Wichtige Informationen für Entscheidungsträger zum Datenschutz nach BDSG und zum Datenschutzbeauftragten

Als Beratungsunternehmen für Datenschutz möchten wir Ihnen einige grundlegende und für Sie als verantwortliche Unternehmensleitung wichtige Informationen zu den Aufgaben und Anforderungen zum Datenschutz nach Bundesdatenschutzgesetz an die Hand geben. Die Informationen stellen eine allgemeine (nicht vollständige) Zusammenfassung dar.

Sandro Swoboda
Projektleiter Datenschutz

Anschrift:

HCONSULT GmbH Unternehmensberatung

Abt. Datenschutz
Bahnhofsplatz 15
07545 Gera

Tel. 0365 8336 9905
Fax. 0365 4328 1516
Mobil 0152 5716 8452

Mail s.swoboda@hconsult.info
Web datenschutz.hconsult.info

Inhalt

Aufgaben des DSB 5
Personenbezogene Daten 5
Bestimmt ist eine Person,..... 5
Bestimmbar ist eine Person, ... 5
Beispiele für personenbezogene Daten 5
Technische und organisatorische Maßnahmen 6
Abgrenzung technisch und organisatorisch 6
TOM gemäß Anlage zu § 9 BDSG..... 6
Zutrittskontrolle 6
Zugangskontrolle..... 7
Zugriffskontrolle 7
Weitergabekontrolle 7
Eingabekontrolle 8
Auftragskontrolle..... 8
Verfügbarkeitskontrolle 8
Trennungsgebot 8
Prinzip der Verhältnismäßigkeit 9
Das Verfahrensverzeichnis 9
Internes Verfahrensverzeichnis..... 9
Mindestanforderung an den Inhalt 10
Verfahrensverzeichnisse und Meldepflichten..... 10
Meldepflichtige Stellen..... 11
Eine Meldepflicht für nicht-öffentliche Stellen besteht, wenn..... 11
Nicht meldepflichtige Stellen 12
Vorabkontrolle 12
Einschalten der Aufsichtsbehörde..... 13

Warum Datenschutz/Persönlichkeitsschutz in der Privatwirtschaft?

Das "Recht auf informationelle Selbstbestimmung" als Bestandteil des allgemeinen Persönlichkeitsrechts nach dem Grundgesetz soll es dem Einzelnen ermöglichen, sich seine Privatsphäre möglichst in dem von ihm gewünschten Umfang zu erhalten.

Viele Menschen fürchten als Kunden, Arbeitnehmer, Patienten, usw. Datenschutzpannen sowie übermäßige Überwachung, Ausforschung und die Zusammenführung verschiedener Daten zu Persönlichkeitsprofilen (Schlagworte: "gläserner Kunde/Mitarbeiter", "Data-Warehouse", "Data-Mining"). Moderne Techniken und Vermarktungsformen sowie moderner Informationsverkehr werden auf Dauer nur akzeptiert, wenn Datenschutz/Persönlichkeitsschutz in ausreichender Weise gewährleistet erscheint.

Welche gesetzlichen Datenschutzregelungen gelten für die Privatwirtschaft?

Für die Privatwirtschaft gelten

• die Abschnitte 1, 3, 4, 5 und 6 des Bundesdatenschutzgesetzes (BDSG), soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen bzw. im Zusammenhang mit manuellen Dateien erhoben, verarbeitet oder genutzt werden (bei Beschäftigtendaten gilt das BDSG auch für sonstige Unterlagen) sowie

• spezielle Datenschutz-Vorschriften für bestimmte Sachverhalte, wie z. B. Betriebsverfassungsgesetz für Personaldaten, Telemedienrecht beim Interneteinsatz, usw.

Wer ist zuständig und verantwortlich für die Einhaltung des Datenschutzes in Unternehmen?

Verantwortlich für den Datenschutz in Unternehmen ist in erster Linie die Unternehmensleitung.

Was fordert das Bundesdatenschutzgesetz (BDSG) von den Unternehmen?

