535.4.10

FAQs
zur Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a Bundesdatenschutzgesetz (BDSG)[1]

Nichtöffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen sind dazu verpflichtet, sowohl die Aufsichtsbehörde als auch die Betroffenen[2] zu benachrichtigen, wenn personenbezogene Daten einer bestimmten, in § 42a Satz 1 BDSG bezeichneten Datenkategorie Dritten unrechtmäßig zur Kenntnis gelangen. Weitere Voraussetzung für die Pflicht zur Mitteilung ist, dass für die Rechte oder schutzwürdigen Interessen der Betroffenen schwerwiegende Beeinträchtigungen drohen. Wann dies im Einzelnen der Fall ist und welche Konsequenzen daraus folgen, soll mit Hilfe der folgenden FAQs näher erläutert werden. Die Fragen und Antworten sollen dabei helfen, die mitteilungspflichtigen Sachverhalte zu identifizieren (Teil A) und die entstehenden Handlungspflichten zu erkennen bzw. umzusetzen (Teil B).

Teil A: Mitteilungspflichtige Sachverhalte identifizieren

Teil B: Handlungspflichten erkennen und umsetzen

[1] Siehe Anhang Punkt 1.

[2] Wieviele Personen betroffen sind, ist unerheblich; auch bei nur einer betroffenen Person kann die Informationspflicht ausgelöst werden.

Teil A: Mitteilungspflichtige Sachverhalte identifizieren

1. Wer ist zur Mitteilung verpflichtet?

Nach § 42a Satz 1 BDSG sind

- nichtöffentliche Stellen (§ 2 Absatz 4 BDSG) sowie
- öffentlich-rechtliche Wettbewerbsunternehmen

verpflichtet.

Nichtöffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht Aufgaben der öffentlichen Verwaltung oder hoheitliche Aufgaben wahrnehmen, oder Vereinigungen von öffentlichen Stellen des Bundes oder der Länder sind.

§ 42a Satz 1 BDSG verweist auf § 27 Absatz 1 Satz 1 Nr. 2 BDSG, so dass auch öffentliche Stellen des Bundes, die als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, § 42a BDSG beachten müssen. Öffentliche Stellen des Landes, die als Wettbewerbsunternehmen tätig sind, werden nur erfasst, wenn das entsprechende Landesdatenschutzgesetz auf § 42a BDSG verweist. Da alle Landesdatenschutzgesetze auf das BDSG bzw. auf einzelne Vorschriften des BDSG (inklusive § 42a BDSG) verweisen, gilt § 42a BDSG ausnahmslos für die öffentlichen Stellen der Länder, die als Wettbewerbsunternehmen tätig sind.

Für sonstige öffentliche Stellen des Bundes und der Länder ist § 42a BDSG nicht anwendbar. Anderes gilt für die dem § 42a BDSG entsprechenden Informationspflichten in § 109a Telekommunikationsgesetz (TKG)[3] und § 15a Telemediengesetz (TMG)[4]. Dort wird keine Unterscheidung zwischen öffentlichen und nichtöffentlichen Stellen getroffen. Diese Vorschriften sind gleichermaßen auf alle Datenverarbeiter anwendbar.

zurück

2. Ist der Auftragsdatenverarbeiter (§ 11 BDSG[5]) zur Mitteilung verpflichtet?

Der Auftragsdatenverarbeiter nach § 11 BDSG ist **selbst nicht** Adressat des § 42a BDSG. Gem. § 11 Absatz 4 BDSG[6] gelten für den Auftragnehmer nur bestimmte Vorschriften des BDSG. § 42a BDSG wird in § 11 Absatz 4 BDSG nicht erwähnt und zählt daher nicht zu den für den Auftragnehmer anwendbaren Vorschriften. Für einen Verlust von Daten, die beim Auftragnehmer im Auftrag gespeichert waren, ist der **Auftraggeber verantwortlich**. Dieser muss die Aufsichtsbehörde und die Betroffenen benachrichtigen. Kommt es hier zu Verzögerungen, z.B. weil der Auftragnehmer den Auftraggeber zu spät von dem Datenverlust in Kenntnis setzt, geht dies zu Lasten des Auftraggebers. Der Auftraggeber muss daher dafür Sorge tragen, dass der Auftragnehmer **zur unverzüglichen Meldung** gegenüber dem Auftraggeber **verpflichtet** ist, sollten Daten beim Auftragnehmer abhandenkommen. Dies er-

[3] Siehe Anhang Punkt 2.

[4] Siehe Anhang Punkt 3.

[5] Siehe Anhang Punkt 4.

[6] Siehe Anhang Punkt 4.

reicht er durch eine klare vertragliche Verpflichtung im Auftragsdatenverarbeitungsvertrag (§ 11 Absatz 2 Nr. 8 BDSG[7]) und eine Kontrolle des Meldeprozesses.

(Siehe z.B. die Formulierung[8] in der Mustervereinbarung Auftrags-DV nach § 11 BDSG des Regierungspräsidiums Darmstadt).

zurück

3. Welche Datenarten sind betroffen?

Erfährt die verantwortliche Stelle z.B. durch das eigene Sicherheitsmanagement, durch Hinweise von Strafverfolgungsbehörden, durch den betrieblichen Datenschutzbeauftragten, durch die Aufsichtsbehörde oder aus anderen Quellen davon, dass Daten abhandengekommen sind, muss sie feststellen, **welche Datenarten** betroffen sind. Eine Pflicht zur Information kommt nach § 42a Satz 1 BDSG nur dann in Betracht, wenn die Daten zu einer der **folgenden Kategorien** gehören:

- besondere Arten personenbezogener Daten (§ 3 Absatz 9 BDSG[9], dazu a.),
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen (dazu b.),
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen (dazu c.), oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten (dazu d.).

