassung

Das vorgeschlagene Prozessmodell bietet vielfältige Anknüpfungspunkte und dadurch Synergien zu den entsprechenden IT-Sicherheitsprozessen der BSI-Standards Diese Synergien können von einer Kooperation der Prozesse, der Integration von Dokumenten (z. B. Datenschutz- und IT-Sicherheitskonzept) und Dokumentation bis hin zur vollständigen Integration der Prozesse reichen. Dies kann sich auch auf Funktionsträger erstrecken: ein IT-Sicherheitsbeauftragter kann die Rolle des Datenschutzbeauftragten in Personalunion wahrnehmen, wenn er die geeignete Sachkunde mitbringt und im Bereich der IT nicht gleichzeitig konzeptionelle und operative Aufgaben wahrnimmt (Vermeidung einer Interessenkollision). Dies ist insbesondere in kleinen Organisationen von Bedeutung.

Die folgende Abbildung 3 stellt dies schematisch dar.

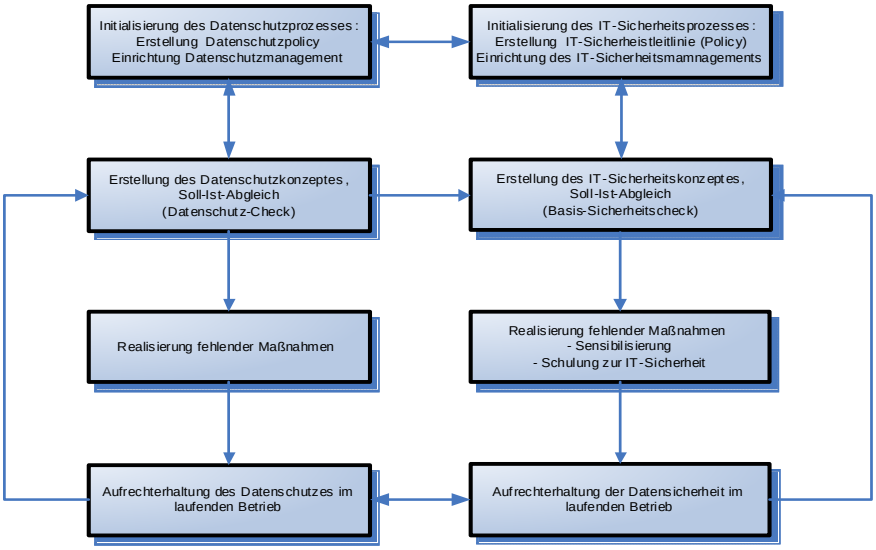

Abbildung 3: Schematische Darstellung von Wechselwirkungen und Synergien zwischen Datenschutz- und Datensicherheitsprozess

Ergänzende Kontrollfragen:

- Wie lassen sich personenbezogene Daten nach dem Stand der Technik sichern?
- Wo und wie lassen sich Privacy Enhancing Technologies (PETs) sinnvoll bei den eigenen IT-Verfahren einsetzen?

M 7.2 Regelung der Verantwortlichkeiten im Bereich Datenschutz

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung

Datenschutz ist für alle IT-Systeme und -Verfahren, mit deren Hilfe personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Die Aspekte des Datenschutzes sind daher von Beginn der Planungen zur Einführung eines IT-Verfahrens im Rahmen des IT-Sicherheitsmanagements zu integrieren. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtlich anfallende Aufgaben effizient und effektiv erledigt werden.

Eine detaillierte Auflistung zu bearbeitender Aufgaben und zu treffender Regelungen, die unter datenschutzrechtlichen Aspekten zu betrachten sind, sind zu finden in M 2.1 *Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz*.

Die Bestellung eines betrieblichen bzw. behördlichen Datenschutzbeauftragten (bDSB) und seine Integration in das IT-Sicherheitsmanagement ist eine Maßnahme, die sich dazu in besonderem Maße eignet. Es besteht auch die Möglichkeit, einen externen bDSB zu bestellen.

Der bDSB kontrolliert eigenständig die Einhaltung des Datenschutzes, bildet aber auch gewissermaßen das Bindeglied zwischen der eigenverantwortlichen Gesetzesanwendung durch die datenverarbeitende Stelle auf der einen und der staatlichen Kontrolle auf der anderen Seite.

Die Bestellung ist, von wenigen Ausnahmen abgesehen, gesetzlich vorgeschrieben:

- Für öffentliche Stellen des Bundes und nicht-öffentliche Stellen im BDSG (§§ 4 f, g) und für die Sozialversicherungsträger im Sozialgesetzbuch (§ 35 SGB I, § 81 Abs. 1 SGB X i. V. m. §§ 4 f, g BDSG).
- Für öffentliche Stellen der Länder ist die Pflicht zur Bestellung in einigen Landesdatenschutzgesetzen ebenfalls vorgeschrieben.

Auch in den Bereichen, in denen eine Bestellung eines Datenschutzbeauftragten nicht erfolgt, muss die Einhaltung der datenschutzrechtlichen Anforderungen sichergestellt sein. Dies kann auch durch das IT-Sicherheitsmanagement erfolgen. Hierzu sollte zumindest eine interne IT-Revision und Datenschutzkontrolle eingerichtet werden (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Bestellung eines Datenschutzbeauftragten

Zum Datenschutzbeauftragten kann nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

Zur Aufgabenerfüllung gehören technische, organisatorische und rechtliche Kenntnisse. Der bDSB muss die gesetzlichen Regelungen, wie z. B. das Recht auf informationelle Selbstbestimmung, die Grundrechte mit Datenschutzbezug, das Bundesdatenschutzgesetz, bereichsspezifische datenschutzrechtliche Regelungen und die einschlägigen Spezialvorschriften des Fachbereichs,

kennen und sicher anwenden können. Er sollte ferner gute Kenntnisse der Organisation und vertiefte Kenntnisse der Informationstechnik besitzen.

Soweit ihm die fachliche Qualifikation in Teilbereichen noch fehlt, ist ihm Gelegenheit zu geben, diese zu erwerben. Mit den Aufgaben und der Arbeitsweise seiner Behörde bzw. seines Unternehmens sollte der bDSB möglichst aus eigener Erfahrung gut vertraut sein, um seinen Kontroll- und Beratungsaufgaben nachkommen zu können.

Der bDSB muss nicht ausschließlich mit den Funktionen eines Datenschutzbeauftragten betraut sein. Je nach Art und Umfang der personenbezogenen Datenverarbeitung und der damit verbundenen Datenschutzprobleme kann es angebracht sein, ihm daneben weitere Aufgaben zu übertragen. Dies wird besonders bei kleineren Behörden bzw. Unternehmen in Betracht kommen, wenn die Einarbeitungszeit oder die Aufbauperiode abgeschlossen ist.

Besonders ist darauf zu achten, dass keine Interessenkonflikte oder Abhängigkeiten entstehen, die seine Aufgabenerfüllung gefährden. Interessenkonflikte können insbesondere dann auftreten, wenn der bDSB gleichzeitig Aufgaben in den Bereichen Personal, Informationstechnik oder in Organisationseinheiten mit besonders umfangreicher oder sensitiver Verarbeitung von personenbezogenen Daten wahrnimmt oder Geheimschutzbeauftragter ist. Möglich ist dagegen die Zusammenlegung der Funktionen des bDSB mit denen des IT-Sicherheitsbeauftragten. Ist der IT-Sicherheitsbeauftragte organisatorisch unabhängig von der für die IT verantwortlichen Organisationseinheit eingerichtet, ist die Zusammenfassung in einer Hand empfehlenswert. Auch der Leiter oder ein Mitarbeiter der Bereiche Justitiariat/Recht oder Organisation bietet sich für die Aufgabe an.

Im Interesse einer späteren vertrauensvollen Zusammenarbeit sollte der Personal- bzw. Betriebsrat im Verfahren der Bestellung des bDSB frühzeitig beteiligt werden.