Das Bundesdatenschutzgesetz fordert von den Unternehmen folgendes:

- Gesetzeskonformer Umgang mit personenbezogenen Daten (§ 4 BDSG, §§ 28 bis 32 BDSG, usw.), z. B. Verwendung der Daten nur im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Kunden oder dem Mitarbeiter, Einwilligung des Betroffenen für weitergehende Datenverarbeitungszwecke, Berücksichtigung des Grundsatzes der Datenvermeidung und Datensparsamkeit nach § 3a BDSG.
- Transparenz der Verarbeitung von personenbezogenen Daten für die davon Betroffenen, z. B. durch Information bei der Datenerhebung nach § 4 Abs. 3 BDSG, bei automatisierten Einzelentscheidungen nach § 6a BDSG oder bei der werblichen Verwendung von Daten nach § 28 Abs. 3 BDSG, durch Benachrichtigungen gemäß § 33 BDSG, durch Auskünfte nach § 34 BDSG, durch Hinweise auf Videoüberwachung nach § 6b Abs. 2 BDSG.

- Information der Datenschutzaufsichtsbehörde und der Betroffenen bei unrechtmäßiger Übermittlung oder sonstiger unrechtmäßiger Kenntniserlangung von personenbezogenen Daten, wenn die Voraussetzungen von § 42a BDSG vorliegen.
- Berücksichtigung von Widerspruchsrechten der Betroffenen (z. B. gegen die Nutzung der Adresse für Werbezwecke, § 28 Abs. 4 BDSG).
- Soweit veranlasst: Berichtigung, Sperrung und Löschung personenbezogener Daten (§ 35 BDSG).
- Ausreichende Sicherheitsmaßnahmen zur Gewährleistung des Datenschutzes (§ 9 BDSG mit Anlage dazu).
- Verpflichtung der bei der Datenverarbeitung beschäftigten Mitarbeiter auf das Datengeheimnis (§ 5 BDSG).
- Firmeninformation zum Datenschutz
- Bayerisches Landesamt für Datenschutzaufsicht 4
- Besondere Vorkehrungen bei automatisierten Abrufverfahren/Online-Anschlüssen (§ 10 BDSG) und bei der Vergabe von Aufträgen an Datenverarbeitungs-Dienstleistungsunternehmen (§ 11 BDSG, schriftliche Regelung des Auftragsverhältnisses, Kontrollen des Auftraggebers beim Auftragnehmer).
- Bestellung eines betrieblichen Beauftragten für den Datenschutz, soweit notwendig (§§ 4f und 4g BDSG), siehe oben.
- Erstellung eines Verfahrensverzeichnisses gemäß § 4g Abs. 2 und Abs. 2a BDSG.

Der Datenschutzbeauftragte

in einem privaten Betrieb wirkt auf die Einhaltung der Datenschutzbestimmungen hin (hat jedoch kein Weisungsrecht). Dabei soll er insbesondere die ordnungsgemäße Anwendung der Computer und Computerprogramme überwachen. Ein wesentliches Augenmerk liegt dabei darauf, dass ausschließlich Befugte eine nur auf den Zweck beschränkte Verarbeitung vornehmen können und dass der Eigentümer der Daten sein Selbstbestimmungsrecht auf Auskunft, Korrektur, Sperrung und Löschung wahrnehmen kann. Außerdem obliegt ihm die Schulung der Mitarbeiter, um sie für die Belange des Datenschutzes zu sensibilisieren.

Der Datenschutzbeauftragte ist in seinem Gebiet weisungsfrei und unabhängig von Vorgesetzten. Er darf wegen Erfüllung seiner Aufgaben nicht benachteiligt werden.

Zum Datenschutzbeauftragten darf nur bestellt werden, wer die notwendige Fachkunde und Zuverlässigkeit besitzt. Die verantwortliche Stelle ist ausdrücklich verpflichtet (§ 4f Abs. 3 Satz 7 BDSG), dem betrieblichen Datenschutzbeauftragten für die Erhaltung seiner Fachkunde die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Die erforderliche Zuverlässigkeit erfordert, dass kein Interessenkonflikt bei der Wahrnehmung der Funktion besteht. Ein solcher besteht vor allem bei allen Personen, die ein eigenes Interesse am Unternehmen (etwa wegen Beteiligung an seinem Vermögen wie z. B. Teilhaber oder Gesellschafter) oder Leitungsfunktion haben. Geschäftsführer oder der Abteilungsleiter, vor allem der Personal- oder der IT-Abteilung, scheiden deshalb regelmäßig aus.