Die Daten müssen **bei der verantwortlichen Stelle gespeichert** sein, d.h. wenn die Daten beim Betroffenen selbst abhandenkommen (z.B. PIN und TAN-Nummer beim Onlinebanking), ist § 42a BDSG nicht einschlägig. Dagegen kann § 42a BDSG in Betracht kommen, wenn Daten **unbefugt aus einem IT-System abgerufen** werden, indem Passwörter, Zugangscodes, Skriptinformationen etc. verwendet werden, die der Angreifer sich beim Betroffenen oder auf anderem Wege (z.B. über Social Engineering) beschafft hat.

a. Besondere Arten personenbezogener Daten

Bei den besonderen Arten personenbezogener Daten handelt es sich um Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Besonders relevant wird die Informationspflicht nach § 42a BDSG im Bereich der Verarbeitung von **medizinischen Daten** (durch Ärzte, Krankenhäuser, Versicherungen etc.). Auch die Tatsache, dass sich jemand in Behandlung befindet, stellt eine Angabe über die Gesundheit dar, so dass auch Kontaktdaten von Patienten unter § 42a Satz 1 Nr. 1 BDSG fallen können.

Besondere Arten personenbezogener Daten können auch betroffen sein, wenn **Personalaktendaten** abhandenkommen. So zählen Krankschreibungen oder die Anzahl von Krankheits-

[7] Siehe Anhang Punkt 4.

[8] Siehe Anhang Punkt 5.

[9] Siehe Anhang Punkt 6.

tagen, die sich ggf. aus einer Personalakte ergeben, zu den Daten über die Gesundheit. Darüber hinaus kann sich in den Lohnsteuerunterlagen ein **Hinweis auf die Religionszugehörigkeit** finden.

b. Berufsgeheimnis

Ein Berufsgeheimnis ist eine **rechtliche Verpflichtung zur Verschwiegenheit**. Es macht bestimmte Berufsinhaber z.B. aufgrund eines besonderen Vertrauensverhältnisses zu Geheimnisträgern. Der Berufsgeheimnisträger darf die ihm anvertrauten Informationen im Regelfall nur offenbaren, wenn der Betroffene zugestimmt hat. Soweit es sich bei dem Inhalt solcher Geheimnisse um personenbezogene Daten handelt und diese unbefugt Dritten zur Kenntnis gelangen, kommt § 42a BDSG in Betracht. Berufsgruppen, deren Angehörige einem Berufsgeheimnis unterliegen, sind in § 203 Strafgesetzbuch (StGB)[10] aufgezählt. Zu diesen gehören z.B. Anwälte, Notare und Ärzte. Das Datengeheimnis nach § 5 BDSG[11] zählt nicht zu den Berufsgeheimnissen, wohl aber Verschwiegenheitspflichten des Steuerberaters und Wirtschaftsprüfers.

Angehörige eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung sind ebenfalls Berufsgeheimnisträger. Die Tatsache, dass ein **Lebensversicherungsvertrag besteht**, stellt z.B. ein personenbezogenes Datum dar, das vom Berufsgeheimnis dieser Personen erfasst wird. Wenn Kundenkontaktdaten abhandenkommen, aus denen sich die Vertragsbeziehung zu einem Lebensversicherer ergibt, kann § 42a Satz 1 Nr. 2 BDSG einschlägig sein.

Das **Personalaktengeheimnis** verpflichtet grundsätzlich nur öffentlich-rechtliche Arbeitgeber, so dass dieses im Zusammenhang mit § 42a BDSG nur für die öffentlich-rechtlichen Wettbewerbsunternehmen relevant werden könnte. Allerdings beinhalten Personalaktendaten häufig auch Daten, die anderen Datenkategorien[12] des § 42a Satz 1 BDSG zugeordnet werden können. Eine Informationspflicht käme dann trotzdem in Betracht.

Daten, die dem **Sozialgeheimnis** (§ 35 Sozialgesetzbuch (SGB) I, § 67 SGB X) unterliegen, werden von Sozialleistungsträgern verarbeitet. Für diese gilt eine spezielle Informationspflicht, die in § 83a SGB X[13] geregelt ist und sich auf besondere Arten personenbezogener Daten (§ 67 Abs. 12 SGB X) bezieht.

c. Informationen zu strafbaren Handlungen oder Ordnungswidrigkeiten

Zu den personenbezogenen Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten beziehen, zählen sämtliche Informationen, die mit Straf- oder Ordnungswidrigkeitstatbeständen in einem Zusammenhang stehen, mindestens aber Informationen zu **laufenden oder abgeschlossenen Verfahren.**

Außerdem kommt § 42a Satz 1 Nr. 3 BDSG in Betracht, wenn personenbezogene Daten abhandenkommen, die sich auf den **Verdacht strafbarer Handlungen oder Ordnungswid-**

[10] Siehe Anhang Punkt 7.

[11] Siehe Anhang Punkt 8.

[12] Siehe Teil A 3. a., Seite 3/4.

[13] Siehe Anhang Punkt 9.

rigkeiten beziehen. Nach § 32 Abs. 1 Satz 2 BDSG[14] ist der Arbeitgeber unter bestimmten Voraussetzungen berechtigt, personenbezogene Daten des Beschäftigten zur **Aufdeckung von Straftaten** zu erheben, zu verarbeiten oder zu nutzen. Bei Abhandenkommen dieser Daten könnte eine Informationspflicht nach § 42a BDSG ausgelöst werden.