Wenn die Bestellung gesetzlich vorgeschrieben ist, gelten meist bestimmte Formvorschriften. In jedem Fall ist die Bestellung zum bDSB allen Mitarbeitern bekannt zu machen. Dabei ist darauf hinzuweisen, dass jeder Mitarbeiter sich in eigenen und dienstlichen Angelegenheiten unmittelbar an den bDSB wenden kann.

Die unabhängige und organisatorisch herausgehobene Stellung ist für eine wirkungsvolle Tätigkeit des bDSB von ausschlaggebender Bedeutung. Er darf bei der Wahrnehmung seiner Aufgaben nicht den Weisungen der Organisationseinheiten unterliegen, die er zu kontrollieren hat. In seiner Funktion als bDSB sollte er der Leitung des Hauses zugeordnet sein, entweder durch unmittelbare Unterstellung oder im Sinne einer Stabsfunktion. Dies ist im Organigramm für alle Mitarbeiter erkennbar darzustellen.

Der bDSB muss das direkte und jederzeitige Vortragsrecht bei der Behörden- bzw. Unternehmensleitung haben und über das Geschehen in der Behörde bzw. dem Unternehmen, soweit es einen Bezug zu seiner Tätigkeit hat, umfassend und frühzeitig unterrichtet werden. Er ist an datenschutzrelevanten Vorgängen zu beteiligen, und Planungen, die den Umgang mit personenbezogenen Daten betreffen, sind ihm bekannt zu geben.

Der bDSB muss von der Behörden- bzw. Unternehmensleitung und von allen Mitarbeitern unterstützt werden. Soweit erforderlich, sind ihm Hilfspersonal sowie Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Für den Fall, dass er vertiefte rechtliche oder technische Beratung benötigt, müssen ihm geeignete Ansprechpartner der betreffenden Fachabteilungen benannt werden, auf die er bei Bedarf zurückgreifen kann.

Der bDSB soll dazu beitragen, dass seine Behörde bzw. sein Unternehmen den Erfordernissen des Datenschutzes umfassend Rechnung trägt. Er hat die Einhaltung der Vorschriften des Datenschutzes in allen Bereichen zu überwachen. Er nimmt seine Aufgaben im Wesentlichen durch Beratung und Kontrollen wahr. Seine vorrangige Aufgabe ist die Beratung. Für die Mitarbeiter sollte der bDSB Ansprechpartner in allen Fragen des Datenschutzes sein, an den sie sich jederzeit vertrauensvoll wenden können.

Bei Schwachstellen und Versäumnissen sollte er zunächst gemeinsam mit den Beteiligten nach konstruktiven Lösungen suchen. Wichtig ist dabei, den Mitarbeitern bewusst zu machen, dass Datenschutz positiv und nützlich ist. Bei angemessener Verwirklichung wird der Datenschutz Arbeitsabläufe im Ergebnis eher fördern als erschweren. Wenn nämlich eine Behörde bzw. ein Unternehmen zu viele personenbezogene Daten sammelt, personenbezogene Daten zu spät löscht oder unberechtigt übermittelt, verstößt sie nicht nur gegen Datenschutzrecht, sondern verursacht auch erhöhten Verwaltungsaufwand und Mehrkosten. Vor allem ist der Datenschutz ein wichtiges Element eines bürger- und kundenfreundlichen Verhaltens, weil er die Verfahrensabläufe transparent macht.

Der bDSB hat das Recht, jederzeit unangekündigte Kontrollen durchzuführen. Zu diesem Zweck hat er Zutritt zu allen Räumen und kann alle Unterlagen einsehen, die personenbezogene Daten enthalten oder den Umgang mit diesen betreffen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Allerdings ist die Einsicht in Personalakten, ärztliche Unterlagen, Beihilfeakten und Sicherheitsvorgänge nur mit Einwilligung des Betroffenen zulässig.

Bei Kontrolle und Beratung im Bereich einer Personalvertretung ist deren unabhängige Stellung zu beachten. Dies schließt die Durchführung von Kontrollen allerdings nicht aus.

Der bDSB hilft der Behörden- bzw. Unternehmensleitung, ihre Verantwortung für die Wahrung des Persönlichkeitsschutzes wahrzunehmen und Zwischenfälle zu vermeiden, die dem Ansehen der Behörde bzw. des Unternehmens abträglich wären. Er sollte auch Kontakt zum Personal- bzw. Betriebsrat halten. Eine gute Zusammenarbeit ist nicht nur wegen der Sensibilität der Personaldatenverarbeitung wünschenswert.

Zur sachgemäßen Durchführung seiner Aufgaben hat sich der bDSB weiterzubilden. Sehr nützlich ist auch der Erfahrungsaustausch im Kreis mit anderen bDSB des Geschäftsbereichs oder aus Behörden bzw. Unternehmen mit ähnlichen Fachaufgaben.

Der spezielle Zuschnitt der Aufgaben des bDSB richtet sich im Einzelfall nach den zu erfüllenden Aufgaben, aber auch nach Größe, dem Aufbau und der Gliederung der jeweiligen Behörde bzw. des Unternehmens.

Der folgende Katalog gibt einen Überblick über die Aufgaben, die dem bDSB in jeder Behörde bzw. jedem Unternehmen übertragen werden können:

Grundlegende Aufgaben:

- Beratung der Hausleitung und der übrigen Mitarbeiter in datenschutz-relevanten Fragen
- Durchführung angekündigter oder unangekündigter Kontrollen

Übersichten und Register:

- Führung oder Überwachung der Führung des Verzeichnisses der eingesetzten Datenverarbeitungs-anlagen
- Führung der Übersicht über alle Dateien und Verfahren, in denen personenbezogene Daten gespeichert sind oder verarbeitet werden
- Wahrnehmung der gesetzlichen Meldepflichten

Automatisierte Abrufverfahren und Auftragsdatenverarbeitung:

- Unterrichtung der zuständigen Datenschutzkontrollinstanz über automatisierte Abrufverfahren
- Kontrolle der Einhaltung der Weisungen des Auftraggebers bei Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

Mitwirkung:

- Erarbeitung oder Mitwirkung bei der Erstellung von Richtlinien, Rundschreiben, Dienstvereinbarungen und weiteren allgemeinen Verlautbarungen, die den Umgang mit personenbezogenen Daten betreffen
- Bearbeitung oder Mitwirkung bei Auskunfts-, Berichtigungs-, Sperrungs- oder Löschungsverlangen, bei der Erstellung von Bürgerinformationen sowie bei allgemeinen Bürgereingaben und Anfragen zum Datenschutz
- Beteiligung bei der Auswertung von Protokolldateien
- Beteiligung bei der Einführung von Verfahren zur Verarbeitung personenbezogener Daten durch die Fachabteilung
- Beteiligung bei Regelungen zur Informationssicherheit

Schulung und Zusammenarbeit:

- Schulung der Mitarbeiter in datenschutzrechtlichen Aspekten sowie zur Umsetzung datenschutzrechtlicher Bestimmungen
- Regelmäßige oder gelegentliche Berichte an die Hausleitung über den Stand des Datenschutzes innerhalb der Behörde bzw. des Unternehmens
- Zusammenarbeit mit dem IT-Sicherheitsbeauftragten
- Ansprechpartner der externen Datenschutz-Kontrollinstanzen, z. B. des Bundesbeauftragten für den Datenschutz und gegebenenfalls der Datenschutzbeauftragten der vorgesetzten Behörde bzw. des Unternehmens, anderer Behörden bzw. Unternehmen des Geschäftsbereichs und öffentlicher Stellen mit verwandten Aufgaben

M 7.3 Aspekte eines Datenschutzkonzeptes

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Datenschutzbeauftragter

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Datenschutzbeauftragter

Für ein Unternehmen bzw. eine Behörde ist festzulegen und zu dokumentieren, welche Anforderungen des Datenschutzes bei der Verarbeitung personenbezogener Daten eingehalten werden müssen und wie diese Anforderungen umgesetzt worden sind. Damit können viele Fälle, in denen eingehende Untersuchungen und die Erstellung eines individuellen Datenschutzkonzeptes für einzelne Verfahren zu aufwendig sind, pauschal behandelt werden. Weiterhin ist damit eine Grundlage gegeben, die generell für alle IT-Systeme gültig und auch für neue IT-Systeme anwendbar ist, für die noch kein Datenschutzkonzept erarbeitet wurde.