Aufgaben des DSB

In den Aufgaben des Beauftragten für den Datenschutz ist in § 4g Abs. 2 BDSG die Verpflichtung zur Erstellung des Verfahrensverzeichnisses festgelegt. Die grundlegenden Inhalte (z.B. Einzelangaben der Verfahren, zugriffsberechtigte Personen) für diese Erstellung des sogenannten "internen Verfahrensverzeichnisses" sind von der verantwortlichen Stelle beizusteuern.

Personenbezogene Daten

Artikel 2 Ziffer a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr lautet:

Im Sinne dieser Richtlinie bezeichnet der Ausdruck "personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kenn-Nummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Die Umsetzung in nationales Recht erfolgt über § 3 Abs. 1 BDSG, wonach personenbezogene Daten alle Angaben über die persönlichen oder sachlichen Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person sind.

Als natürliche Person ist jeder Mensch zu verstehen. Das Gegenteil bilden juristische Personen. Unter juristischen Personen sind rechtliche Subjekte zu verstehen, die keine Menschen sind, wie etwa Aktiengesellschaften, GmbHs, Einzelunternehmen u.ä.

Bestimmt ist eine Person,

wenn aus den Angaben auf einen einzelnen Menschen geschlossen werden kann. Dies ist meist bei Angaben der Fall, bei welchen der Name des Betroffenen konkret mit genannt ist.

Bestimmbar ist eine Person,

wenn über zusätzliche Angaben ein Bezug zur Person herstellbar ist. Etwa bei Kontonummern, Personalausweisnummer oder KFZ-Kennzeichen. Zu diesen Angaben existieren Verzeichnisse die auf die konkrete Person schließen lassen. Strittig ist inwieweit man von Bestimmbarkeit spricht wenn kein Zugang zu den Verzeichnissen besteht welche die Bestimmbarkeit ermöglichen.

Beispiele für personenbezogene Daten

- Klaus Meier hat blaue Augen.
- Erika Mustermann besitzt einen VW Golf.
- Der erste Kanzler der Bundesrepublik Deutschland war gebürtiger Kölner.

Im ersten Beispiel wird die Angabe hat blaue Augen der Person Klaus Meier zugeordnet. Die Angabe "hat blaue Augen" wird dadurch zu einem personenbezogenen Datum. (Im Regelfall wird die Gesamtinformation "Klaus Meier hat blaue Augen" als personenbezogenes Datum angesehen.)

Im zweiten Beispiel ist "besitzt einen VW Golf" das personenbezogene Datum. Ein personenbezogenes Datum muss nicht zwangsläufig ein körperliches Merkmal der Person sein. Es genügt ein Bezug zwischen der Person und einer Sache, einer anderen Person, einem Ereignis, einem Sachverhalt.

Im dritten Beispiel ist die Person, auf die sich die Angabe gebürtiger Kölner bezieht, zwar nicht namentlich genannt. Sie ist jedoch bestimmbar, da allgemein bekannt ist (oder leicht herausgefunden werden kann), dass Konrad Adenauer der erste Kanzler der Bundesrepublik Deutschland war.

Technische und organisatorische Maßnahmen

Gemäß § 9 Bundesdatenschutzgesetz (BDSG) sind alle Stellen, welche personenbezogene Daten verarbeiten, erheben oder nutzen verpflichtet, technische und/oder organisatorische Maßnahmen (kurz: TOM) zu treffen um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind. Die Spezifizierung dieser Anforderungen ergibt sich aus der Anlage (zu § 9 Satz 1) BDSG.