Informationen zu Ordnungswidrigkeiten können z.B. beim Betrieb eines Fuhrparks im Unternehmen eingehen. Dies ist der Fall, wenn Mitarbeiter mit **Dienstwagen** Verkehrsordnungswidrigkeiten begehen und die Polizei sich per Anhörungsschreiben an den Halter, d.h. den Arbeitgeber, wendet. Wenn diese Informationen unbefugt an Dritte gelangen, kommt § 42a Satz 1 Nr. 3 BDSG in Betracht.

d. Personenbezogene Daten zu Bank- und Kreditkartenkonten

Personenbezogene Daten zu Bank- und Kreditkartenkonten sind sämtliche Informationen, die mit solchen Konten im Zusammenhang stehen. Auch die Tatsache, dass eine Kontobeziehung besteht, gehört dazu. **Kreditkarten- und Kontonummern** mit oder ohne Namen des Kreditkarten- und Bankkontoinhabers sind ebenfalls personenbezogene Daten zu Bank- oder Kreditkartenkonten. Jegliche **Transaktionsdaten** sind ebenso wie **Prägespurdaten**, ausgefüllte **Überweisungsvordrucke, Kreditkartenbelege, Kontoauszüge** von § 42a Satz 1 Nr. 4 BDSG erfasst. Soweit aus Bankunterlagen, -mitteilungen bzw. -daten ein Bezug zu einem Bank- oder Kreditkartenkonto hervorgeht, ist § 42a Satz 1 Nr. 4 BDSG einschlägig.

zurück

4. In welchen Fällen ist von einer unrechtmäßigen Kenntniserlangung auszugehen?

Die Pflicht zur Mitteilung setzt nach § 42a Satz 1 BDSG weiterhin voraus, dass die Daten **unrechtmäßig übermittelt** oder **auf sonstige Weise Dritten unrechtmäßig zur Kenntnis** gelangt sind.

Unrechtmäßig ist die Übermittlung oder sonstige Kenntniserlangung dann, wenn sie **ohne Rechtsgrund** erfolgt. Dies ist der Fall, wenn die Betroffenen nicht zugestimmt haben und die Offenbarung weder durch Gesetz noch sonstige Rechtsvorschrift erlaubt ist. Auf ein etwaiges Verschulden beim Datenverlust, auf eine selbst initiierte Weitergabe oder auf eine sonstige Mitwirkung der datenverarbeitenden Stelle kommt es insgesamt nicht an. Eine Informationspflicht kann z. B. auch dann in Betracht kommen, wenn die datenverarbeitende Stelle eine bewusste Datenübermittlung vorgenommen hat, die unzulässig war. Für die Frage, ob § 42a BDSG anwendbar ist, spielt es keine Rolle, ob eine Übermittlung vorliegt oder die Daten „in sonstiger Weise Dritten“ zur Kenntnis gelangt sind. Wie der Begriff „auf sonstige Weise“ zum Ausdruck bringt, soll die Übermittlung einen Spezialfall darstellen.

Die Kenntniserlangung durch einen Dritten muss **nicht positiv festgestellt** werden. Es ist ausreichend, wenn es entweder **offensichtlich** ist, dass Dritte Kenntnis erlangt haben, oder wenn anhand von **tatsächlichen Anhaltspunkten** mit einer **gewissen Wahrscheinlichkeit** davon ausgegangen werden kann. Es liegt letztlich in der Verantwortung der Daten verarbeitenden Stelle, über die Frage der Benachrichtigung zu entscheiden. Es kann Fälle geben, in denen es auf einzelne Stunden ankommt, innerhalb welcher Betroffene durch die Benachrichtigung in die Lage versetzt werden, Abwehrmaßnahmen zu ergreifen. Wenn in solchen Fällen von einer Benachrichtigung mangels Gewissheit über die Kenntniserlangung abgese-

[14] Siehe Anhang Punkt 10.

hen wird, kann dies nicht nur zu datenschutzrechtlichen Konsequenzen führen, sondern auch in Schadensersatzfällen die Frage der Mitschuld aufwerfen.

Eine Übermittlung bzw. unrechtmäßige Kenntniserlangung ist in Fällen von nicht gerechtfertigter Sammeladressierung gegeben bzw. wenn Daten an einen falschen Adressaten übermittelt werden. Ebenso sind **Veröffentlichungen im Internet** erfasst, z.B. in Fällen, in denen Informationen aufgrund eines technischen Fehlers durch Suchmaschinen indexiert oder auf andere Weise für Dritte zugänglich werden.

Eine Informationspflicht kommt auch in Fällen des **Datenverlusts** in Betracht, wenn Laptops oder andere Datenträger an Orten verlorengehen, wo sie Dritten zugänglich sind und die Daten **nicht verschlüsselt** sind. Gleiches gilt, wenn **Daten gestohlen** oder illegal aus IT-Systemen abgerufen werden. Auch in diesem Zusammenhang ist von einer Kenntniserlangung immer dann auszugehen, wenn die Daten, z.B. die Festplatte eines gestohlenen Laptops, nicht verschlüsselt waren. Eine Festplattenverschlüsselung eines Notebooks bietet allerdings nur dann ausreichende Sicherheit, wenn es zum Zeitpunkt des Verlusts ausgeschaltet ist, das Passwort eine ausreichende Länge[15] aufweist und nicht (so) notiert wird, dass es einem potenziellen Angreifer in die Hände gelangen kann. Eine Zugangssperre, etwa in Form des Windows-Login, reicht nicht aus. Diese kann technisch leicht umgangen werden.

