Unser Wissen
für Ihren Erfolg

Leseprobe zum Download

Liebe Besucherinnen und Besucher unserer Homepage,

tagtäglich müssen Sie wichtige Entscheidungen treffen, Mitarbeiter führen oder sich technischen Herausforderungen stellen. Dazu brauchen Sie verlässliche Informationen, direkt einsetzbare Arbeitshilfen und Tipps aus der Praxis.

Es ist unser Ziel, Ihnen genau das zu liefern. Dafür steht seit mehr als 25 Jahren die FORUM VERLAG HERKERT GMBH.

Zusammen mit Fachexperten und Praktikern entwickeln wir unser Portfolio ständig weiter, basierend auf Ihren speziellen Bedürfnissen.

Überzeugen Sie sich selbst von der Aktualität und vom hohen Praxisnutzen unseres Angebots.

Falls Sie noch nähere Informationen wünschen oder gleich über die Homepage bestellen möchten, klicken Sie einfach auf den Button „In den Warenkorb“ oder wenden sich bitte direkt an:

FORUM VERLAG HERKERT GMBH
Mandichostr. 18
86504 Merching
Telefon: 08233 / 381-123
Telefax: 08233 / 381-222

E-Mail: service@forum-verlag.com
www.forum-verlag.com

Übersicht
Rechtliche Vorgaben zum Datenschutz

Was ist Datenschutz?

Der Datenschutz soll die Bürgerinnen und Bürger vor den nachteiligen Folgen einer Datenverarbeitung gleich welcher Art schützen. Insofern umschreibt § 1 BDSG das Ziel des Datenschutzes wie folgt:

> Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Warum ist Datenschutz so wichtig?

Der gesetzliche Auftrag zum Datenschutz leitet sich aus dem Grundgesetz, genauer dem sog. Persönlichkeitsrecht (Art. 2 Abs. 1 GG) ab. In seinem wegweisenden Volkszählungsurteil[1] hat das Bundesverfassungsgericht bestimmt:

> Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

In späteren Entscheidungen wurde das Grundrecht zu einem umfassenden „Grundrecht auf informationelle Selbstbestimmung" weiterentwickelt. Daneben ist stets auch das gesondert geschützte Fernmeldegeheimnis (Art. 10 GG) zu beachten.

Wozu bedarf es gesetzlicher Regelungen zum Datenschutz?

Zum einen wird mit den gesetzlichen Regelungen das Recht auf informationelle Selbstbestimmung verwirklicht. Auf der anderen Seite ist die Erhebung und Verarbeitung von Daten in jedem Lebensbereich unerlässlich. Die öffentliche und kirchliche Verwaltung käme ohne Daten nicht aus. Folglich sind in engen Grenzen Einschränkungen des Rechts auf informationelle Selbstbestimmung notwendig. Erforderlich ist dabei stets eine gesetzliche Grundlage, in der insb. die Voraussetzungen und Grenzen der Einschränkung, also der Datenerhebung und -verarbeitung, geregelt sind. Diese gesetzliche Grundlage bildet auf Bundesebene das Bundesdatenschutzgesetz (BDSG).

Generell sind folgende Grundsätze bei der Einschränkung des Rechts auf informationelle Selbstbestimmung zu beachten:

1. Es darf nur das unbedingt notwendige Maß an Daten erhoben und verarbeitet werden.
2. Die Daten dürfen nur für den Zweck verwendet werden, für den sie auch erhoben oder erfasst wurden.
3. Bei der Erhebung und dem Umgang mit Daten ist auf die Rechte der Betroffenen ausreichend Rücksicht zu nehmen, z. B. durch Kontroll-, Auskunfts- und Mitwirkungsrechte.

Wo finden sich gesetzliche Regelungen zum Datenschutz?

Datenschutzrechtliche Regelungen finden sich nicht nur in bundesdeutschen Gesetzen oder Gesetzen der Bundesländer, sondern auch in europarechtlichen Rechtsakten sowie internationalen Verträgen. Vor allem aufgrund der fortschreitenden Globalisierung und des ungehinderten Datenaustausches mittels des Internets sind weitreichendere Regulierungen von Nöten.

Datenschutzrechtliche Vorgaben auf europäischer Ebene[2]

Für die Organe und Behörden der Europäischen Union (EU) ist v. a. die Charta der Grundrechte der Europäischen Union[3] zu beachten, welche durch den Vertrag von Lissabon rechtsverbindlich wurde und damit für alle Mitgliedsstaaten gilt. Diese enthält in Art. 8 ein explizites Datenschutzgrundrecht, welches – ähnlich den vom Bundesverfassungsgericht entwickelten Grundsätzen – den Schutz personenbezogener Daten regelt. Erwähnenswert sind darüber hinaus noch die Allgemeine Datenschutzrichtlinien 95/46/EG[4] und die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG[5].

1 Urteil des Bundesverfassungsgerichts vom 15.12.1993, Az. 1 BvR 209/83.

2 Zur Datenschutzgrundverordnung s. Übersicht *Aktuelle Entwicklungen im Datenschutzrecht.*

3 2000/C 364/01, Amtsblatt der Europäischen Union vom 18.12.2000.

4 RL 95/46/EG, Amtsblatt der Europäischen Union 1995, L 281, Seite 31.

5 RL 2002/58/EG, Amtsblatt der Europäischen Union 2002, L 201, Seite 37.

Die europarechtlichen Vorschriften unterscheiden meist nicht zwischen Datenerhebung und -verarbeitung im privaten und öffentlichen Bereich. Sofern es also keine ausdrücklichen Bereichsausnahmen gibt (z. B. für die Landesverteidigung), gelten die Bestimmungen gleichermaßen. Aufgrund der umfassenden Regelungen im deutschen Recht sind die europarechtlichen Bestimmungen für die tägliche Praxis aber von geringer Bedeutung. Nur in Einzelfällen (z. B. grenzüberschreitende Sachverhalte) können die Richtlinien Bedeutung haben.