Vorrangig sind natürlich die jeweils geltenden gesetzlichen Bestimmungen zu beachten. In diesem Umfeld gibt es allerdings allgemein gültige Aspekte, die bei der Verarbeitung personenbezogener Daten in der Regel zu berücksichtigen sind. Die genannten Aspekte sollen auch als Orientierungshilfe für individuelle Datenschutzkonzepte dienen.

Das Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen und kann auch als Grundlage für datenschutzrechtliche Prüfungen genutzt werden.

Zu berücksichtigende Aspekte

- Verzeichnis aller Verfahren
- Umfang und Verwendung der zu verarbeitenden personenbezogenen Daten. Ist ein direkter Bezug (z. B. Adresse, Steuerdaten) oder ein indirekter Bezug vorhanden (z. B. Kfz-Kennzeichen, Flurstück)?
- Rechtsgrundlage der Verarbeitung
- Zweckbindung
- Berücksichtigung besonderer Datenarten
- Einhaltung von Datensparsamkeit, Datenvermeidung
- Schutzbedarf der Daten: Schutzbedarfsfeststellung nach Schutzstufenkonzept und unter Berücksichtigung des Verwendungszusammenhangs (normal, hoch, sehr hoch) nach datenschutzrechtlichen Gesichtspunkten, Kategorienbetrachtung siehe BSI-Standard 100-2, Kapitel 4.2 oder auch Schutzstufenkonzepte in verschiedenen Bundesländern
- Besonderheiten bei "Automatisierten Abrufverfahren"
- Verbot automatisierter Bewertungen
- Recht auf Auskunft, Berichtigung, Sperrung, Widerspruch, Schadensersatz
- Vermeidung von Rechtsverletzungen und ihrer Folgen
- Löschung von Daten

- Protokollierung
- Vorabkontrolle (dazu gibt es Checklisten in verschiedenen Bundesländern)
- Regelung der Verantwortlichkeiten im Datenschutz (siehe M 7.2 Regelung der Verantwortlichkeiten im Bereich Datenschutz)
- Dokumentation und Verfahrensweise der Beteiligung des betrieblichen bzw. behördlichen Datenschutzbeauftragten
- Dokumentation und Verfahrensweise der Beteiligung des Bundes- oder Landesbeauftragten für Datenschutz oder Beteiligung der Aufsichtsbehörde
- Vertragliche Regelungen einer Auftragsdatenverarbeitung
- Besonderheiten einer Datenverarbeitung in Drittländern (unter Anderem Safe-Harbor-Regeln)
- Technische und organisatorische Maßnahmen nach der Anlage zu § 9 BDSG bzw. entsprechenden Regelungen in den Landesdatenschutzgesetzen oder/und nach den spezialgesetzlichen Bestimmungen, Zuordnung der Maßnahmen der IT-Grundschutz-Kataloge nach Zielvorgaben der Gesetze (Basis-Sicherheitscheck-Tabellen des BSI, eine Tabelle zu Baustein B 1.5 Datenschutz ist auf den BSI-Webseiten unter den Hilfsmitteln zum IT-Grundschutz zu finden), Soll-Ist-Abgleich bei der Umsetzung und späteren Revision und datenschutzrechtlichen Kontrolle
- Verpflichtung auf den Datenschutz bzw. entsprechende Unterrichtung (siehe Formblatt des BfDI im Internetangebot unter www.bfdi.de oder entsprechende Merkblätter der Datenschutzbeauftragten und Aufsichtbehörden)
- Freigabe der Verfahren
- Verfahrensbeschreibung für jedes Verfahren
- Meldungen an Registerstellen (siehe auch M 7.10 Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten)
- Bestellung und Aufgaben eines Datenschutzbeauftragten (siehe Maßnahme M 7.2 Regelung der Verantwortlichkeiten im Bereich Datenschutz)
- Berücksichtigung der unterschiedlichen datenschutzrechtlichen Zuständigkeiten (Bundesbeauftragter für Datenschutz, Landesbeauftragte für Datenschutz, Aufsichtsbehörden)

Ergänzende Kontrollfragen:

- Werden sämtliche Mitarbeiter, auch neu eingestellte, auf das Datenschutzkonzept hingewiesen und verpflichtet bzw. unterrichtet?
- Wird das Datenschutzkonzept regelmäßig aktualisiert?
- Werden die notwendigen Betriebsmittel für die Umsetzung des Datenschutzkonzepts bereitgestellt?
- Wurde ein Datenschutzbeauftragter bestellt?
- Liegen dem Datenschutzbeauftragten alle notwendigen Dokumentationen (z.B. Verfahrensbeschreibungen) vor?

M 7.4 Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Datenschutzbeauftragter, Fachverantwortliche

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Datenschutzbeauftragter, Fachverantwortliche

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

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

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

Zulässigkeit der Datenverarbeitung

Für die Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt (z. B. § 4 Abs. 1 BDSG).

Die Prüfung der Zulässigkeit der Datenverarbeitung sollte im Regelfall in Zusammenarbeit mit den fachlich zuständigen Stellen erfolgen.

Vor der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist zu prüfen, ob

- dies durch die Datenschutzgesetze oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet ist oder
- der Betroffene gemäß § 4 BDSG oder entsprechender landes- oder spezialgesetzlicher Regelungen eingewilligt hat.

Bei der Speicherung, Veränderung und Übermittlung personenbezogener Daten durch nicht-öffentliche Stellen ist zu prüfen, ob dies

- im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen erfolgt oder
- zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (im Sinne von §§ 28 ff. BDSG).

Prüfung der Erforderlichkeit

Für öffentliche Stellen gilt der Grundsatz, dass personenbezogene Daten nur erhoben werden dürfen, wenn sie für die Aufgabenerfüllung erforderlich sind. Das ist der Fall, wenn ohne ihre Kenntnis die Durchführung der betreffenden Aufgaben unmöglich oder wesentlich erschwert wäre. Dies ist im Einzelfall zu überprüfen.

Die einzelnen Nutzer dürfen nur auf diejenigen Daten zugreifen, die für die Erfüllung ihrer Aufgaben erforderlich sind.

Schwierigkeiten bereitet dies hinsichtlich der Systemverwalter. Sie haben in den marktüblichen Systemen beliebigen Zugriff auf alle Daten. Auch sie müssen in bestimmtem Umfang im Zugriff beschränkt werden, insbesondere dann, wenn es sich um Daten handelt, die einem besonderen Amtsgeheimnis unterliegen, wie etwa Personalaktendaten. Geeignete Maßnahmen hierfür sind Verschlüsselung der Daten, Zugriffsbeschränkungen, abgestufte Berechtigungskonzepte, Menüführung, Aufteilung der Systemadministratorfunktionen auf verschiedene Rollen sowie die sichere Protokollierung der Aktivitäten des Systemverwalters.

Bei der Gestaltung von Technik sind solche Verfahren zu wählen, bei denen möglichst wenig personenbezogene Daten verarbeitet werden. Es gilt das Gebot der Datenvermeidung bzw. Datensparsamkeit. Soweit möglich, sind Verfahren anonym zu gestalten oder Pseudonyme zu verwenden. Bei Dienstleistungsangeboten sollte den Kunden zumindest die Möglichkeit gegeben werden, ein anonymes Verfahren zu wählen.

Prüfung der Verwendung von Daten hinsichtlich der Zweckbindung

Vor der Speicherung, Veränderung und Nutzung personenbezogener Daten ist zu prüfen, ob dies für die Zwecke erfolgt, für die die Daten erhoben worden sind bzw., falls keine Erhebung voranging, es für die Zwecke erfolgt, für die sie gespeichert worden sind.