Auch **Mitarbeiter** können „Dritte“ im Sinne des § 42a Satz 1 BDSG sein. Wenn Mitarbeiter etwa Daten unbefugt an private eigene E-Mail-Adressen versenden oder auf externen Medien speichern und diese mitnehmen, kann § 42a BDSG den Arbeitgeber zur Mitteilung verpflichten. Darüber hinaus kann § 42a BDSG einschlägig sein, wenn Mitarbeiter Daten unbefugt aus automatisierten Abrufverfahren abfragen (z.B. unzulässige Bonitätsabfrage des Mitarbeiters eines Kreditinstituts im automatisierten Abrufverfahren). In solchen Fällen erhält der Mitarbeiter die Daten nicht im Rahmen seiner arbeitsvertraglich festgelegten Befugnisse, sondern als Privatperson. Damit ist er **nicht mehr Teil der Organisation**, sondern steht außerhalb der verantwortlichen Stelle und wird mithin zum „Dritten“ (§ 3 Abs. 8 Satz 2 BDSG[16]). Die Daten, die er mitgenommen bzw. abgerufen hat, sind damit einem Dritten unrechtmäßig zur Kenntnis gelangt. Ob das Handeln des Mitarbeiters dem Arbeitgeber zuzurechnen ist oder nicht, spielt für die Informationspflicht des Arbeitgebers keine Rolle. Diese wird allein dadurch ausgelöst, dass die Daten, die beim Arbeitgeber gespeichert waren, nunmehr einer als „Dritter“ anzusehenden Person zur Kenntnis gelangt sind.

zurück

5. In welchen Fällen drohen schwerwiegende Beeinträchtigungen?

Eine Informationspflicht besteht nur dann, wenn die vorgenannten Voraussetzungen erfüllt sind und nach § 42a Satz 1 BDSG zusätzlich **schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen** drohen. Dabei kommt es darauf an, welche **Auswirkungen** die unrechtmäßige Kenntniserlangung durch Dritte für die Betroffenen haben kann.

Die verantwortliche Stelle muss eine Prognoseentscheidung treffen, d.h. sie muss **mögliche Folgen** nach Lage der Dinge identifizieren und diese anhand der **Belastung** für die Betroffe-

[15] Laut Empfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI) sollten hierfür nicht nur 8, sondern 20 Zeichen verwendet werden; siehe www.bsi-fuer-buerger.de.

[16] Siehe Anhang Punkt 11.

nen und der **Wahrscheinlichkeit**, dass die Belastung eintritt, bewerten. Dabei wird es in vielen Fällen hilfreich sein, **mögliche Verwendungsszenarien** zu entwerfen und diese „durchzuspielen". Relevant ist dabei nicht nur, was Dritte aufgrund der Beschaffenheit der Daten mit diesen anfangen können, sondern auch, welche Arten der Verwendung (z.B. Identitätsbetrug, Verbreitung) in Betracht kommen. Unter Umständen spielt es auch eine Rolle, wer die Daten – soweit bekannt – in die Hände bekommen hat und über **welches Zusatzwissen / welche Fähigkeiten diese Personen** verfügen bzw. welche Ziele verfolgt werden.

Die Szenarien sind daraufhin zu analysieren, welche potentiellen Beeinträchtigungen, materieller wie immaterieller Art (z.B. Vermögensschäden, soziale Nachteile), entstehen können. Je größer die mögliche Beeinträchtigung der Rechte oder Interessen der Betroffenen ist, desto geringere Anforderungen sind an die Eintrittswahrscheinlichkeit zu stellen.

Außer Acht zu lassen ist, ob den Betroffenen Ausgleichs-, Widerrufs-, Rückbuchungsansprüche oder sonstige Möglichkeiten zustehen, etwaige Schäden auszugleichen. Auf **zivilrechtliche Haftungsfragen** oder Fragen der Mitschuld kommt es nicht an. Die Informationspflicht des § 42a BDSG soll die Betroffenen in die Lage versetzen, **erhöhte Missbrauchsgefahren zu erkennen** und ggf. **weitere Vorsorgemaßnahmen** zu treffen. Dabei spielt es keine Rolle, ob die Betroffenen z.B. vertraglich verpflichtet sind, Unregelmäßigkeiten umgehend anzuzeigen (Bsp.: Pflicht zur Prüfung der Kreditkartenabrechnung). Wenn Kreditkartendaten beim Kartenemittenten abhandenkommen, erhöht sich die Gefahr der missbräuchlichen Nutzung stark. Die Betroffenen müssen in die Lage versetzt werden, die Überprüfungen ihrer Abrechnungen in Umfang und Intensität **der neuen Gefährdungslage anzupassen**. Der Maßstab dafür, wie stark die Betroffenen belastet sein „müssen", damit eine Informationspflicht ausgelöst wird, ist daher nicht zu hoch anzulegen. Die verantwortliche Stelle sollte stets berücksichtigen, dass sie das volle Risiko trägt, dass sie sich irrt. Es ist also eher umgekehrt zu fragen, **welche Konstellationen denkbar** sind, in denen die bezeichneten Arten von Daten, bei denen es sich in der Regel ohnehin um sehr sensible Daten handelt, Dritten zur Kenntnis gelangen, **ohne** dass hieraus schwerwiegende Beeinträchtigungen entstehen. Letzteres kann z.B. der Fall sein, wenn die Daten **stark verschlüsselt** sind.[17]

Für den Fall, dass die verantwortliche Stelle zu dem Ergebnis kommt, dass keine schwerwiegenden Beeinträchtigungen drohen und sie die Benachrichtigung der Betroffenen folglich unterlässt, muss sie gegenüber der Aufsichtsbehörde nachweisen können, warum sie zu diesem Ergebnis gekommen ist. Dazu ist zu empfehlen, dass die verantwortliche Stelle den **Entscheidungsprozess dokumentiert** und **das prognostizierte Ergebnis nachvollziehbar** begründen kann.