Übersicht: Systematik des deutschen Datenschutzrechts

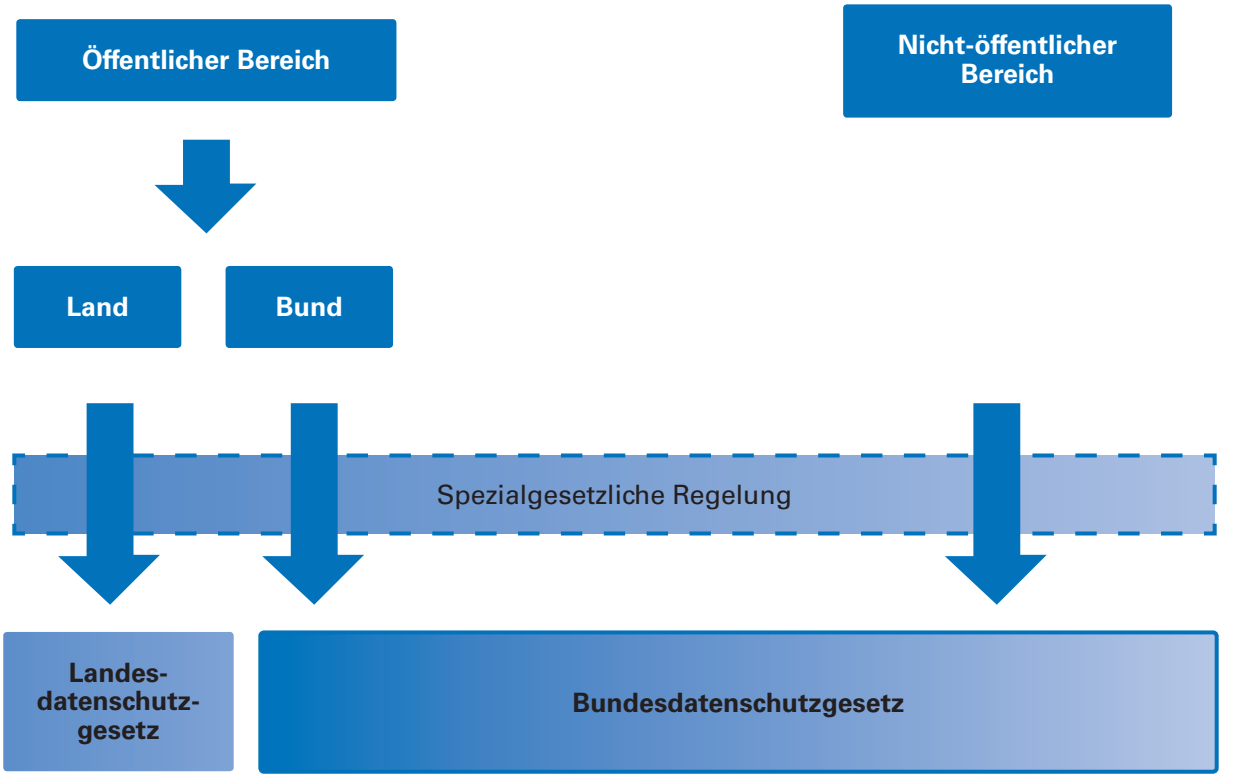

Abb. 1: Systematik des deutschen Datenschutzrechts (Quelle: M. Schumann)

Aus dieser Systematik ergibt sich folgende Prüfungsreihenfolge:

- Wer trägt für die zu prüfende Maßnahme die Verantwortung: Eine Stelle aus dem öffentlichen Bereich oder aus dem nicht-öffentlichen Bereich?
- Wenn es eine Stelle aus dem öffentlichen Bereich ist: Handelt es sich um eine öffentliche Stelle des Bundes oder eines Bundeslandes?
- Gibt es für die zu prüfende Maßnahme eine spezialgesetzliche Regelung, z. B. das Telemediengesetz oder das Telekommunikationsgesetz?

Merke: Spezialgesetzliche Bestimmungen (sog. bereichsspezifische Regelungen) gehen dem BDSG und den Landesdatenschutzgesetzen i. d. R. vor (vgl. § 1 Abs. 3 Satz 1 BDSG) – allerdings nur in dem Umfang, in dem das Spezialgesetz auch Regelungen für den konkreten Sachverhalt enthält. So ist die Erhebung von Sozialdaten durch die gesetzlichen Krankenkassen in §§ 67d ff. SGB X geregelt. Ein Rückgriff auf das BDSG ist insoweit ausgeschlossen.

Anwendungsbereich des Bundesdatenschutzgesetzes

Das BDSG ist nach § 1 BDSG anwendbar auf die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch:

- Öffentliche Stellen des Bundes, d. h. vor allem durch Behörden (z. B. Ministerien, Bundesbehörden), Organe der Rechtspflege (z. B. Bundesgerichte) und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes (z. B. Bundesagentur für Arbeit, Deutsche Rentenversicherung, Bundesstiftungen)
- Öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und diese Bundesrecht ausführen
- Nicht-öffentliche Stellen, d. h. natürliche und juristische Personen des Privatrechts, die keine hoheitlichen Aufgaben wahrnehmen

Vom Anwendungsbereich des BDSG und der Landesdatenschutzgesetze ausgenommen ist nach § 1 Abs. 2 Nr. 3 letzter Halbsatz BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ausschließlich zu privaten Zwecken (z. B. Führen eines privaten Adressbuchs; Erarbeitung einer Familienchronik).