Von diesem Zweckbindungsgrundsatz gibt es eine Reihe, zum Teil weit reichender gesetzlicher Ausnahmen (siehe z. B. § 14 BDSG).

Prüfung der Verwendung der Daten hinsichtlich der besonderen Zweckbindung

Es ist zu prüfen, ob personenbezogene Daten, die zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, auch ausschließlich für diese Zwecke verwendet werden (siehe z. B. § 14 Abs. 4, § 31 BDSG).

Vorabkontrolle

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

Weist eine Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen auf wie z. B. die Verarbeitung besonderer Datenarten (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) oder soll damit die Persönlichkeit des Betroffenen einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens bewertet werden, ist vor dem Beginn der Verarbeitung eine Vorabkontrolle durchzuführen (§ 4d Abs. 5 BDSG). Eine Vorabkontrolle ist nicht durchzuführen, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. In manchen Landesdatenschutzgesetzen ist eine Vorabkontrolle generell bei allen Verfahren vorgeschrieben, mit denen personenbezogene Daten durch öffentliche Stellen verarbeitet werden. Die Voraussetzungen hierfür können von den beim Bund geltenden Regelungen abweichen.

Automatisierte Verfahren dürfen nur dann eingesetzt werden, wenn sichergestellt ist, dass keine Gefahren für das informationelle Selbstbestimmungsrecht bestehen.

Folgende Aspekte sind hierbei zu überprüfen:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobene Daten

Die zu ergreifenden Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Gefahren und der Art der zu schützenden personenbezogenen Daten angemessen ist.

Werden personenbezogene Daten nicht automatisiert verarbeitet, sind Maßnahmen zu treffen, die den Zugriff Unbefugter bei der Verarbeitung, der Aufbewahrung, dem Transport und der Vernichtung verhindern.

Die Anforderungen weichen in den Formulierungen und Konsequenzen der einzelnen Landesdatenschutzgesetze voneinander ab. Eine Entscheidung über die Durchführung der Vorabkontrolle ist daher im Einzelfall zu treffen.

M 7.5 Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Fachverantwortliche, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter

Ein sehr wichtiger Bereich des Datenschutzes sind die technischen und organisatorischen Maßnahmen, die getroffen werden müssen, damit das Recht auf informationelle Selbstbestimmung gewährleistet ist und die personenbezogenen Daten vor Missbrauch, Fehlern und Unglücksfällen möglichst sicher sind.

Welche Maßnahmen notwendig sind, hängt nicht nur von der Art der Daten und der Aufgabe ab, für die sie verwendet werden sollen, sondern ebenso von den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen.

Die Gesetze verzichten deshalb darauf, bestimmte einzelne Maßnahmen zwingend vorzuschreiben, sondern verlangen nur allgemein, "die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieser Gesetze zu gewährleisten".

Welche Wirkung diese Maßnahmen im Bereich der automatisierten Verarbeitung haben müssen, legen die Datenschutzgesetze katalogmäßig fest. Nach 9 BDSG müssen die Maßnahmen geeignet sein,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Diese Anforderungen weichen in den Formulierungen und Konsequenzen der einzelnen Landesdatenschutzgesetze voneinander ab.

Entscheidend bei Planung und Durchführung der technischen und organisatorischen Maßnahmen ist, dass sie als ein zusammenwirkendes Schutzsystem verstanden werden. Ein solches Schutzsystem sichert neben dem rechtlich erforderlichen Datenschutz auch die ordnungsgemäße Aufgabenerfüllung und einen ordentlichen Betriebsablauf. Deshalb ist es wichtig, das Datenschutzkonzept jeweils in Abstimmung mit den Fachkonzepten der betreffenden Organisationseinheiten und den sonstigen Sicherheitskonzepten, z. B. dem IT-Sicherheitskonzept, zu entwickeln und anzuwenden.

Der Aufwand für die notwendigen Maßnahmen sollte in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen (zu den Schutzstufen siehe BSI-Standard 100-2 bzw. landesspezifische Regelungen zum Datenschutz). Je schwerer die den Betroffenen drohende Rechtsverletzung und je größer das Risiko eines Schadenseintritts ist, umso höher ist der angemessene Aufwand. Ein Ermessen besteht zwar bei der Auswahl der einzelnen Maßnahmen, nicht aber bei der Festlegung des Schutzniveaus. Als notwendig erkannte Maßnahmen sind auch dann zu treffen, wenn sie die Entwicklung und den Einsatz einer IT-Anwendung erschweren. Ist dies mit den vorgesehenen Maßnahmen nicht zu gewährleisten, muss entweder ein höherer Aufwand in Kauf genommen werden oder eine andere, mit weniger Aufwand verbundene Verfahrensgestaltung in Betracht gezogen werden. Diese Maßnahmen sind entsprechend dem aktuellen Stand der Technik fortzuschreiben.

Ebenso ist sicherzustellen, dass die gesetzlichen Datenschutzvorschriften durch IT-Sicherheits- und Datenschutz-Regelungen umgesetzt werden.

Soweit ein behördlicher bzw. betrieblicher Datenschutzbeauftragter (bDSB) institutionalisiert ist (in einigen Datenschutzgesetzen bestehen hierzu gesetzliche Vorgaben), sollten Richtlinien, Rundschreiben o. ä., die die Hausleitung als Querschnittsregelung zum Umgang mit personenbezogenen Daten in der gesamten Dienststelle erlässt, mit seiner Beteiligung erarbeitet werden.

Er sollte stets bei der Behandlung von Dienst- bzw. Betriebsvereinbarungen zwischen Dienststelle bzw. Betrieb und Personal- bzw. Betriebsrat über den Umgang mit personenbezogenen Daten hinzugezogen werden. Die Einhaltung der Regelungen sollte kontrolliert werden.

Beispiele für technisch-organisatorische Maßnahmen sind

- das physikalische Löschen von Daten (siehe z. B. M 4.32 Physikalisches Löschen der Datenträger vor und nach Verwendung),
- die kryptographische Verschlüsselung (siehe z. B. M 5.36 Verschlüsselung unter Unix und Windows NT),
- interne IT- und Datenschutz-Regelungen (siehe z. B. M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz) sowie

- Protokollierung und Dokumentation von Verfahren, um die Nachvollziehbarkeit zu gewährleisten (siehe z. B. M 4.25 Einsatz der Protokollierung im Unix-System).

Eine Übersicht der Maßnahmen der IT-Grundschutz-Kataloge, die zur Erreichung der oben genannten Anforderungen geeignet sind, wird in der Tabelle zu Baustein B 1.5 *Datenschutz* unter den Hilfsmitteln zum IT-Grundschutz dargestellt.

M 7.6 Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Datenschutzbeauftragter, Personalabteilung, Vorgesetzte

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

Einzelne Landesdatenschutzgesetze haben die Verpflichtung durch eine Unterrichtung ersetzt.

Hinweis:

Auch wenn eine Verpflichtung bzw. Unterrichtung der Mitarbeiter zur Wahrung des Datengeheimnisses bereits aus anderen Gründen besteht, sollte sie wiederholt werden, um die Mitarbeiter für die Belange des Datenschutzes zu sensibilisieren. Sowohl für den behördlichen als auch den betrieblichen Datenschutzbeauftragten gibt es als Hilfsmittel entsprechende Muster-Verpflichtungserklärungen des Bundesbeauftragten für Datenschutz unter www.bfdi.de. Für die Unterrichtung gibt es geeignete Merkblätter bei den Landesbeauftragten für Datenschutz.