Es empfiehlt sich, den **betrieblichen Datenschutzbeauftragten** im Rahmen der Prognoseentscheidung, aber auch bei der gesamten Prüfung der Voraussetzungen des § 42a BDSG frühzeitig **einzubinden**.

zurück

[Siehe Schaubild zu Teil A.]

[17] Siehe WP 213 der Art. 29-Datenschutzgruppe, Stellungnahme vom 25. März 2014 (bislang nur engl. Fassung): Opinion 03/2014 on Personal Data Breach Notification

Teil B: Handlungspflichten erkennen und umsetzen

1. Wann müssen Aufsichtsbehörde und Betroffene benachrichtigt werden?

Die Betroffenen und die zuständige Aufsichtsbehörde[18] sind nach § 42a Satz 1 BDSG grundsätzlich **unverzüglich**, d.h. ohne schuldhaftes Zögern, zu benachrichtigen.[19]

Für die **Benachrichtigung der Aufsichtsbehörde** steht der verantwortlichen Stelle eine zur Ermittlung des Sachverhalts und Prüfung der Voraussetzungen des § 42a BDSG angemessene Frist zu, die sich an den **Umständen des Einzelfalles** bemisst. Dabei kommt es auf die Komplexität des Vorfalles an. Die Frist beginnt mit der **Kenntnis der verantwortlichen Stelle**, dass Daten übermittelt oder unrechtmäßig zur Kenntnis gelangt sind. Für die Benachrichtigung der Aufsichtsbehörde ist es unerheblich, ob alle Sicherheitslücken bereits geschlossen sind oder ob ein Ermittlungsverfahren der Strafverfolgungsbehörden noch läuft. Maßgeblich ist allein die Frage, ob ein Fall des § 42a BDSG[20] vorliegt.

Die **Benachrichtigung der Betroffenen** muss unverzüglich erfolgen, sobald

- angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind (dazu a.) und
- die Strafverfolgung nicht mehr gefährdet wird (dazu b.).

Die verantwortliche Stelle muss gegenüber der Aufsichtsbehörde im Zweifel nachweisen können, warum die Zurückstellung der Benachrichtigung der Betroffenen gerechtfertigt war. Die **Gründe, das Vorgehen** (z.B. die Kontaktaufnahme zum Hersteller von Software[21]) und ggf. die Kommunikation mit der Staatsanwaltschaft[22] sollten **dokumentiert** werden.

a. Angemessene Maßnahmen zur Sicherung der Daten

Wenn es möglich ist, **angemessene Maßnahmen zur Sicherung der Daten** zu ergreifen, haben diese Vorrang, soweit die Benachrichtigung der Betroffenen den Erfolg der Maßnahmen gefährden würde. Die Betroffenen sind dann unverzüglich zu benachrichtigen, sobald die Maßnahmen ergriffen wurden. Welche Datensicherungsmaßnahmen dabei in Betracht kommen, hängt vom Einzelfall ab. Etwaige **technische Sicherheitslücken**, die zur Ursache für den Datenverlust geworden sind, müssen analysiert und wenn möglich behoben werden. Für den Fall, dass eine Sicherheitslücke in der **eingesetzten Software** festgestellt wird, sollte zunächst der Hersteller der Software hierüber unterrichtet werden. Dieser sollte unter Fristsetzung aufgefordert werden, die Sicherheitslücke zu schließen. Auf diesem Weg der sog. **„Responsible Disclosure“** („verantwortungsvolle Offenlegung“) wird dem Hersteller die Gelegenheit gegeben, die Schwachstellen zu beseitigen, bevor die Sicherheitslücke öf-

[18] Siehe Anhang Punkt 12.

[19] Die zuständige Aufsichtsbehörde soll von der verantwortlichen Stelle gemäß der Richtlinie 2002/58/EG und der Verordnung (EU) Nr. 611/2013 von der Verletzung des Schutzes personenbezogener Daten binnen 24 Stunden nach Feststellung der Verletzung, soweit dies möglich ist, benachrichtigt werden (Erstbenachrichtigung).

[20] Siehe Teil A.

[21] Siehe Teil B 1. a., Seite 8.

[22] Siehe Teil B 1. b., Seite 9.

fentlich wird. Allerdings ist die Benachrichtigung der Betroffenen nicht weiter zurückzuhalten, wenn der Hersteller auf die Forderungen der verantwortlichen Stelle nicht reagiert bzw. eine Schließung der Sicherheitslücke ohne vernünftigen Grund unterlässt oder verzögert.

b. Gefährdung der Strafverfolgung

Wenn **Ermittlungen der Strafverfolgungsbehörden gefährdet** werden könnten, hat die Benachrichtigung der Betroffenen zunächst zu unterbleiben. Diese Möglichkeit, die Benachrichtigung nach § 42a BDSG aus Strafverfolgungsgründen aufzuschieben, betrifft natürlich nur solche Strafverfolgungen, die infolge des Vorfalls der unrechtmäßigen Kenntniserlangung angestoßen bzw. durchgeführt werden. Sobald die Strafverfolgung nicht mehr gefährdet ist, muss unverzüglich benachrichtigt werden. Zumeist wird die verantwortliche Stelle nicht selbst ermessen können, ob die Ermittlungen durch die Offenlegung beeinträchtigt sind. Es empfiehlt sich daher, die **Einschätzung der Strafverfolgungsbehörden**, insbesondere den Rat des leitenden Staatsanwaltes, einzuholen.