Abgrenzung technisch und organisatorisch

Unter technischen Maßnahmen sind alle Schutzversuche zu verstehen, die im weitesten Sinne physisch umsetzbar sind, wie etwa

- Umzäunung des Geländes
- Sicherung von Türen und Fenstern
- bauliche Maßnahmen allgemein
- Alarmanlagen jeglicher Art

oder Maßnahmen die in Soft- und Hardware umgesetzt werden, wie etwa

- Benutzerkonto
- Passworterzwingung
- Logging (Protokolldateien)
- biometrische Benutzeridentifikation

Als organisatorische Maßnahmen sind solche Schutzversuche zu verstehen die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden. Beispiele hierfür sind

- Besucheranmeldung
- Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
- Vier-Augen-Prinzip
- festgelegte Intervalle zur Stichprobenprüfungen

TOM gemäß Anlage zu § 9 BDSG

Die Anlage zu gibt vor, in welchen Kategorien Schutzmaßnahmen sichergestellt sein müssen. Nachfolgend werden die einzelnen Anforderungen nebst Beispielen beschrieben.

Zutrittskontrolle

Gemeint sind Maßnahmen um zu verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden.

- Gebäudesicherung

    - Zäune
    - Pforte
    - Videoüberwachung
- Sicherung der Räume
    - Sicherheitsschlösser
    - Chipkartenleser
    - Codeschlösser
    - Sicherheitsverglasung
    - Alarmanlagen

Zugangskontrolle

Gemeint sind Maßnahmen um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können, wobei allerdings das Wort "nutzen" sich nicht auf die Legaldefinition des § 3 Abs. 5 BDSG beschränkt.

- Zugang zu Rechnern/Systemen (Authentifizierung)
- Benutzerkennung mit Passwort
- biometrische Benutzeridentifikation
- Firewall
- zertifikatsbasierte Zugangsberechtigung

Zugriffskontrolle

Es muss gewährleistet werden, dass die zur Benutzung von DV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können für welche sie berechtigt sind und das personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

- Berechtigungskonzept
- Benutzerkennung mit Passwort
- gesicherte Schnittstellen (USB, Firewire, Netzwerk, etc.)
- Datenträgerverwaltung
- zertifikatsbasierte Zugriffsberechtigung

Weitergabekontrolle

Es muss verhindert werden, dass personenbezogenen Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.

Sicherung bei der elektronischen Übertragung

- Verschlüsselung
    - VPN
    - Firewall
    - Fax-Protokoll
- Sicherung beim Transport
    - Verschlossene Behälter

    - Verschlüsselung
- Sicherung bei der Übermittlung
    - Verfahrensverzeichnis
    - Protokollierungsmaßnahmen

Eingabekontrolle

Es muss sichergestellt werden, dass nachträglich überprüft werden kann ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

- Protokollierung
- Benutzeridentifikation

Auftragskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden.

- Weisungsbefugnisse festlegen
- Vor-Ort Kontrollen
- Datenschutzvertrag gemäß den Vorgaben nach § 11 BDSG
- Stichprobenprüfung
- Kontrollrechte

Verfügbarkeitskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

- Brandschutzmaßnahmen
- Überspannungsschutz
- Unterbrechungsfreie Stromversorgung
- Klimaanlage
- RAID (Festplattenspiegelung)
- Backupkonzept
- Virenschutzkonzept
- Schutz vor Diebstahl

Trennungsgebot

Es ist sicher zu Stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden getrennt verarbeitet werden können.

- Trennung von Produktiv- und Testsystemen
- getrennte Ordnerstrukturen (Auftragsdatenverarbeitung)
- separate Tables innerhalb von Datenbanken
- getrennte Datenbanken

Insbesondere sind allgemein Verschlüsselungsverfahren nach aktuellem Stand der Technik zu berücksichtigen.

Zu vielen dieser Maßnahmen sind GF auch auf Grundlage anderer Gesetze verpflichtet. (z.B. HGB, BetrVG, StGb etc.)