M 7.7 Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten

Verantwortlich für Initiierung: Fachverantwortliche, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Fachverantwortliche, Datenschutzbeauftragter

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

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

Beispiele:

- Ein Verfahren zur Verarbeitung personenbezogener Daten enthält ein Auswerteprogramm oder einen Menüpunkt, mit dessen Hilfe ein vollständiger Ausdruck der gespeicherten Daten des Betroffenen erzeugt wird.
- Ein Verfahrensverzeichnis wird mit Hilfe einer Datenbank so automatisiert, dass über bestimmte Stichworte ein sehr einfacher Zugriff auf den umfangreichen Datenbestand möglich ist und damit alle Querbezüge erkannt werden können.

M 7.8 Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten

Verantwortlich für Initiierung: Leiter IT, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Fachverantwortliche, Datenschutzbeauftragter

Neben den zentralen Datenverarbeitungsanlagen sind bei dezentraler Datenverarbeitung alle eingesetzten IT-Systeme zu erfassen (siehe auch BSI-Standard 100-2, Erfassung der IT-Systeme und Erfassung der IT-Anwendungen und der zugehörigen Informationen).

Es muss jederzeit auf ein aktuelles Verzeichnis der eingesetzten Hardware, Software und Verfahren sowie der erfassten personenbezogenen Daten zugegriffen werden können. In einigen Datenschutzvorschriften gibt es konkrete Vorgaben für die Ausgestaltung dieser Verzeichnisse.

Verfahren automatisierter Verarbeitungen zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sind von der verantwortlichen Stelle in einer Übersicht (Verfahrensverzeichnis) zu führen. Die Übersicht enthält grundsätzlich die Angaben nach §§ 4d und 4e BDSG und wird nach § 4g Absatz 2 BDSG in den meisten Fällen vom bDSB geführt. Ähnliche Regelungen enthalten auch die Datenschutzgesetze der Länder, sofern die Bestellung eines bDSB vorgesehen ist.

Unter bestimmten Voraussetzungen sind nicht-öffentliche Stellen verpflichtet, Registermeldungen, die mit den Angaben des Verfahrensverzeichnisses weitgehend übereinstimmen, gegenüber der zuständigen Aufsichtsbehörde abzugeben. Von der Meldepflicht sind nach § 4d Abs. 4 BDSG im Prinzip nur Stellen erfasst, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung verarbeiten.

Während für öffentliche Stellen des Bundes gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit keine Meldepflicht besteht, sind öffentliche Stellen in den Ländern nach Landesrecht teilweise dazu verpflichtet, solche Meldungen gegenüber den jeweiligen Landesbeauftragten für den Datenschutz abzugeben, insbesondere auf Grund von Regelungen in den Bereichen der Strafverfolgung und der Gefahrenabwehr.

Damit der bDSB seiner Aufgabe zur Führung des Verfahrensverzeichnisses nachkommen kann, müssen die dafür erforderlichen Angaben nach § 4e BDSG vollständig und aktuell sein. Dabei ist besonders darauf zu achten, dass die Rechtsgrundlage für die Datenverarbeitung und die Zweckbindung hinreichend präzisiert sind, damit eine spätere Zweckänderung ausschließlich im Rahmen der gesetzlichen Anforderungen erfolgen kann.

M 7.9 Datenschutzrechtliche Freigabe

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung

Software und IT-Verfahren sind mit systematisch entwickelten Fall-Konstellationen (Testdaten, keine personenbezogenen Echtdaten) nach einem Testplan, aus dem das gewünschte Ergebnis hervorgeht, zu überprüfen (siehe auch M 2.83 *Testen von Standardsoftware*). Massentests können, wenn erforderlich, nach Zustimmung und Vorgaben der fachlich dafür zuständigen Stelle mit anonymisierten Originaldaten durchgeführt werden. Die Zustimmung der fachlich zuständigen Stelle zur Anonymisierung von Originaldaten und alle Testergebnisse sind revisionssicher zu dokumentieren.

Tests mit einer Kopie der erforderlichen, nicht-anonymisierten Originaldaten (personenbezogene Echtdaten) sind nur zulässig, wenn

- eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder
- sich im Ausnahmefall trotz Nachbildung im Testbereich ein Fehler aus dem Produktionsbetrieb nicht ermitteln, sondern nur mit Originaldaten aufklären lässt, oder die Verfahrenssicherheit nicht anders gewährleistet werden kann,
- eine bereichsspezifische Rechtsvorschrift dies nicht ausdrücklich untersagt,
- eine Anonymisierung der Originaldaten für die vorgesehene Test-Konstellation nur mit einem unvertretbar hohem Aufwand verbunden wäre,
- die fachliche verantwortliche Stelle dem Vorgehen schriftlich zugestimmt hat,
- bei der Durchführung oder Auswertung des Tests die schutzwürdigen Belange der Betroffenen und die Informationssicherheit angemessen berücksichtigt werden,
- sichergestellt ist, dass nur die für die Fehlerbehebung und Durchführung des Tests erforderlichen Personen die Daten nutzen können und
- Zugang zu diesen Daten nur Personen erhalten, die den jeweils maßgebenden Vertraulichkeitsgrundsätzen und insbesondere datenschutzrechtlichen Vorschriften unterliegen.

Der/die behördliche bzw. betriebliche Datenschutzbeauftragte bzw. eine sonstige dafür zuständige Stelle ist rechtzeitig vor den geplanten Tests mit Originaldaten zu informieren.

Der Kopierzugriff auf die Originaldaten ist zu protokollieren. Nach Beendigung des Tests ist die benutzte Kopie der Originaldaten unverzüglich aus dem Testbereich zu löschen bzw. im Testbereich zu anonymisieren. Die Verwendung von Originaldatenkopien ist mit Anlass, Begründung, Umfang und Dauer, die getroffenen Sicherheitsmaßnahmen sowie die vorangehenden Tests mit Testdaten revisionssicher zu dokumentieren.

Es muss geregelt sein, wie IT-Verfahren abgenommen, freigegeben, eingespielt bzw. benutzt werden dürfen. Auf die Maßnahmen M 2.62 *Software-Abnahme- und Freigabe-Verfahren* bzw. Baustein B 1.10 *Standardsoftware* wird verwiesen.

Die Freigabe von IT-Verfahren mit der Verarbeitung personenbezogener Daten setzt eine Prüfung auch aus datenschutzrechtlicher Sicht voraus. Die vorherige Beteiligung des Landesbeauftragten für den Datenschutz wird in einigen Landesdatenschutzgesetzen vorgeschrieben.

M 7.10 Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten

Verantwortlich für Initiierung: Leiter IT, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Fachverantwortliche, Datenschutzbeauftragter

Den automatisierten Abrufverfahren kommt unter dem Aspekt des Datenschutzes und der Datensicherung besondere Bedeutung zu, weil die abrufende Stelle je nach Einrichtung eines solchen Anschlusses ohne Einzelentscheidung der zuständigen Stelle über den gesamten Bestand oder wesentliche Teile der von der übermittelnden Stelle bereitgehaltenen personenbezogenen Daten verfügen kann. Deshalb sehen die entsprechenden gesetzlichen Regelungen (z. B. § 10 BDSG) den technischen und organisatorischen Datenschutz zwingend bereits als Teil der Planung von Abrufverfahren vor.

Automatisierte Abrufverfahren werden in den Datenschutzgesetzen als eine Phase der Datenverarbeitung definiert, bei der gespeicherte oder durch Datenverarbeitung gewonnene personenbezogene Daten an einen Dritten in der Weise bekannt gegeben werden, dass die Daten durch die datenverarbeitende Stelle zum Abruf bereitgestellt werden und der Abruf durchgeführt wird.

Ein Beispiel für ein automatisiertes Abrufverfahren ist das Elektronische Grundbuch, das zugelassenen Teilnehmern nach Maßgabe der gesetzlichen Bestimmungen die unmittelbare Online-Einsicht auf Grundbuchdaten von ihren Arbeitsplatz-Rechnern ermöglicht. Dieser Dienst kann insbesondere von Notaren, Rechtsanwälten, Banken, Sparkassen und Versicherungen, aber auch Landes- und Kommunalbehörden genutzt werden, die zur Ausübung ihrer Tätigkeiten häufig auf die Grundbucheinsicht angewiesen sind.