zurück

2. Worüber ist die Aufsichtsbehörde zu unterrichten?

Die Benachrichtigung der Aufsichtsbehörde sollte schon aus Nachweisgründen **schriftlich** erfolgen oder zumindest **schriftlich nachgereicht** werden. Mit der Benachrichtigung müssen die folgenden Fragen beantwortet werden:

- **Wann sind die Daten abhandengekommen bzw. wann wurde dies von der verantwortlichen Stelle festgestellt?**

- **Welche Daten sind betroffen und wie wurden diese unrechtmäßig übermittelt bzw. wie sind diese Daten unrechtmäßig zur Kenntnis gelangt?**
  Der Vorfall sollte detailliert beschrieben werden, d.h. sämtliche zur Verfügung stehenden, relevanten Informationen müssen der Aufsichtsbehörde mitgeteilt werden. Für den Fall, dass die verantwortliche Stelle aufgrund tatsächlicher Anhaltspunkte mit einer gewissen Wahrscheinlichkeit von einer Kenntniserlangung ausgeht, sind Anhaltspunkte und Schlussfolgerungen konkret darzulegen.

- **Welche nachteiligen Folgen der unrechtmäßigen Kenntniserlangung sind möglich?**
  In diesem Zusammenhang sind die von der verantwortlichen Stelle zusammengestellten Verwendungsszenarien, deren Eintrittswahrscheinlichkeit und deren Folgen darzustellen. Bei den möglichen nachteiligen Folgen geht es nicht nur um die unmittelbaren Belastungen für die Rechte und schutzwürdigen Interessen der (schon) Betroffenen, sondern auch um etwaige nachteilige Folgen für die IT-Sicherheit der verantwortlichen Stelle, soweit dies datenschutzrechtlich relevant ist.

- **Welche Maßnahmen wurden von der verantwortlichen Stelle ergriffen?**
  Die Maßnahmen sind so detailliert zu beschreiben, dass die Aufsichtsbehörde feststellen kann, ob die Sicherheitslücke geschlossen wurde bzw. wie die festgestellte unrechtmäßige Kenntnisnahme für die Zukunft ausgeschlossen ist. Es ist z.B. darzulegen, ob Server, zu denen sich Dritte unbefugt Zugriff verschafft haben, vom Netz genommen wurden bzw. ob Karten, Passwörter, Zugangscodes ausgetauscht wurden und ggf. VPN-Zugänge, die über gestohlene Laptops aktiviert werden könnten, geschlossen wurden.

- **Sind die Betroffenen bereits benachrichtigt worden und was wurde diesen empfohlen?**
  Wenn die Betroffenen noch nicht informiert wurden, ist darzulegen, aus welchen Gründen die Benachrichtigung zurückgehalten wurde. Außerdem ist zu beschreiben, wie die Betroffenen informiert werden sowie welche Maßnahmen ihnen zur Minderung möglicher nachteiliger Folgen empfohlen werden sollen.

zurück

3. Worüber sind die Betroffenen zu unterrichten?

Den Betroffenen muss die **Art der unrechtmäßigen Kenntniserlangung** dargelegt und **Maßnahmen zur Minderung möglicher nachteiliger Folgen** empfohlen werden. Dabei geht es darum, den Betroffenen transparent und verständlich zu machen, was passiert ist und welche Gefahren drohen. Den Betroffenen muss die **erhöhte Missbrauchsgefahr** vergegenwärtigt werden. Sie sollten durch die Benachrichtigung dazu veranlasst werden, ggf. weitere **Vorsorge- oder Schadensabwehrmaßnahmen** zu ergreifen. Anhand des Inhalts der Benachrichtigung müssen die Betroffenen abschätzen können, von wem welche rechtswidrige Nutzung der Daten drohen könnte und was sie dagegen unternehmen können. Dafür ist es auch erforderlich, dass die Betroffenen in Kenntnis gesetzt werden, **welche konkreten Daten betroffen** sind. Es sollte eine Sprache gefunden werden, die auf die Empfänger der Benachrichtigungen abgestimmt ist. Bei den Schadensminderungsmaßnahmen sind **konkrete Handlungsempfehlungen** zu geben (z.B. Austausch von Kreditkarten/Passwörtern, Änderung von Kontonummern/Kundennummern). Es können auch **weitere Unterstützungsleistungen** (z.B. Hotlines) angeboten werden, insbesondere wenn technische Abwehrmaßnahmen einer weniger technikaffinen Gruppe von Betroffenen begreiflich zu machen sind.

Bei Betroffenen, die unter **Betreuung** stehen, muss der gesetzliche Betreuer benachrichtigt werden. Wenn die betroffene Person einsichtsfähig ist, muss auch sie über den Vorfall informiert werden.

Ggf. sind Angehörige zu benachrichtigen. Dies ist etwa der Fall, wenn abhandengekommene Angaben zu Verstorbenen zugleich personenbezogene Daten der lebenden Angehörigen darstellen.