Aufbau des Bundesdatenschutzgesetzes

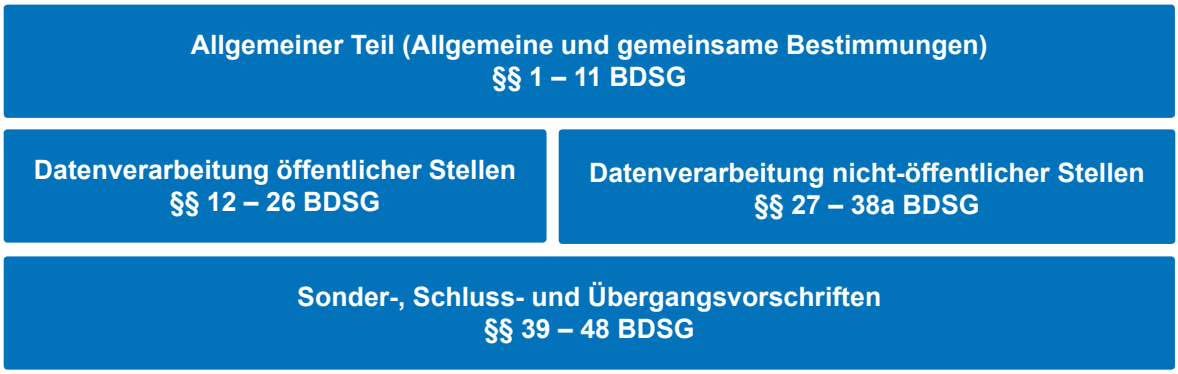

Abb. 2: Aufbau des BDSG (Quelle: M. Schumann)

Wesentliche Begriffsbestimmungen des Bundesdatenschutzgesetzes:

- **Personenbezogene Daten:** Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)
- **Verantwortliche Stelle:** jede Person oder Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt
- **Dritter:** jede Person oder Stelle außerhalb der verantwortlichen Stelle (mit Ausnahme des Betroffenen und des Auftragnehmers) bei der Auftragsdatenverarbeitung i. S. v. § 11 BDSG
- **Erhebung von Daten:** Beschaffen von Daten über den Betroffenen
- **Verarbeitung von Daten:** Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten
- **Nutzung von Daten:** jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt

Beispiele: personenbezogene Daten

Angaben über

Persönliche Verhältnisse

- Name
- Anschrift
- Familienstand
- Bankverbindung
- Fotos
- Beruf
- Gesundheitszustand

Sachliche Verhältnisse

- Angaben über Eigentums- und Besitzverhältnisse
- Vertragliche Beziehungen
- Informationen über Kommunikations- und Nutzungsverhalten

Achtung: Die Art der Darstellung der personenbezogenen Daten ist irrelevant (analog, digital, Texte, Bilder etc.).

Der Umgang mit personenbezogenen Daten nach dem BDSG

Übersicht: Umgang mit personenbezogenen Daten

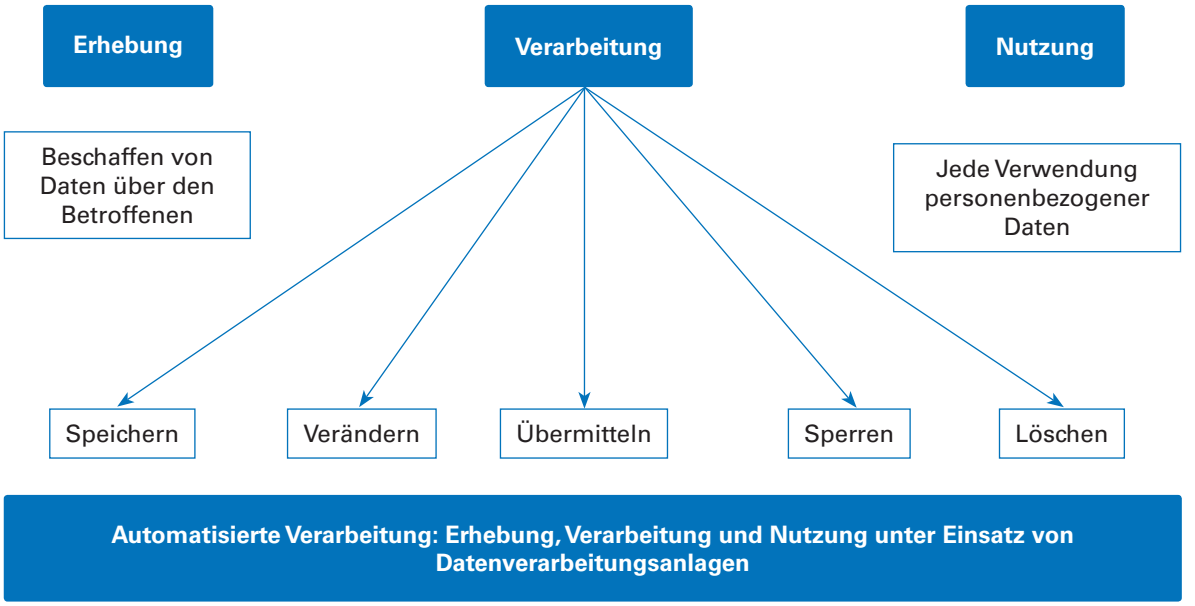

Abb. 3: Übersicht – Umgang mit personenbezogenen Daten (Quelle: M. Schumann)

Überblick: Grundprinzipien des Bundesdatenschutzgesetzes

Prinzip des Verbots mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG)
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist grundsätzlich verboten und nur dann zulässig, wenn und soweit

- ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt bzw. anordnet oder
- der Betroffene einwilligt.