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

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

Zu beachten ist, dass die Unterrichtung des Bundes- bzw. Landesbeauftragten für den Datenschutz über die Einrichtung eines Abrufverfahrens in einigen Datenschutzgesetzen gefordert ist.

Allgemeine Aspekte:

- Anlass und Zweck sowie beteiligte Stellen am Abrufverfahren sind festzulegen.
- Abrufberechtigungen sind festzulegen und zu kontrollieren.
- Art und Umfang der bereitgehaltenen Daten sind festzulegen.
- Sperr- und Löschfristen für Daten sind zu definieren.
- Es ist festzulegen, in welchen Fällen die speichernde Stelle von der abrufenden Stelle zu informieren ist.

Maßnahmen gegen unbefugten Abruf:

- Der Abruf von Daten durch nicht Abrufberechtigte ist durch geeignete Vorkehrungen zu verhindern:
- Nach einer festgelegten Anzahl von Fehlversuchen ist die Berechtigung zu sperren.
- Passwörter müssen in regelmäßigen Abständen gewechselt werden. Soweit möglich, ist dies durch die entsprechenden Programme zu erzwingen.
- Der Abruf besonderer Arten personenbezogener Daten muss durch ein höheres Schutzniveau gesichert werden (Besitz und Wissen).
- Zur Überprüfung der Protokolldateien sollten programmgesteuerte Prüfungsverfahren eingesetzt werden.
- Art und Umfang der Protokollierung müssen festgelegt werden.
- Es sollten zufallsgesteuerte Stichprobenkontrollen oder eine Dauerprotokollierung durchgeführt werden.
- Es ist festzulegen, an welcher Stelle die Protokollierungen durchgeführt werden, ob bei der abrufenden Stelle, bei der speichernden Stelle, oder an beiden Stellen.
- Die Protokollierung muss so konzipiert sein, dass nachträglich festgestellt werden kann, aufgrund wessen Abrufberechtigung Daten abgerufen wurden.
- Die Gründe des Abrufs müssen protokolliert werden.
- Beim Abruf von Daten sollte protokolliert werden, über welchen Anschluss und welche Endgeräte die Übertragung stattfindet.

Netzanbindung:

Bei der Vernetzung von IT-Systemen ist zu überprüfen, wie der Netzanschluss der Endsysteme realisiert ist. Bei Wählanschlüssen ist beispielsweise zu überprüfen, welche IT-Sicherheitsmaßnahmen vorgesehen sind, bei virtuellen Festverbindungen, ob geschlossene Benutzergruppen eingerichtet worden sind. In lokalen Netzen sollten geschlossene Benutzergruppen so eingerichtet werden, dass sie jeweils nur geschlossene Organisationseinheiten umfassen.

M 7.11 Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten

Verantwortlich für Initiierung: Leiter IT, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Fachverantwortliche, Datenschutzbeauftragter

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

Der Auftrag ist im Rahmen der gesetzlichen Vorgaben schriftlich zu erteilen und etwaige Unterauftragsverhältnisse sind festzulegen (§ 11 BDSG). In einigen Bereichen sind zusätzliche gesetzliche Regelungen zu beachten, z. B. Krankenhausgesetze der Länder.

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

Auftragnehmer müssen sicherstellen, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Unterauftragsverhältnisse unterliegen der Zustimmung des Auftraggebers.

Wenn der Auftragnehmer keine öffentliche Stelle ist, sind die mit der Verarbeitung personenbezogener Daten beschäftigten Personen bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

Bei Sozialdaten sind die Regelungen des Sozialgesetzbuches (SGB) zu beachten. Die Verarbeitung personenbezogener Daten im Auftrag durch nichtöffentliche Stellen ist nur zulässig, wenn anders Störungen im Betriebsablauf auftreten können oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfass (§ 80 Abs. 5 SGB X). Bei den Aufsichtsbehörden haben die erforderlichen Anzeigen zu erfolgen.

Der Auftraggeber und gegebenenfalls der zuständige Datenschutzbeauftragte haben ein jederzeitiges Kontrollrecht.

M 7.12 Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten

Verantwortlich für Initiierung: Leiter IT, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Fachverantwortliche, Datenschutzbeauftragter

In den typischen IT-Anwendungen wird der Benutzer am Bildschirm vom Rechner mittels "Masken" durch ein "Menü" geführt. Diese erleichtern ihm die Benutzung des Programms durch vorformulierte "Fragebögen", in denen er seine Abfragen z. B. "ankreuzen" kann. Sie erlauben nur solche Abfragen und Auswertungen, die vom Anwendungsprogramm vorgegeben, unter Datenschutzaspekten geprüft und genehmigt sind. Andere Abfragen werden abgewiesen. Anders ist dies bei Datenbanksprachen ("freien Abfragesprachen") und moderner Office-Software: Sie ermöglichen dem Anwender, selbst Abfragen über den Datenbestand zu formulieren, ohne an die Restriktionen einer strikten Menüführung gebunden zu sein. Damit könnten auch Auswertungen gemacht werden, die nicht erforderlich und damit nicht zulässig sind.

Da die technische Entwicklung inzwischen Möglichkeiten bietet, die mit einer "freien Abfragesprache" verbundenen datenschutzrechtlichen Risiken abzubauen, kann in begründeten Einzelfällen der eingeschränkte Einsatz "freier Abfragesprachen" vertretbar sein. Eine Beeinträchtigung des Persönlichkeitsrechts der Betroffenen muss aber ausgeschlossen sein. Auch die Zustimmung der Personal- bzw. Betriebsräte ist einzuholen. Die Möglichkeit zum Einsatz "freier Abfragesprachen" bzw. der Funktionalität von Office-Software ist weitestgehend zu beschränken. Datenauswertungen, die voraussehbar regelmäßig zur Aufgabenerfüllung benötigt werden, sind über Menüsteuerung bzw. Bildschirmmasken zur Verfügung zu stellen. Der Einsatz "freier Abfragesprachen" sollte auf Ausnahmefälle beschränkt bleiben.

Bevor die sogenannten freien Abfragesprachen im Zusammenhang mit personenbezogener Datenverarbeitung zugelassen werden, muss geprüft werden, ob dies mit der Schutzwürdigkeit der Daten vereinbar ist. Wenn es grundsätzlich vereinbar ist, sollten folgende Anforderungen beachtet werden: Das System muss eine technische Begrenzung aufweisen, ähnlich einem Filter, der sicherstellt, dass die "freie Abfragesprache" nur im vereinbarten Umfang eingesetzt werden kann. Der Umfang kann beispielsweise durch eine Zugriffsbeschränkung auf bestimmte, weniger sensitive Datenfelder festgelegt sein. Ein Umgehen des Filters ist insbesondere programmtechnisch zu verhindern.

Die Daten, auf die mit einer solchen Abfragesprache zugegriffen werden soll, und die zu eröffnenden Abfragearten müssen vorab geprüft werden. Kriterien sind hierbei insbesondere

- die Erforderlichkeit für die Aufgabenerfüllung,
- der Nachweis, dass eine anonymisierte Auswertung für den jeweils verfolgten Zweck nicht genügt;

- die Sensibilität der einzelnen Daten in der vorgesehenen Verknüpfung und Systemumgebung sowie
- der jeweilige Zweck und Kontext der Datennutzung.

Keine datenschutzrechtlichen Bedenken bestehen gegen den Einsatz einer "freien Abfragesprache" dann, wenn die Auswertung nur zu anonymisierten Ergebnissen führt, d. h. Rückschlüsse auf einzelne Personen nicht möglich sind.