Prinzip der Verhältnismäßigkeit

Das BDSG schränkt sich in den zu treffenden Schutzmaßnahmen selbst ein. Für TOM gilt ein sog. Verhältnismäßigkeitsprinzip. Demnach müssen personenbezogene Daten nicht unendlich stark geschützt werden, wenn die Maßnahmen dafür wirtschaftlich unangemessen hoch ausfallen würden. Daraus lässt sich ableiten dass bei einer Auftragsdatenverarbeitung (ADV) der Dienstleister, welcher nur einen Teil der Daten zur Bearbeitung erhält, nicht zwingend die gleichen Schutzmaßnahmen treffen muss, wie sie etwa die verantwortliche Stelle ausführt.

Das Verfahrensverzeichnis

Verfahren automatisierter Verarbeitung

Den Begriff des "Verfahrens" definiert das Gesetz selbst nicht. Abgeleitet aus Art. 18 Abs.1 der EU-Richtlinie 95/46 EG hat sich die folgende Definition durchgesetzt:

"Unter Verfahren ist die Gesamtheit an Verarbeitungen zu verstehen, mit denen eine oder mehrere miteinander verbundene Zweckbestimmung(en) realisiert werden sollen. Ein Verfahren kann danach eine Vielzahl von DV-Dateien umfassen." (siehe Merkblatt zur Meldepflicht)

Als Beispiele für Verfahren können danach

- Personalverwaltungs-,
- Betreuungs- und Abrechnungssysteme,
- Verfahren zur Abwicklung von Kundenaufträgen,
- Telekommunikationssysteme,
- Teledienste und
- sonstige Systeme, die eine geschlossene Struktur von Verarbeitungen umfassen,

genannt werden.

Eine Zusammenfassung mehrerer demselben Zweck dienenden Verarbeitungen ist zulässig und zweckmäßig, wenn sie der Vereinfachung und einer besseren Transparenz dient. Werden beispielsweise innerhalb des Verfahrens "Abwicklung von Kundenaufträgen" verschiedene Verarbeitungen vorgenommen (Aufnahme der Kundendaten, Verarbeitung der Aufträge, Abrechnung), so können diese als ein Verfahren der automatisieren Verarbeitung angesehen werden, denn der Zweck der einzelnen evtl. mehrfach wiederholten Verarbeitungen dient innerhalb des Verfahrens der gleichen Bestimmung.

Jedoch sollte dabei keinesfalls auf die detaillierte Beschreibung der einzelnen geforderten Inhalte (Personengruppen, Übermittlungen usw.) verzichtet werden.

Internes Verfahrensverzeichnis

Die datenschutzrechtlich konforme Gestaltung des Umgangs mit personenbezogenen Daten erfordert zunächst die Ermittlung der Information, welche Daten genutzt werden und welche Verfahren zur Nutzung im Einsatz sind. Durch diese Bestandsaufnahme bildet sich die Grundlage für den Bezug

- vorhandene Daten
- Quelle der Daten (von wem wurden sie wann erhoben, existiert eine Einwilligung)
- Zweck der Erhebung, Nutzung und Speicherung (wofür werden die Daten genutzt)
- Weitergabe der Daten (wer bekommt die Daten außer dem verarbeitenden Unternehmen)
- eingesetzte Verfahren zur Nutzung
- Art und Weise der Speicherung (wo werden die Daten gespeichert bzw. zur Nutzung freigegeben)
- Zugriff auf die Daten (wer darf die Daten lesen, ändern, löschen)

⇒ welche Schutzmaßnahmen müssen evtl. zusätzlich getroffen werden

⇒ welche eingesetzten Verfahren müssen evtl. angepasst werden

Die Aufbereitung der gesammelten Informationen ermöglicht somit die Einsicht in Funktionsweisen und Zusammenhänge, die z.B. auch für eine Vorabkontrolle benötigt werden.

Mindestanforderung an den Inhalt

Nach § 4e BDSG werden folgende Angaben für meldepflichtige Verfahren automatisierter Verarbeitungen gefordert:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -Verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 (und Anlage) zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Verfahrensverzeichnisse und Meldepflichten

Anforderungen an die Angaben zu Verfahren der automatisierten Verarbeitung personenbezogener Daten.