Für den öffentlichen Bereich ergibt sich die Generalklausel zur Erhebung personenbezogener Daten aus § 13 BDSG.

Nach § 13 Abs. 1 BDSG ist die Erhebung personenbezogener Daten durch öffentliche Stellen dann zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Abweichend davon ist die Erhebung besonderer personenbezogener Daten i. S. v. § 3 Abs. 9 BDSG an strengere Voraussetzungen geknüpft (§ 13 Abs. 2 BDSG).

§ 13 BDSG setzt voraus, dass stets die sachlich und örtlich zuständige Behörde die Daten erhebt, da andernfalls die Datenerhebung nicht für die Erfüllung der Aufgaben erforderlich ist. Zudem muss die Aufgabenerfüllung rechtmäßig sein.

Auf die Einwilligung des Betroffenen kommt es also nicht an, wenn eine gesetzliche Regelung den Umgang mit personenbezogenen Daten ausdrücklich erlaubt oder sogar anordnet. In allen anderen Fällen ist die Einwilligung des Betroffenen zwingende Voraussetzung für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten[6].

An eine wirksame Einwilligung werden folgende Anforderungen gestellt (§4a BDSG):
- Die Einwilligung muss freiwillig erfolgen.
- Grundsätzlich bedarf die Einwilligung der Schriftform, sofern nicht wegen der besonderen Umstände eine andere Form angemessen ist.
- Der Betroffene ist über die Tragweite der Einwilligung aufzuklären.

6 Neben der allgemeinen Regelung zur Einwilligung (§ 4 a BDSG) gibt es noch besondere Regelungen, z. B. bei der Einwilligung zu Werbezwecken (§ 28 BDSG).

Grundsatz der Direkterhebung (§ 4 Abs. 2 BDSG)
Personenbezogene Daten sind grundsätzlich beim Betroffenen selbst zu erheben. Damit wird sichergestellt, dass der Betroffene die ihm zustehenden Rechte wahrnehmen kann. Zudem gehen damit umfassende Informations- und Unterrichtungspflichten einher (§ 4 Abs. 3 BDSG). So ist der Betroffene bspw. über die Identität der verantwortlichen Stelle und die Zweckbestimmung zu unterrichten. Wird vom Grundsatz der Direkterhebung abgewichen, bestehen u. U. besondere Hinweispflichten (z. B. § 13 Abs. 1a BDSG).

Nur in wenigen Ausnahmefällen dürfen personenbezogene Daten ohne Mitwirkung des Betroffenen erhoben werden, z. B. wenn eine Rechtsvorschrift dies vorsieht oder sogar zwingend voraussetzt (§ 4 Abs. 2 Satz 2 Nr. 1 BDSG) oder die Direkterhebung nur mit unverhältnismäßig hohem Aufwand möglich wäre (§ 4 Abs. 2 Satz 2 Nr. 2 lit. b BDSG).

Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a BDSG)
Es gilt das übergeordnete Ziel, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen. Soweit es möglich und zweckdienlich ist, sind personenbezogene Daten zu anonymisieren und zu pseudonymisieren.

Zweckbindungsgrundsatz (§ 14 BDSG)
Vor allem für öffentliche Stellen relevant ist die Beachtung der Zweckbindung der Datenerhebung und -verarbeitung. Damit soll verhindert werden, dass Daten quasi auf Vorrat erhoben und gespeichert werden. Öffentliche Stellen dürfen personenbezogene Daten daher grundsätzlich nur speichern, verändern und nutzen, wenn und soweit das für Zwecke erfolgt, für die die Daten erhoben worden sind.

Von diesem Grundsatz gibt es aber zahlreiche, in § 14 Abs. 2 BDSG normierte Ausnahmen, z. B.

- wenn es eine Rechtsvorschrift vorsieht oder zwingend voraussetzt;
- wenn der Betroffene eingewilligt hat;
- zur Gefahrenabwehr und zur Verfolgung von Straftaten und Ordnungswidrigkeiten oder
- zur Durchführung wissenschaftlicher Forschung.

Achtung: Eine strikte Zweckbindung besteht bei Daten, die ausschließlich gespeichert werden dürfen zur Datenschutzkontrolle, zur Datensicherung, zur Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage (§ 14 Abs. 4 BDSG) oder zur wissenschaftlichen Forschung (§ 40 BDSG). Für nicht-öffentliche Stellen gilt der Zweckbindungsgrundsatz generell nur eingeschränkt (§ 28 Abs. 1 Satz 2 und Abs. 2 BDSG).

Besonderer Schutz sensibler Daten (§ 3 Abs. 9 BDSG)

Sensible Daten sind Angaben über

- rassische und ethnische Herkunft (auch Angaben über die Hautfarbe)
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit (auch Angaben über Drogen- und Alkoholmissbrauch)
- Sexualleben

Der besondere Schutz sensibler Daten wird z. B. gewährleistet durch

- das Erfordernis einer ausdrücklichen und bestimmten Einwilligung (§ 4a Abs. 3 BDSG) und
- strenge Voraussetzungen für die Datenerhebung (§ 13 Abs. 2 BDSG), die Datennutzung (§ 14 Abs. 5 BDSG) und Datenübermittlung (§ 16 Abs. 1 Nr. 2 Satz 2 BDSG).