M 7.13 Dokumentation der datenschutzrechtlichen Zulässigkeit

Verantwortlich für Initiierung: Leiter IT, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Fachverantwortliche

Bevor Software oder Hardware für die Verarbeitung von personenbezogenen Daten eingesetzt werden, sollten sie, bezogen auf den vorgesehenen Einsatz, auf die datenschutzrechtliche Zulässigkeit geprüft werden. Hier wird es je nach IT-System (z. B. nicht vernetzter PC oder zentrales Rechenzentrum) sehr unterschiedliche Anforderungen geben. Das Prüfungsergebnis sollte dokumentiert werden. Für Datenschutzkontrollen sind derartige Dokumentationen besonders wichtig.

Der betriebliche bzw. behördliche Beauftragte für den Datenschutz (bDSB) ist nach § 4g Abs. 1 BDSG über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten. Er hat die ordnungsgemäße Anwendung (vorhandener und neuer) Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet sollen, zu überwachen. Aus diesem Grunde empfiehlt es sich, den bDSB von Anfang an, d.h. im Rahmen der ersten Planungen, mit einzubeziehen. Nur so können bereits in der Planungsphase datenschutzrechtliche Fehler vermieden werden, deren Behebung zu einem späteren Zeitpunkt unter Umständen zeit- und kostenintensiv sein könnten.

M 7.14 Aufrechterhaltung des Datenschutzes im laufenden Betrieb

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter

Abgesehen von der Bestellung eines betrieblichen bzw. behördlichen Datenschutzbeauftragten (bDSB) ist die Einrichtung einer internen IT-Revision und Datenschutzkontrolle eine wichtige Maßnahme im Rahmen der durch die Datenschutzgesetze vorgeschriebenen Organisationskontrolle. Sie hilft dabei, vor Ort und zeitnah die Sicherheit der Datenverarbeitung und die Einhaltung der datenschutzrechtlichen Anforderungen zu gewährleisten.

Die IT-Revision überprüft die Ordnungsmäßigkeit der Datenverarbeitung durch Kontrolle der Umsetzung des IT-Sicherheitskonzeptes. Dazu gehören insbesondere eine Kontrolle der Dokumentation der Verfahren, der vorgeschriebenen Verfahrensanwendung und der gesamten Sicherheitsmaßnahmen.

Die interne Datenschutzkontrolle, die meist dem Datenschutzbeauftragten obliegt (vergleiche M 7.2 *Regelung der Verantwortlichkeiten im Bereich Datenschutz*), überprüft hingegen die Einhaltung der aus den Datenschutzgesetzen herrührenden Anforderungen. Dazu gehören:

- die Kontrolle der Verfahren auf Einhaltung der Rechtsgrundlage und der Zweckbestimmung,
- die Sicherstellung der Rechte des Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung und Schadensersatz,
- die Unterrichtung über bzw. die Verpflichtung der Mitarbeiter auf den Datenschutz,
- das Führen von Datei- bzw. Verfahrensübersichten und Geräteverzeichnissen und
- die Kontrolle der aus den gesetzlichen Vorschriften abgeleiteten technisch-organisatorischen Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und "getrennte Verarbeitung gemäß der Zweckbestimmung".

IT-Revision und Datenschutzkontrolle arbeiten sinnvollerweise zusammen und ergänzen sich. Durch zeitnahe Überprüfung der Protokolldaten helfen sie z. B. mit, einen möglichen Missbrauch schnell aufzudecken und die Aufbewahrungszeit und den Umfang der Protokolldaten so gering wie möglich zu halten. Sie können die Leitung der datenverarbeitenden Stelle bei der Neukonzeption und der Fortentwicklung von Verfahren beraten und dienen als kompetente Ansprechpartner bei Kontrollbesuchen der Aufsichtsbehörden oder des Bundes- und der Landesbeauftragten für Datenschutz. Beide Funktionen können Mitarbeitern auch im Nebenamt übertragen und bei kleinen Stellen auch in einer Hand zusammengelegt werden. Grundsätzlich ist aber darauf zu achten, dass keine Interessenkollision

mit sonst wahrgenommenen Aufgaben eintritt (siehe auch M 7.2 *Regelung der Verantwortlichkeiten im Bereich Datenschutz*).

M 7.15 Datenschutzgerechte Löschung/Vernichtung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter

Sicheres Löschen magnetischer Datenträger

Sowohl aus der Sicht des Datenschutzes als auch der IT-Sicherheit ist beim Löschen von sensiblen oder vertraulichen Daten auf magnetischen Datenträgern zu gewährleisten, dass die Daten sicher, d.h. vollständig und unumkehrbar gelöscht werden. Einfache Löschbefehle des jeweiligen Betriebssystems oder auch das Formatieren des Datenträgers reichen hierzu in der Regel nicht aus, da eine Rekonstruktion der Daten mit frei verfügbaren Softwarewerkzeugen leicht möglich ist. Daten, die sicher gelöscht werden sollen, müssen durch physikalische Maßnahmen (mechanische oder thermische Zerstörung, magnetische Durchflutung des Datenträgers) oder durch mehrmaliges Überschreiben unkenntlich gemacht werden. Beim Löschen durch Überschreiben sind die spezifischen Besonderheiten der Verwaltung und Speicherung von Daten zu berücksichtigen, wie z.B. die Existenz von Sicherheitskopien, von automatisch durch das System oder einzelne Anwendungen angelegten temporären und Auslagerungsdateien oder von Journalen bei bestimmten Dateisystemen.

Aus Datenschutzsicht gibt es in diesem Zusammenhang die folgenden Empfehlungen:

- Der Problemkreis des sicheren Löschens von Daten erfordert die Sensibilisierung der verantwortlichen Entscheidungsträger, Administratoren, Sicherheits- und Datenschutzbeauftragten sowie jedes einzelnen Nutzers. Dies ist durch geeignete Information und Schulung zu erreichen.
- Im jeweiligen Verantwortungsbereich sind technisch-organisatorische Maßnahmen festzulegen, die eine sichere Löschung von Daten gewährleisten. Sie sind in das übergreifende Datenschutz- bzw. Sicherheitskonzept zu integrieren. Insbesondere sind Maßnahmen vor der Veräußerung, Vermietung, Aussonderung, Rückgabe, Reparatur und Wartung von Datenträgern zu bestimmen.
- Die Maßnahmen sind durch konkrete Handlungsanweisungen für das sichere Löschen zu untersetzen. Diese Anweisungen müssen den Schutzbedarf der zu löschenden Daten ebenso berücksichtigen wie den Aufwand und die Kosten für eine mögliche Datenwiederherstellung.
- Schutzwürdige Daten sind (soweit möglich) bereits in verschlüsselter Form auf dem Datenträger zu speichern. Hierzu sollten verschlüsselte Dateisysteme verwendet werden. Auch für temporäre und Auslagerungsdateien sowie für Sicherheitskopien sollten verschlüsselte Dateisysteme verwendet werden, da diese ebenfalls schutzwürdige Daten enthalten können.
- Daten auf intakten Datenträgern sind durch das ein- oder mehrmalige, komplette Überschreiben mit Zufallszahlen zu löschen. Hierbei können spezielle Softwarewerkzeuge zum Einsatz kommen.

Die Verwendung gleichförmiger Überschreibmuster beim Löschen ist nicht zu empfehlen, da so kein Schutz gegen ausführliche Laboranalysen besteht.