Nicht-öffentliche Stellen, die personenbezogene Daten für kommerzielle Zwecke durch automatisierte Verfahren verarbeiten und in den Anwendungsbereich des BDSG fallen, sind verpflichtet, eine Gesamtübersicht über die im Einsatz befindlichen Verarbeitungsverfahren zu erstellen. Zweck dieses Verfahrensverzeichnisses ist die Überprüfbarkeit der Zulässigkeit des Umgangs mit personenbezogenen Daten. Allgemein wird zwischen einem

- "internen" Verfahrensverzeichnis, das durch detaillierte betriebsinterne Informationen sowohl dem Unternehmen als auch dem Datenschutzbeauftragten die Möglichkeit bietet, den Umgang mit Daten zu organisieren und zu kontrollieren.

- und einem "öffentlichen" Verfahrensverzeichnis, welches aus den Informationen der internen Übersicht nach den Mindestanforderungen des BDSG erstellt wird und zum Zweck der Transparenz für jedermann zur Verfügung steht.

Wobei jedoch angemerkt werden muss, dass das BDSG keine Unterscheidung dieser beiden Verfahrensverzeichnisse kennt. Die interne Übersicht dient demnach dem Zweck einer umfangreichen innerbetrieblichen Transparenz, welche die Selbstkontrolle des Unternehmens erleichtert.

Meldepflichtige Stellen

Abs. 1 legt die grundsätzliche Meldepflicht für die „Verfahren automatisierter Verarbeitungen“ aller verantwortlichen Stellen im nicht-öffentlichen und öffentlichen Bereich fest und bezieht damit auch die Stellen ein, die i.S. des § 39 „einem Berufs- oder besonderen Amtsgeheimnis unterliegen“ (z.B. Ärzte, Beratungsstellen, Rechtsanwälte). Verantwortliche Stellen, die öffentliche Aufgaben erledigen, unterliegen außerdem der Meldepflicht des jeweiligen Landesrechtes.

Die Meldepflicht für nicht-öffentliche Stellen besteht regelmäßig, wenn personenbezogene Daten nach § 29 bis § 30a verarbeitet werden. Gleichermaßen sind Unternehmen meldepflichtig, die keinen Datenschutzbeauftragten bestellt haben und deren Datenverarbeitung nicht auf der Einwilligung der Betroffenen beruht und nicht durch § 28 Abs. 1 Nr. 1 gerechtfertigt ist, sobald personenbezogene Daten im Eigeninteresse verarbeitet werden (z.B. kleine Gewerbeunternehmen oder Kleinunternehmen wie Apotheker, Architekten, Optiker, Ärzte, Steuerberater).

Ausschlaggebend für die Meldepflicht ist allein die ständige Beschäftigung der Personen mit der Datenverarbeitung; die Art des Beschäftigungsverhältnisses spielt dabei keine Rolle, ebenso wenig eine nur gelegentliche, jedoch über einen längeren Zeitraum stattfindende Tätigkeit.

Eine Meldepflicht für nicht-öffentliche Stellen besteht, wenn

die verantwortliche Stelle personenbezogene Daten für eigene Geschäftszwecke verwendet und somit als Datenverarbeiter nach § 28 tätig wird - jedoch bestimmen Abs. 2 und Abs. 3 Ausnahmen von der Meldepflicht (siehe unten).

- die verantwortliche Stelle personenbezogene Daten zum Zwecke der Übermittlung oder zum Zwecke der anonymisierten Übermittlung speichert (§ 29 bis § 30a). In diesen Fällen unterliegt die Stelle durch die Regelung in Abs. 4 ausnahmslos der Meldepflicht. Davon erfasst werden folglich nach Abs. 4 Nr. 1 bis 3
- Unternehmen wie Auskunfteien, Kreditschutzorganisationen, Warn- und Informationsdienste, die nach § 29 geschäftsmäßig Daten „zum Zweck Übermittlung“ erheben und speichern,
- Unternehmen, die gem. § 30 geschäftsmäßig personenbezogene Daten „zum Zweck der Übermittlung in anonymisierter Form“ erheben und speichern oder
- Unternehmen, insbesondere Markt- und Meinungsforschungsinstitute, die geschäftsmäßig Daten gem. § 30a erheben und speichern.