Besondere Vorschriften zur Speicherung, Veränderung, Nutzung und Übermittlung von Daten durch öffentliche Stellen

Neben der Erhebung der Daten spielt die weitere Nutzung eine erhebliche Rolle für die verantwortlichen Stellen. Die Erhebung von personenbezogenen Daten ist in den meisten Fällen kein Selbstzweck, sondern dient der Aufgabenerfüllung und andere gesetzlich vorgesehenen Zwecken. Aus diesem Grunde schließt sich i. d. R. an den Prozess der Datenerhebung ein Prozess der Datenverarbeitung an, der von der bloßen Speicherung der Daten über deren Veränderung und Nutzung bis hin zur Übermittlung der Daten an Dritte reicht. Infolgedessen hat der Gesetzgeber für diese weitreichenden Formen der Datenverarbeitung besondere Zulässigkeitsvoraussetzungen statuiert, die von der jeweils verantwortlichen Stelle einzuhalten sind.

Zulässigkeit der Speicherung, Veränderung und Nutzung von Daten (§ 14 BDSG)
Neben dem Zweckbindungsgrundsatz ergibt sich aus § 14 BDSG auch die generelle Rechtsgrundlage für die Verarbeitung und Verwendung von Daten. Erforderlich ist dabei stets, dass die Speicherung, Veränderung und Nutzung von Daten

- zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und
- für Zwecke erfolgt, für die die Daten erhoben worden sind.

Im Hinblick auf die Erforderlichkeit gelten dieselben Voraussetzungen wie bei der Erhebung der Daten, also insbesondere die Zuständigkeit der verantwortlichen Stelle und die Rechtmäßigkeit der Aufgabenerfüllung.

Zulässigkeit der Übermittlung von Daten (§§ 15 und 16 BDSG)
Bei der Übermittlung von Daten ist danach zu unterscheiden, ob diese an eine öffentliche Stelle (§ 15 BDSG) oder eine nicht-öffentliche Stelle (§ 16 BDSG) übermittelt werden sollen[7].

Datenübermittlung an öffentliche Stellen (§ 15 BDSG)
Die Datenübermittlung an öffentliche Stellen setzt nach § 15 Abs. 1 BDSG voraus, dass

- dies zur Erfüllung der Aufgaben der übermittelnden Stelle oder der Daten empfangenden Stelle erforderlich ist und
- die Voraussetzungen des § 14 BDSG vorliegen (bei Vorliegen einer Zweckänderung muss also ein Ausnahmetatbestand i. S. v. § 14 Abs. 2 BDSG gegeben sein).

Achtung: Die Verantwortlichkeit für die Zulässigkeit der Übermittlung der Daten trägt nach § 15 Abs. 2 Satz 1 BDSG grundsätzlich die übermittelnde Stelle. Sie muss also prüfen, ob sämtliche Voraussetzungen vorliegen und muss dies notfalls gegenüber dem Betroffenen begründen. Zudem haftet sie für etwaige Rechtsverletzungen. Etwas anderes gilt nur, wenn der Dritte, also die Daten empfangende Stelle, um Übermittlung der Daten ersucht hat (Übermittlungsersuchen). Im Rahmen des Übermittlungsersuchens hat der Dritte aber darzulegen, warum er die Daten für seine Aufgabenerfüllung benötigt.

Die Daten empfangende Stelle muss ihrerseits wieder den Zweckbindungsgrundsatz beachten, darf also die Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung die Daten übermittelt wurden (§ 15 Abs. 3 BDSG). Freilich gelten auch hier wieder die in § 14 Abs. 2 BDSG normierten Ausnahmetatbestände.

Für die praktisch relevante interne Datenweitergabe enthält § 15 Abs. 6 BDSG eine Sonderregelung. Die Übermittlung von Daten innerhalb einer öffentlichen Stelle ist immer dann zulässig, wenn nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen.

Datenübermittlung an nicht-öffentliche Stellen (§ 16 BDSG)
Die Datenübermittlung an nicht-öffentliche Stellen ist nur zulässig, wenn

- dies zur Aufgabenerfüllung der übermittelnden Stelle erforderlich ist und die Voraussetzungen der Nutzung der Daten nach § 14 BDSG vorliegen oder
- der Empfänger der Daten ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und kein schutzwürdiges Interesse des Betroffenen entgegensteht.

Achtung: Die Verantwortlichkeit für die Zulässigkeit der Übermittlung der Daten trägt nach § 16 Abs. 2 BDSG immer die übermittelnde Stelle. Sie muss zudem in den Fällen des § 16 Abs. 1 Nr. 2 BDSG den Betroffenen von der Übermittlung der Daten in Kenntnis setzen. Das gilt allerdings nicht, wenn der Betroffene bereits anderweitig davon Kenntnis erlangt hat oder Sicherheitsinteressen entgegenstehen (§ 16 Abs. 3 BDSG).

Datenübermittlung ins Ausland (§§ 4b und 4c BDSG)
Bei der Datenübermittlung ins Ausland ist zu unterscheiden zwischen der Datenübermittlung an Mitgliedsstaaten oder Institutionen der Europäischen Union und des Europäischen Wirtschaftsraums (EWR) einerseits und an sonstige Staaten andererseits.

Im ersten Fall sind nach § 4b Abs. 1 BDSG im Wesentlichen die Bestimmungen zur inländischen Datenübermittlung anzuwenden, also insbesondere §§ 15 und 16 BDSG. Voraussetzung ist jedoch, dass die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

7 Daneben kann sich die Zulässigkeit der Datenübermittlung noch aus bereichsspezifischen Vorschriften oder aus der Einwilligung des Betroffenen ergeben.