- Das einmalige, komplette Überschreiben mit Zufallszahlen sollte beim Löschen von Daten jeder Art praktiziert werden. Die Überschreibprozedur sollte aus mindestens zwei, besser drei Durchläufen bestehen. Beim zweiten Durchlauf sollte das zum ersten Durchlauf komplementäre Muster (Bitfolge) verwendet werden. Für den dritten Durchlauf werden Zufallsdaten empfohlen. Dadurch wird eine verbesserte Schutzwirkung erzielt.
- Soll ein noch intakter Datenträger verkauft, vermietet, ausgesondert, zurückgegeben oder einer neuen Nutzung zugeführt werden, ist zuvor der gesamte Datenträger mehrmals komplett mit Zufallszahlen zu überschreiben. Diese Form der Wiederaufbereitung gestattet anschließend die weitere Nutzung des Datenträgers (z.B. die Neuinstallation eines Betriebssystems).
- Das selektive Löschen einzelner Dateien durch Überschreiben ist meist problematisch. Es eignet sich nur dann, wenn sichergestellt ist, dass keine Kopien der in diesen Dateien enthaltenen Daten an anderen Orten abgelegt wurden (z.B. in temporären Dateien, Auslagerungsdateien oder Sicherungskopien) oder diese Orte eindeutig bestimmt und auch die Kopien sicher gelöscht werden können. Weiter ist zu gewährleisten, dass die Metadaten der gelöschten Dateien überschrieben werden, falls sie sensible Informationen enthalten.
- Bei der Festlegung von technisch-organisatorischen Maßnahmen sowie von Handlungsanweisungen für das Löschen durch Überschreiben sind geeignete Softwarewerkzeuge anhand eines Kriterienkatalogs auszuwählen, zu bewerten und für die betreffenden Nutzer bereitzustellen. Die Anwendung der Werkzeuge ist stichprobenartig zu kontrollieren.
- Defekte Datenträger, deren Daten nicht mehr mit Softwarewerkzeugen überschrieben werden können, sind durch mechanische oder thermische Zerstörung (Disketten, Festplatten) bzw. durch magnetische Durchflutung (Disketten) unbrauchbar zu machen. Um die Zuverlässigkeit der Verfahren zu sichern, ist eine korrekte Anwendung zu gewährleisten.
- Müssen Datenträger ohne sicheres Löschen der Daten aus der Hand gegeben werden (z.B. Reparatur, Rückgabe an den Hersteller in der Garantiezeit), ist in Abhängigkeit von der Sensibilität der Daten durch vertragliche Regelungen und eventuell mit Schadensersatzansprüchen zu verhindern, dass unerwünschte Informationsflüsse stattfinden oder von Angreifern ausgenutzt werden. Gegebenenfalls ist auf Garantieansprüche zu verzichten.

Vernichten von Unterlagen

Da die Aussonderung und Vernichtung von Unterlagen im Allgemeinen in mehreren Schritten erfolgt, sind von der Zwischenlagerung in Papierkörben oder Sammelbehältern oder dem Sammeln der Unterlagen am Arbeitsplatz über den Transport und die zentrale Deponierung bis hin zum eigentlichen Vernichtungsverfahren alle Sicherheitsaspekte zu betrachten.

Allgemeine Anforderungen

Soweit keine bereichsspezifischen Vernichtungsregelungen einschlägig sind, unterliegt die Vernichtung von Unterlagen mit personenbezogenen Daten in den öffentlichen Stellen des Bundes und im nicht-öffentlichen Bereich dem Bundesdatenschutzgesetz, ansonsten den jeweiligen Landesdatenschutzgesetzen.

Dabei sind die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung der Daten sicherzustellen; dies gilt auch für den Verarbeitungsschritt "Vernichtung". Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Werden personenbezogene Daten in nicht-automatisierten Dateien oder in Akten verarbeitet, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

Grundsätzlich gilt, dass eine Stelle für die Sicherheit der Daten in Unterlagen, die vernichtet werden sollen, solange verantwortlich ist, bis die in den Unterlagen enthaltenen personenbezogenen Daten als gelöscht im Sinne der Datenschutzgesetze gelten können, die Vernichtung also abgeschlossen ist. Die betroffene Stelle muss daher über alle Unterlagen mit personenbezogenen Daten bis zu deren Vernichtung die uneingeschränkte Verfügungsgewalt besitzen. Insbesondere dürfen zu vernichtende Unterlagen mit personenbezogenen Daten vor Abschluss der Vernichtung nicht in das Eigentum Dritter übergehen.

Der Zustand, in dem die Unterlagen als vernichtet gelten können, ist festzulegen. Als Orientierung kann hierzu die Norm DIN 32757 (Vernichten von Informationsträgern) herangezogen werden. Hiernach ist eine Informationsträgervernichtung dann ausreichend, wenn die Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter erheblichem Aufwand an Personen, Hilfsmitteln oder Zeit möglich ist (Sicherheitsstufe 3).

Auch für die Vernichtung von Unterlagen gilt, dass sich die betroffene Stelle regelmäßig durch Kontrollen von der ordnungsgemäßen Durchführung der Vernichtung zu überzeugen hat. Daraus folgt, dass insbesondere dann, wenn die Vernichtung als Auftrag nach außerhalb vergeben wurde, die betroffene Stelle den gesamten technischen Vorgang oder das Verfahren kennen muss. Mit der Kontrolle der Vernichtung von Unterlagen sollte eine Person oder Organisationseinheit schriftlich beauftragt werden.

Vernichtung von Unterlagen in Eigenregie

Oberstes Prinzip sollte sein, dass Unterlagen möglichst umgehend von den Stellen vernichtet werden, die die Einstufung zur Aussonderung vornehmen. Zwischenlagerungen und Weiterreichungen über viele Hände sind fehleranfällig und erfordern genaue Regelungen und Kontrollen. Insofern ist eine unmittelbare Unterlagenvernichtung durch die zuständige Sachbearbeitung ein wirksamer Datenschutz. In jedem Fall sollte schriftlich geregelt sein, wie Mitarbeiterinnen und Mitarbeiter die Vernichtung ihrer

Unterlagen durchzuführen haben. Daneben sind sie zu verpflichten, die Unterlagen bis zu deren Vernichtung sicher zu verwahren.

Werden Unterlagen zentral vernichtet, ist der gesamte Ablauf schriftlich zu regeln. Dies gilt beispielsweise für zentrale, besonders zu sichernde Sammelstellen, wie auch für den Transport zur Sammelstelle. Die Sicherheit der zu vernichtenden Unterlagen ist ebenfalls bis zu deren Ablieferung bei der Sammelstelle zu gewährleisten. Falls die Unterlagen durch einen zentralen Dienst eingesammelt werden, ist auch diese Phase unter Sicherheitsaspekten zu betrachten. Die Vernichtung der Unterlagen ist in geeigneter Weise zu protokollieren.

Vernichtung von Unterlagen durch externe Stellen

Werden Unterlagen durch externe Dritte als "**Datenverarbeitung im Auftrag**" vernichtet, ist die gesamte Handhabung und Sicherung der Unterlagen zwischen der Übergabe und dem Abschluss der Vernichtung vertraglich festzulegen. Es müssen der Transport, eine eventuell erforderliche Zwischenlagerung, der Vernichtungsort und der höchstzulässige Zeitraum zwischen der Übergabe der Unterlagen sowie dem Abschluss der Vernichtung geregelt sein. Weiter ist schriftlich festzulegen, in welchem Zustand sich die Unterlagen zu befinden haben, um als vernichtet gelten zu können. Durch den Auftragnehmer ist zu gewährleisten, das Unbefugte keine Kenntnis der in den Unterlagen gespeicherten Daten erhalten können. Die Übergabe von Unterlagen an das Auftragsunternehmen sollte quittiert werden und die Durchführung jeder Vernichtungsaktion sollte schriftlich bestätigt werden. Generell gilt, dass die Erteilung von Unterauftragsverhältnissen möglichst ausgeschlossen werden sollte.

Die betroffene Stelle muss über ihre Unterlagen bis zum Abschluss der Vernichtung uneingeschränkt verfügen können. Die Unterlagen müssen deshalb bis zum Abschluss der Vernichtung in ihrem Eigentum bleiben. Dies beinhaltet, dass sie vor ihrer Vernichtung nicht mit fremden Unterlagen vermischt werden dürfen. Es ist deshalb auch mit dem Auftragsnehmer zu vereinbaren, dass der Auftraggeber und der zuständige Datenschutzbeauftragte bis zum Abschluss der Vernichtung zu Kontrollen berechtigt ist.

Bezüglich der Regelungen zur Auftragsdatenverarbeitung wird auf Maßnahme M 7.11 *Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten* verwiesen.