Für die Erfüllung der Meldepflicht persönlich verantwortlich sind entsprechend der in § 43 Abs. 1 Nr. 1 geregelten Ordnungswidrigkeit Inhaber, Vorstände, Geschäftsführer oder „sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter“ (§ 4e Abs. 1 Nr. 2) der verantwortlichen Stelle.

Meldung vor Inbetriebnahme

Die vorab zu prüfende Zulässigkeit der Verfahren erfordert die Meldung „vor ihrer Inbetriebnahme“, gleichermaßen eine Veränderung oder Beendigung bereits implementierter Verfahren (§ 4e Satz 2).

Das BDSG schreibt keine verbindliche Form der Meldung vor. Im Allgemeinen hat sich die Schriftform (Formular) oder auch die Übersendung eines Datenträgers bewährt. Näheres (siehe auch Merkblatt zur Meldepflicht) sollte mit der zuständigen Aufsichtsbehörde geklärt werden.

Nicht meldepflichtige Stellen

Keine Meldepflicht besteht

- für nicht-öffentliche Stellen, die einen betrieblichen Datenschutzbeauftragten nach § 4f Abs. 1 bestellt hat (Abs. 2)
- wenn bei der die verantwortliche Stelle weniger als zehn Personen ständig mit der Verwendung personenbezogener Daten beschäftigt sind (Abs. 3). Voraussetzung für diese Ausnahme ist die Einwilligung der Betroffenen oder die automatisierte Datenverarbeitung zur Vertragserfüllung.
- Ebenso entfällt die Meldepflicht für nicht-öffentliche Stellen, deren Mitarbeiteranzahl zwar unter der geforderten Mindestanzahl liegt, die jedoch durch die Verarbeitung von Daten nach § 3 Abs. 9 einer Vorabkontrolle verpflichtet sind (Abs. 5) und einen Datenschutzbeauftragten nach § 4f Abs. 1 Satz 6 bestellen müssen. Der Grundsatz der Meldepflicht bei der Verwendung personenbezogener Daten durch mehr als neun Personen bleibt davon unberührt.
- für Auftragsdatenverarbeiter oder andere Stellen, die i.S.d. § 11 nicht für die Verarbeitung personenbezogener Daten verantwortlich, mithin als Verarbeiter fremder Geschäftszwecke zu beurteilen sind.

Dazu zählen beispielsweise

- Service-Rechenzentren
- privat-ärztliche Verrechnungsstellen
- einem Konzern angehörende Unternehmen, die für andere Gesellschaften des Konzerns Aufgaben der Datenverarbeitung erledigen
- Datenträgervernichter oder -entsorger
- Mikroverfilmer oder -konvertierer

Die Befreiung von der Meldepflicht gilt jedoch nur im Rahmen der Auftragsdatenverarbeitung; eine eigenverantwortliche automatisierte Verarbeitung ist davon nicht erfasst.

für öffentliche Stellen des Bundes, da sie nach § 4f Abs. 1 Satz 1 grundsätzlich zur Bestellung eines behördlichen Datenschutzbeauftragten verpflichtet sind.

Vorabkontrolle

Zuständig für die Vorabkontrolle ist nach § 4d Abs. 6 Satz 1 der Beauftragte für den Datenschutz. Die verantwortliche Stelle ist gem. Satz 2 verpflichtet, ihm vor der Inbetriebnahme - also noch in der Planungsphase - die Verfahrensübersicht zur Verfügung zu stellen (§ 4g Abs. 2 Satz 1). Um dem Beauftragten eine ordnungsgemäße Stellungnahme nach eigenem Ermessungsspielraum zu ermöglichen, sollte die Übersicht in ausreichend detaillierter Form vorliegen.