Liegen die Voraussetzungen des § 4b Abs. 1 BDSG nicht vor, also insbesondere bei einer Übermittlung von Daten an sonstige Staaten und ausländische Institutionen, hängt die Zulässigkeit der Übermittlung v. a. davon ab, ob in dem Empfängerstaat ein angemessenes Datenschutzniveau gewährleistet ist (§ 4b Abs. 2 Satz 2 BDSG). Die Feststellung des Datenschutzniveaus erfolgt dabei entweder durch die verantwortliche Stelle nach § 4b Abs. 3 BDSG oder durch die Europäische Union nach Art. 25 Abs. 6 der RL 95/46/EG. Abweichend davon lässt die Ausnahmeregelung des § 4c BDSG in den dort bestimmten Fällen auch eine Übermittlung von Daten an ausländische Stellen zu, selbst wenn dort ein angemessenes Datenschutzniveau nicht gewährleistet ist (z. B. bei einer Einwilligung des Betroffenen).

Auftragsdatenverarbeitung (§ 11 BDSG)
Auch in der öffentlichen Verwaltung werden zunehmend Aufgaben der Datenverarbeitung und EDV (z. B. Betrieb eines Rechenzentrums, elektronische Aktenbearbeitung) im Rahmen eines sog. Outsourcings an Drittanbieter vergeben. Das sind zumeist Unternehmen der Privatwirtschaft, mitunter aber auch kommunale Unternehmen oder Zweckverbände. § 11 BDSG regelt hierzu vereinfacht, dass der Auftraggeber für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich ist und auch bleibt. Der Auftragnehmer ist insoweit nicht Dritter i. S. d. BDSG, sodass beim Datenaustausch zwischen Auftragnehmer und Auftraggeber datenschutzrechtlich keine Datenübermittlung stattfindet.

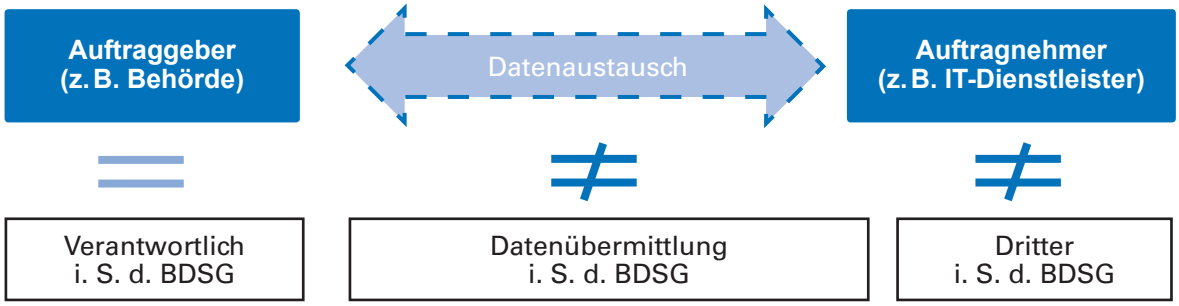

Abb. 4: Schema Auftragsdatenverarbeitung (Quelle: M. Schumann)

Voraussetzungen einer wirksamen Auftragsdatenverarbeitung:

- schriftlicher Auftrag zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten mit dem in § 11 Abs. 2 Satz 2 BDSG enthaltenen Mindestinhalten der Auftragserteilung
- Vorgabe der technischen und organisatorischen Maßnahmen i. S. v. § 9 BDSG
- regelmäßige Prüfung der Einhaltung der vorgegebenen technischen und organisatorischen Maßnahmen einschließlich einer nachvollziehbaren Dokumentation des Prüfungsergebnisses (die Prüfung ist vor Beginn der Datenverarbeitung und sodann regelmäßig durchzuführen)
- ausschließliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen der Weisungen des Auftraggebers

Praktische Schwierigkeiten kann die regelmäßige Prüfung der Einhaltung der vorgegebenen Maßnahmen hervorrufen. Wenngleich eine „Vor-Ort-Kontrolle“ wünschenswert ist, kann die Prüfung auch an Dritte (Wirtschaftsprüfer, unabhängige Sachverständige etc.) delegiert werden.

Eine Auftragsdatenverarbeitung liegt nicht vor, wenn dem Auftragnehmer im Rahmen seiner Aufgaben eine Eigenverantwortlichkeit und Entscheidungsbefugnis zukommt, er also keine reine Hilfsfunktion ausübt. In diesem Fall ist der Auftragnehmer selbst verantwortliche Stelle.

Meldepflichten und Vorabkontrolle (§§ 4d bis 4g BDSG)
Aufgrund der besonderen Risiken bei der automatisierten Datenverarbeitung sind solche Verfahren vor ihrer Inbetriebnahme den zuständigen Datenschutzbehörden zu melden (§ 4d Abs. 1 BDSG). Der Inhalt der Meldepflicht ergibt sich dabei aus § 4e BDSG.

Gehen von der automatisierten Datenverarbeitung besondere Risiken für die Rechte und die Freiheiten des Betroffenen aus, unterliegen die entsprechenden Verfahren einer sog. Vorabkontrolle nach § 4d Abs. 5 BDSG. Das ist insbesondere dann der Fall, wenn sensible Daten i. S. v. § 3 Abs. 9 BDSG verarbeitet werden sollen.

Ist eine Vorabkontrolle vorgeschrieben, dann ist deren Durchführung eine Zulässigkeitsvoraussetzung für die Datenverarbeitung. Wurde die Vorabkontrolle unterlassen, ist die Datenverarbeitung rechtswidrig.