Bei **Minderjährigen** müssen das Alter und die Reife der Betroffenen berücksichtigt werden.[23] Die Minderjährigen müssen in der Lage sein, die Tragweite und die Konsequenzen des Vorfalls selbst abschätzen zu können. Ab wann ein Minderjähriger die notwendige Einsichtsfähigkeit besitzt, kann nicht pauschal an einer Altersgrenze festgemacht werden. Es bedarf daher einer Betrachtung im Einzelfall. Als Anhaltspunkt kann davon ausgegangen werden, dass Minderjährige unter, die das 14 Jahren. Lebensjahr vollendet haben, die notwendige Einsichtsfähigkeit nicht besitzen. In diesem Fall sind nicht nur die Eltern bzw. die gesetzlichen Vertreter, sondern auch die minderjährigen Betroffenen zu benachrichtigen.

zurück

4. In welcher Form sind die Betroffenen zu benachrichtigen?

[23] Siehe WP 213 der Art. 29-Datenschutzgruppe, Stellungnahme vom 25. März 2014(bislang nur engl. Fassung): Opinion 03/2014 on Personal Data Breach Notification

Die Betroffenen sind grundsätzlich **einzeln** zu benachrichtigen. Für die Einzelbenachrichtigung schreibt das Gesetz keine besondere Form vor. Da die verantwortliche Stelle im Zweifel **nachweisen können muss**, dass sie die Betroffenen benachrichtigt hat, ist eine Benachrichtigung per (verschlüsselter) E-Mail oder per Post (soweit Adressen vorhanden sind) dringend geboten. Ob ein einfacher Brief letztlich ausreicht oder ein Einschreiben anzuraten ist, richtet sich nach den Umständen des Einzelfalls. In etwaigen Schadensersatzverfahren könnte es darauf ankommen, den **Zugang der Schreiben beweisen** zu können.

Für den Fall, dass die Benachrichtigung der Betroffenen einen **unverhältnismäßigen Aufwand** erfordern würde, ersetzt die **Information der Öffentlichkeit** die Individualbenachrichtigung. Ein unverhältnismäßiger Aufwand an Zeit und Kosten kann z.B. bei einer Vielzahl von Fällen entstehen. Darüber hinaus könnte eine Individualbenachrichtigung dann unverhältnismäßig sein, wenn die verantwortliche Stelle zunächst die Adressen der Betroffenen ermitteln muss, weil diese ihr vorher nicht bekannt waren.

Die Information der Öffentlichkeit kann durch **Anzeigen**, die mindestens eine **halbe Zeitungsseite** umfassen, in mindestens **zwei bundesweit erscheinenden Tageszeitungen** sichergestellt werden. Es kommen auch andere Formen der Veröffentlichung in Betracht. Voraussetzung ist allerdings, dass diese im Hinblick auf die Information der Betroffenen den **gleichen Wirkungsgrad** haben. Wenn die Gruppe der Betroffenen aufgrund einer bestimmten Mitgliedschaft oder aufgrund ihres Wohnortes regional eingrenzbar ist, kann die Veröffentlichung sich auf diesen Bereich (z.B. Mitgliederzeitschrift, regionale Tageszeitung) beschränken. Dabei muss das Mittel der Veröffentlichung aber eine **gleich geeignete Erreichbarkeit** der Betroffenen gewährleisten.

zurück

5. Welche Konsequenzen kann es haben, wenn die Benachrichtigung unterbleibt?

Erfolgt die Mitteilung gegenüber der Aufsichtsbehörde oder den Betroffenen aufgrund von Fahrlässigkeit oder mit Vorsatz nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig, so kann die Aufsichtsbehörde ein Bußgeldverfahren einleiten und ein Bußgeld in Höhe von bis zu 300.000 Euro erlassen (§ 43 Abs. 2 Nr. 7, Abs. 3 BDSG[24]).

zurück

6. Welche Konsequenzen ergeben sich für die interne Organisation?

Innerhalb der verantwortlichen Stellen muss sichergestellt werden, dass Sachverhalte, die eine Informationspflicht nach § 42a BDSG auslösen könnten, der **Unternehmens-/Betriebsleitung bzw. dem Vorstand unverzüglich zur Kenntnis** gelangen. Die Mitarbeiter sollten über die Informationspflicht informiert und dazu geschult werden. Es empfiehlt sich, im Rahmen einer Dienstanweisung einen **internen Meldeweg bzw. Alarmketten** festzulegen und insbesondere zu bestimmen, wer im Falle eines möglichen § 42a-Vorfalles zu benachrichtigen ist sowie wer für welche Aufgaben bei der Analyse bzw. Prüfung der Meldepflicht verantwortlich sein soll. Für **technische Sicherheitsvorfälle** sollte im IT-Sicherheitskonzept ein solches Verfahren bereits beschrieben sein. Es empfiehlt sich, eine zentrale Kontaktstelle für Meldungen von möglichen § 42a-Vorfällen zu bestimmen, da es für viele Mitarbeiter schwierig sein wird festzustellen, ob tatsächlich ein meldepflichtiger Tatbestand vorliegt. Der **betriebliche Datenschutzbeauftragte** bietet sich als Ansprechperson

[24] Siehe Anhang Punkt 13.

an, ist aber nicht die zwingende Wahl. Allerdings ist es dringend geboten, diesen bei der Analyse des Vorfalles und der Prüfung der Informationspflicht **einzubinden**. Analyse und Überprüfungen sollten **immer dokumentiert** werden. Dies gilt nicht nur für den Fall, dass die verantwortliche Stelle zu dem Ergebnis kommt, dass keine schwerwiegenden Beeinträchtigungen drohen[25]. Vielmehr muss die verantwortliche Stelle in der Lage sein, die Aufsichtsbehörde vollständig zu benachrichtigen[26] und auch eine mögliche Zurückstellung der Benachrichtigung[27] der Betroffenen zu begründen. Der Auftragsdatenverarbeiter (§ 11 BDSG[28]) sollte ebenfalls zur Mitteilung möglicher Sicherheitsvorfälle verpflichtet werden[29].

Der Datenschutzbeauftragte sollte Informationen über Anwendbarkeit und Konsequenzen des § 42a BDSG bei der Schulung der Mitarbeiter[30] berücksichtigen und auch bei seinen Datenschutzkontrollen[31] das interne Meldeverfahren zu § 42a BDSG testen.

zurück

[25] Siehe Teil A 5., Seite 7.

[26] Siehe Teil B 2., Seite 9/10.