Der Gesetzgeber - wenngleich es im BDSG nicht verankert ist - sieht die Aufgabe des Datenschutzbeauftragten in der „Prüfung der materiellen Zulässigkeit der Datenverarbeitung“ und verlangt mithin die Kontrolle insbesondere von § 4e Nr. 5, 6 und 9. Das bedeutet zunächst die Prüfung der beabsichtigten Verarbeitung und ihrer Grundlagen nach

- der Zulässigkeit der Verarbeitung nach § 4 Abs. 1 i.V.m. einer Rechtsvorschrift oder nach § 4a i.V.m. einer Einwilligung
- den Datenkategorien und betroffenen Personengruppen sowie deren evtl. Gefährdungen („besondere Risiken“ und Auswirkungen auf die informationelle Selbstbestimmung)
- dem Grundsatz der Datenvermeidung und Datensparsamkeit gem. § 3a
- der Wahrung der Rechte betroffener Personengruppen nach § 6 und Beachtung des Grundsatzes der Transparenz
- den technisch organisatorischen Maßnahmen gem. § 9 und Anlage zu § 9 Satz 1

Eine materielle Zulässigkeit oder Rechtmäßigkeit des beabsichtigten Verfahrens ergibt sich nicht aus einer ordnungsgemäßen Vorabkontrolle, vielmehr ist diese als Bedingung automatisierter Verfahren, die besondere Risiken für die Betroffenen bergen, anzusehen. Sinn und Zweck der Vorabkontrolle ist die vorab festgestellte Zulässigkeit des vorgesehenen Verfahrens bzw. das Festhalten von Vorbehalten, um rechtzeitig (vor Inbetriebnahme) erforderliche Maßnahmen von datenschutzrechtlicher Relevanz umsetzen zu können.

Die schriftliche Dokumentation der Kontrolle ergibt sich aus den organisatorischen Verpflichtungen des § 9; sie ist der verantwortlichen Stelle vorzulegen.

Die Entscheidung, ob das Verfahren in Betrieb genommen wird, liegt allein in der Verantwortung der verantwortlichen Stelle. Sie hat dabei vorgetragene Bedenken des Datenschutzbeauftragten bezüglich der Rechtmäßigkeit zu würdigen. Sie ist aber nicht von "Genehmigung" des Beauftragten abhängig. Das Gesetz regelt nicht die Folgen bei einer Unterlassung der Vorabkontrolle. Zeigt sich allerdings später, dass das Verfahren teilweise rechtswidrig ist, weil die verantwortliche Stelle sich über die Bedenken des Datenschutzbeauftragten hinweggesetzt hat, so deutet dies auf eine Verletzung ihrer Sorgfaltspflicht nach § 7 Satz 2 hin und kann entsprechende und zivilrechtliche Konsequenzen haben.

Einschalten der Aufsichtsbehörde

§ 4d Abs. 6 Satz 3 verpflichtet den Datenschutzbeauftragte, sich „in Zweifelsfällen an die Aufsichtsbehörde“ zu wenden. Zweifelsfälle können Unsicherheiten bei festgestellten Mängeln oder vorhandene Zweifel an der Rechtmäßigkeit des Verfahrens aber auch die Konfliktsituation beinhalten, die durch unterschiedliche Beurteilungen - Bedenken des Datenschutzbeauftragten einerseits und nicht für notwendig gehaltene Maßnahmen der verantwortlichen Stelle andererseits - entstehen. Bestehen offensichtliche rechtliche Mängel, hat der Datenschutzbeauftragte die Aufsichtsbehörde auf jeden Fall zu informieren.

Bei berechtigten Zweifeln jedweder Art muss demnach die Aufsichtsbehörde konsultiert werden. Es ist dringend anzuraten, die verantwortlichen Stelle von der entsprechenden Absicht vorab zu informieren und ihr Gelegenheit zu geben, doch noch eine - auch aus der Sicht des Datenschutzbeauftragten - tragfähige Lösung zu finden.

Die Aufsichtsbehörde hat den Bedenken des Datenschutzbeauftragten nachzugehen, trifft ihre Beurteilung nach § 38 aber in eigener Verantwortung.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Auszüge, Quelle: http://www.bfdi.bund.de/