Rechte des Betroffenen

Für die Datenverarbeitung von öffentlichen Stellen enthalten die §§ 19 ff. BDSG zahlreiche Vorschriften, die die Rechte des Betroffenen regeln. Aber auch an anderen Stellen finden sich Rechte, die ein Betroffener gegenüber einer öffentlichen Stelle geltend machen kann. Die gesetzlich normierten Rechte des Betroffenen sind zwingend erforderlich, um sein Recht auf informationelle Selbstbestimmung auch effektiv wahrnehmen und notfalls durchsetzen zu können. Aus diesem Grunde bestimmt auch § 6 BDSG, dass die Rechte des Betroffenen auf Auskunft, Berichtigung, Löschung und Sperrung nicht durch Rechtsgeschäft zum Nachteil des Betroffenen verändert werden dürfen.

Die wesentlichsten Rechte sind:

Benachrichtigung (§ 19a BDSG)	**Auskunftsrecht** (§ 19 BDSG)	**Korrekturpflicht** (§ 20 BDSG)	**Anrufungsrecht** (§ 21 BDSG)

Benachrichtigung (§ 19a BDSG)
Nach § 19a BDSG ist der Betroffene umfassend zu informieren, wenn Daten ohne seine Kenntnis erhoben werden. Die Information hat spätestens mit der ersten Übermittlung der Daten zu erfolgen, sofern eine solche vorgesehen ist (§ 19a Abs. 1 Satz 3 BDSG).

Der Betroffene ist dabei zu unterrichten über:

- die Speicherung seiner Daten,
- die Art der Daten,
- die Identität der verantwortlichen Stelle (mit Name und Anschrift) und
- die Zweckbestimmung der Datenverarbeitung[8].

Eine bestimmte Form der Information ist dabei gesetzlich nicht vorgeschrieben. Gleichwohl ist eine Kenntnisnahme durch den Betroffenen sicherzustellen.

Die Benachrichtigungspflicht besteht nach § 19a Abs. 2 Satz 1 BDSG nicht, wenn

- der Betroffene bereits auf andere Weise Kenntnis von der Speicherung und Übermittlung erhalten hat,
- die Unterrichtung des Betroffenen einen unverhältnismäßig hohen Aufwand erfordert oder
- wenn die Speicherung oder Übermittlung der Daten gesetzlich vorgesehen ist.

Aufgrund dieser Ausnahmeregelungen sowie der entsprechenden Anwendung der Ausnahmeregelungen des § 19 Abs. 2 – 4 BDSG (vgl. § 19a Abs. 3 BDGS) hat die Benachrichtigungspflicht im öffentlichen Bereich nur geringe praktische Bedeutung.

Auskunftsrecht (§ 19 BDSG)
Eine hohe praktische Bedeutung hat hingegen das Auskunftsrecht, obgleich dieses durch eine Reihe bereichsspezifischer Ausnahmen und Sonderregelungen eingeschränkt oder gänzlich aufgehoben wird[9]. Das Auskunftsrecht setzt stets einen entsprechenden Antrag des Betroffenen voraus, der auch formlos möglich ist. Allerdings soll der Betroffene zumindest die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen (§ 19 Abs. 1 Satz 2 BDSG).

Sind die Daten nur „in Akten verfügbar", d. h. weder in automatisierten noch in nicht automatisierten Dateien gespeichert, dann muss der Betroffene auch Angaben machen, die das Auffinden der Daten ermöglichen (z. B. Angabe Aktenzeichen etc.). Zudem darf der Arbeitsaufwand nicht außer Verhältnis zum Informationsinteresse des Betroffenen stehen.

Liegt ein Antrag vor, ist dem Betroffenen Auskunft zu erteilen über

- die zu seiner Person gespeicherten Daten,
- die Empfänger, an die die Daten weitergegeben werden, und
- den Zweck der Speicherung.

Die konkrete Form der Auskunftserteilung bestimmt die verantwortliche Stelle (§ 19 Abs. 1 Satz 4 BDSG). Die Auskunft ist nach § 19 Abs. 7 BDSG stets unentgeltlich.

8 Darüber hinaus ist in bestimmten Fällen auch über die Empfänger der Daten zu unterrichten (§ 19a Abs. 1 Satz 2 BDSG).

9 z. B. § 15 BVerSchG, § 7 BNDG, § 9 MADG, § 23 SÜG, §§ 90 ff. BBG, § 83 SGB X.

In einer Reihe von Fällen[10], darf die öffentliche Stelle die Auskunft verweigern, z. B. dann, wenn

- die Daten nur aufgrund von Aufbewahrungsvorschriften nicht gelöscht werden dürfen und die Auskunftserteilung einen unverhältnismäßig hohen Aufwand verursacht;
- die ordnungsgemäße Erfüllung der Aufgaben der verantwortlichen Stelle durch die Auskunftserteilung gefährdet ist;
- die öffentliche Sicherheit und Ordnung durch die Auskunft gefährdet ist oder
- eine Geheimhaltungspflicht aufgrund einer Rechtsvorschrift besteht.

Sind Behörden des Sicherheitsbereichs betroffen (Bundesverfassungsschutz u. a.), ist die Auskunftserteilung von deren Zustimmung abhängig (§ 19 Abs. 3 BDSG).

Soll das Auskunftsersuchen abgelehnt werden, ist das zu begründen. Etwas anderes gilt nur, wenn durch eine Begründung der mit der Ablehnung verfolgte Zweck vereitelt werden würde. Der Betroffene ist dann aber darauf hinzuweisen, dass er sich an die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wenden kann (§ 19 Abs. 5 BDSG).

Korrekturpflicht/-anspruch (§ 20 BDSG)
§ 20 BDSG regelt die Pflicht der verantwortlichen Stelle, personenbezogene Daten unter den dort genannten Voraussetzungen

- zu berichtigen (§ 20 Abs. 1 BDSG),
- zu löschen (§ 20 Abs. 2 BDSG) und
- zu sperren (§ 20 Abs. 3 BDSG).