[27] Siehe Teil B 1., Seite 8.

[28] Siehe Anhang Punkt 4.

[29] Siehe Teil A 2., Seite 2/3.

[30] Siehe Anhang Punkt 14.

[31] Siehe Anhang Punkt 14.

Anhang: Gesetzestexte und Erläuterungen

1.

§ 42a BDSG

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

[1] Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. [2] Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. [3] Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. [4] Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. [5] Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. [6] Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

zurück

2.

§ 109a TKG
Datensicherheit

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen. Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten Teilnehmer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden, hat der Anbieter des Telekommunikationsdienstes zusätzlich die Betroffenen unverzüglich von dieser Verletzung zu benachrichtigen. In Fällen, in denen in dem Sicherheitskonzept nachgewiesen wurde, dass die von der Verletzung betroffenen personenbezogenen Daten durch geeignete technische Vorkehrungen gesichert, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gespeichert wurden, ist eine Benachrichtigung nicht erforderlich. Unabhängig von Satz 3 kann die Bundesnetzagentur den Anbieter des Telekommunikationsdienstes unter Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten zu einer Benachrichtigung der Betroffenen verpflichten. Im Übrigen gilt § 42a Satz 6 des Bundesdatenschutzgesetzes entsprechend.

(2) Die Benachrichtigung an die Betroffenen muss mindestens enthalten:

1. die Art der Verletzung des Schutzes personenbezogener Daten,
2. Angaben zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind, und
3. Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen.

In der Benachrichtigung an die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat der Anbieter des Telekommunikationsdienstes zusätzlich zu den Angaben nach Satz 1 die Folgen der Verletzung des Schutzes personenbezogener Daten und die beabsichtigten oder ergriffenen Maßnahmen darzulegen.

(3) Die Anbieter der Telekommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen, das Angaben zu Folgendem enthält:

1. zu den Umständen der Verletzungen,
2. zu den Auswirkungen der Verletzungen und
3. zu den ergriffenen Abhilfemaßnahmen.

Diese Angaben müssen ausreichend sein, um der Bundesnetzagentur und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Prüfung zu ermöglichen, ob die Bestimmungen der Absätze 1 und 2 eingehalten wurden. Das Verzeichnis enthält nur die zu diesem Zweck erforderlichen Informationen und muss nicht Verletzungen berücksichtigen, die mehr als fünf Jahre zurückliegen.

(4) Vorbehaltlich technischer Durchführungsmaßnahmen der Europäischen Kommission nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG kann die Bundesnetzagentur Leitlinien vorgeben bezüglich des Formats, der Verfahrensweise und der Umstände, unter denen eine

Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten erforderlich ist.

zurück

3.

§ 15a TMG

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.

zurück

4.

§ 11 BDSG

Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen [siehe Musterformulierung[32]],

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,

   b) nichtöffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

   die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nichtöffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

zurück

5.

Musterformulierung zu § 11 Abs. 2 Nr. 8 BDSG

„Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers

[32] Siehe Anhang Punkt 5.

nach § 42a BDSG. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach § 42a BDSG zu unterstützen.“ (Quelle: Mustervereinbarung Auftrags-DV nach § 11 BDSG des Regierungspräsidiums Darmstadt; abrufbar unter http://www.datenschutz.hessen.de/mustervereinbarung_auftrag.htm)

zurück

6.

§ 3 BDSG

Weitere Begriffsbestimmungen

…

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

…

zurück

7.

§ 203 StGB

Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,

2. für den öffentlichen Dienst besonders Verpflichteten,

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,

5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder

6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist, anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfasst worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) Die Absätze 1 und 2 gelten entsprechend, wenn ein Beauftragter für den Datenschutz unbefugt ein fremdes Geheimnis im Sinne dieser Vorschriften offenbart, das einem in den Absätzen 1 und 2 Genannten in dessen beruflicher Eigenschaft anvertraut worden oder sonst bekannt geworden ist und von dem er bei der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz Kenntnis erlangt hat.

(3) Einem in Absatz 1 Nr. 3 genannten Rechtsanwalt stehen andere Mitglieder einer Rechtsanwaltskammer gleich. Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen Nachlass erlangt hat.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

zurück

8.

§ 5 BDSG

Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

zurück

9.

§ 83a SGB X

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Sozialdaten

Stellt eine in § 35 des Ersten Buches genannte Stelle fest, dass bei ihr gespeicherte besondere Arten personenbezogener Daten (§ 67 Absatz 12) unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies unverzüglich der nach § 90 des Vierten Buches zuständigen Aufsichtsbehörde, der zuständigen Datenschutzaufsichtsbehörde sowie den Betroffenen mitzuteilen. § 42a Satz 2 bis 6 des Bundesdatenschutzgesetzes gilt entsprechend.

zurück

10.

§ 32 BDSG

Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) … [2]Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

…

zurück

11.

§ 3 BDSG

Weitere Begriffsbestimmungen

...

(8) … [2]Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle.

…

zurück

12.

Zuständige Aufsichtsbehörde

Zuständig ist die Aufsichtsbehörde des Bundeslandes, in welchem die verantwortliche Stelle ihren Sitz hat. Die Kontaktdaten der einzelnen Datenschutzaufsichtsbehörden sind abrufbar unter

http://www.bfdi.bund.de/cln_134/DE/AnschriftenUndLinks/AufsBehoerdFuerDenNichtOeffBereich/AnschriftenAufsichtsbehoerdenFuerDenNichtoeffentlichenBereich.html?nn=408930 .

zurück

13.

§ 43 BDSG

Bußgeldvorschriften

…

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

…

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

zurück

14.

§ 4g BDSG

Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

…

zurück