Berichtigung unrichtiger Daten
So ist die verantwortliche Stelle nach § 20 Abs. 1 BDSG verpflichtet, unrichtige Daten von Amts wegen zu berichtigen. Eines Antrages des Betroffenen bedarf es daher nicht. Unrichtig sind die Daten u. a. dann, wenn sie unvollständig (fehlende Angabe des Familienstandes) oder tatsächlich falsch (z. B. falsches Geburtsdatum) sind.

Löschung von Daten
Ebenfalls von Amts wegen sind nach § 20 Abs. 2 BDSG Daten zu löschen, wenn deren Speicherung unzulässig ist oder ihre Kenntnis von der verantwortlichen Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Die Löschung erfolgt durch Unkenntlichmachung der Daten (§ 3 Abs. 4 Satz 1 Nr. 5 BDSG). Sie betrifft allerdings nur automatisiert verarbeitete Daten und in nicht automatisierten Dateien gespeicherte Daten, also nicht klassische Akten.

Eine besondere Löschungspflicht besteht nach § 6b Abs. 5 BDSG im Falle von Daten, die im Rahmen einer Videoüberwachung öffentlich zugänglicher Räume erfasst wurden. Solche Daten sind zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen des Betroffenen einer weiteren Speicherung entgegenstehen.

Sperrung von Daten
In bestimmten Fällen tritt anstelle der Löschung von Daten die Sperrung derselben, z. B. wenn und soweit der Löschung bestimmte Aufbewahrungspflichten entgegenstehen[11] (§ 20 Abs. 3 Nr. 1 BDSG), schutzwürdige Interessen des Betroffenen beeinträchtigt werden könnten[12] (§ 20 Abs. 3 Nr. 2 BDSG) oder eine Löschung unverhältnismäßig hohen Aufwand verursachen würde (§ 20 Abs. 3 Nr. 3 BDSG). Die Sperrung der Daten erfolgt durch das Kennzeichnen derselben, um eine weitere Verarbeitung oder Nutzung einzuschränken (§ 3 Abs. 4 Nr. 4 BDSG).

Automatisiert verarbeitete oder in nicht automatisierten Dateien gespeicherte Daten sind weiterhin dann zu sperren, wenn der Betroffene die Richtigkeit der Daten bestreitet und sich nicht feststellen lässt, ob die Daten nun richtig oder falsch sind (§ 20 Abs. 4 BDSG).

Für die klassischen Akten besteht hingegen eine Pflicht zur Sperrung nach § 20 Abs. 6 BDSG dann, wenn schutzwürdige Interessen des Betroffenen beeinträchtigt werden und die Daten für die Aufgabenerfüllung der verantwortlichen Stelle nicht mehr erforderlich sind.

Anrufungsrecht (§ 21 BDSG)

Jedermann kann nach § 21 BDSG den Bundesbeauftragten für Datenschutz und Informationsfreiheit anrufen. Dieser geht den Beschwerden nach und unterrichtet den Betroffenen über das Ergebnis. Die Angaben des Betroffenen werden dabei vertraulich behandelt.

10 Vgl. § 19 Abs. 2 und 4 BDSG.

11 z. B. handels- und steuerrechtliche Aufbewahrungspflichten, aber auch kommunal- oder haushaltsrechtliche Aufbewahrungspflichten.

12 z. B. die Vernichtung von Beweismitteln

Widerspruchsrecht (§ 20 Abs. 5 BDSG)

Der Betroffene kann nach § 20 Abs. 5 BDSG auch einer an sich rechtmäßigen (automatisierten) Datenverarbeitung widersprechen, wenn

- besondere Umstände in der Person des Betroffenen vorliegen,
- diese im Rahmen einer Abwägung dem Interesse der verantwortlichen Stelle an der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten überwiegen und
- die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten nicht durch eine Rechtsvorschrift vorgeschrieben ist.

Exkurs: Anspruch auf Schadensersatz (§§ 7 und 8 BDSG)

Wird dem Betroffenen durch eine unzulässige oder unrichtige Datenverarbeitung ein Schaden zugefügt, hat dieser einen Anspruch auf Schadensersatz nach § 7 BDSG. Die verantwortliche Stelle kann sich von einer Haftung befreien, wenn sie die gebotene Sorgfalt beachtet hat.

Bei einer unzulässigen oder unrichtigen automatisierten Datenverarbeitung besteht nach § 8 Abs. 1 BDSG der Schadensersatzanspruch unabhängig vom Verschulden der verantwortlichen Stelle. Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen auch ein Schmerzensgeld zu zahlen (§ 8 Abs. 2 BDSG). Allerdings sieht das Gesetz eine generelle Haftungsbeschränkung auf 130.000 Euro vor (§ 8 Abs. 3 BDSG).

Unser Wissen
für Ihren Erfolg

Bestellmöglichkeiten

Die neue Datenschutz- und IT-Sicherheitsmappe

Für weitere Produktinformationen oder zum Bestellen hilft Ihnen unser Kundenservice gerne weiter:

Kundenservice

Telefon: 08233 / 381-123

E-Mail: service@forum-verlag.com

Oder nutzen Sie bequem die Informations- und Bestellmöglichkeiten zu diesem Produkt in unserem Online-Shop:

Internet

http://www.forum-verlag.com/details/index/id/8903

FORUM VERLAG HERKERT GMBH, Mandichostraße 18, 86504 Merching,
Tel.: (08233) 381 123, E-Mail: service@forum-verlag.com, Internet: www.forum-verlag.com