Betrieblicher Datenschutz

Rechtshandbuch

von

Prof. Dr. Nikolaus Forgó, Prof. Dr. Marcus Helfrich, Prof. Dr. Jochen Schneider, Marian Arning, Till Baer, Benno Barnitzke, Dr. Christiane Bierekoven, Dr. Dirk Bieresborn, Prof. Dr. Georg Borges, Tobias Born, Isabell Conrad, Dr. Kai Cornelius, Dr. Eugen Ehmann, Dr. Sandro Gaycken, Dr. Uwe Günther, Dr. Nils Christian Haag, Dr. Oliver M. Habel, Dr. Stefan Hanloser, Dominik Hausen, Christian Hawellek, Joerg Heidrich, Dr. Michael Karger, Lars Klatte, JProf. Dr. Timoleon Kosmides, Dr. Jens Lütcke, Dr. Flemming Moos, Eckart C. Müller, Dr. Stephan Ott, Hans-Hermann Schild, Dr. Fabian Schmieder, Jörn Schoof, Dr. Christian Schröder, Georg F. Schröder, Dr. Axel Spies, Dr. Christoph Wegener, Hans Peter Wiesemann, Dr. Anna Zeiter

1. Auflage

Thematische Gliederung:

Datenschutz- und Melderecht

Verlag C.H. Beck München 2014

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 63468 0

Inhaltsverzeichnis: Betrieblicher Datenschutz – Forgó / Helfrich / Schneider / et al.

– ständige Aktualisierung von Verfahrensverzeichnissen,
– Bestellung eines Datenschutzbeauftragten,
– Durchführung von Mitarbeiterschulungen,
– Beschwerde- und Data-Breach-Management.

Im Einzelnen könnten die Bestandteile eines Datenschutzmanagements wie folgt aussehen:

I. Prozess: Einbindung des Datenschutzbeauftragten bei neuen Verfahren

39 **Der wichtigste Prozess** eines funktionierenden Datenschutzmanagements ist die **kommunikative Einbindung des betrieblichen Datenschutzbeauftragten** bei der Einführung oder Änderung datenschutzrelevanter Verfahren. Wenn der Datenschutzbeauftragte von solchen Vorgängen keine Kenntnis erhält, kann er diese auch nicht rechtlich prüfen und seiner Hauptaufgabe nachgehen, die in dem Hinwirken auf die Einhaltung datenschutzrechtlicher Vorgaben besteht. Ein solcher Prozess sollte vorgeben, dass bei jeder Einführung oder Änderung einer EDV-Anwendung oder eines Vorhabens, das Mitarbeiter-, Kunden- oder sonstige personenbezogene Daten betreffen könnte, der Datenschutzbeauftragte zu informieren und um eine rechtliche Stellungnahme zu bitten ist. Bereits bei der Vermutung, personenbezogene Daten könnten betroffen sein, sollte eine Information des Datenschutzbeauftragten vorgesehen sein. Kernbestandteil des Prozesses ist die Beratung des jeweiligen Mitarbeiters zu dem geplanten Vorhaben, die gleichzeitig als eine der Hauptaufgaben des Datenschutzbeauftragten zu verstehen ist. Am Abschluss steht eine rechtliche Stellungnahme und Handlungsempfehlung des Datenschutzbeauftragten, die aus Haftungsgründen dokumentiert werden sollte (telefonische Auskünfte sollten zumindest per E-Mail zusammengefasst werden).

40 Dieser Kommunikationsprozess sollte durch **regelmäßige Meetings** des Datenschutzbeauftragten mit den für ihn wichtigsten Abteilungen (insbesondere IT und HR) unterstützt werden. Auch der Betriebsrat stellt häufig eine wichtige Informationsquelle für den Datenschutzbeauftragten dar, so dass auch mit diesem ein regelmäßiger Austausch angestrebt werden sollte.

41 Voraussetzung für diese kommunikative Einbindung ist eine **starke Wahrnehmung des Datenschutzbeauftragten** im Unternehmen. Bei einem externen Datenschutzbeauftragten ist deshalb eine regelmäßige persönliche Präsenz vor Ort von großer Bedeutung. Die Wahrnehmung bei den Mitarbeitern kann zudem durch Rundmails, Schulungen und sonstige Informationen zum Thema Datenschutz verstärkt werden.

42 In **Konzernen mit mehreren Standorten,** die von einem Konzerndatenschutzbeauftragten betreut werden, bietet sich die Einsetzung sog. Datenschutzkoordinatoren an.[21] Diese stehen den Mitarbeitern des Standorts vor Ort für Datenschutzfragen zur Verfügung, sammeln Informationen für den Datenschutzbeauftragten und halten diesen auf dem Laufenden.

II. Prozess: Datenschutzrechtliche Prüfung

43 Die zum dargestellten Informationsprozess gehörende **datenschutzrechtliche Prüfung eines geplanten Vorhabens** kann auch als eigenständiger Prozess beschrieben

[21] *Gola/Schomerus,* BDSG, § 4f Rn. 8.

werden. Hierzu gehört ein rechtliches Prüfungsschema. In diesem muss zunächst die sachliche und dann die örtliche Anwendbarkeit des BDSG untersucht werden, gefolgt von der Prüfung einer Legitimation des Verfahrens durch eine Einwilligung des Betroffenen oder einen normierten Erlaubnistatbestand.[22] Als weitere Schritte sollten in dem Prozess „datenschutzrechtliche Prüfung eines geplanten Vorhabens" die **Dokumentation** dieser rechtlichen Untersuchung genannt sein sowie die Prüfung der **Erforderlichkeit einer Vorabkontrolle** und die **Aktualisierung der Verfahrensverzeichnisse.**

III. Prozess: Schulungen und Verpflichtung auf das Datengeheimnis

44 Weiterer wichtiger Bestandteil eines funktionierenden Datenschutzmanagements ist zudem die **Sensibilisierung der Mitarbeiter** für datenschutzrelevante Fragestellungen (Schaffung von „awareness"). Dabei geht es nicht darum, den Mitarbeitern juristisches Detailwissen beizubringen, das ihnen die eigenständige Lösung datenschutzrechtlicher Fragestellungen ermöglicht. Hierfür können sie sich an den Datenschutzbeauftragten wenden. Damit sie ihn aber auch tatsächliche einbinden, wenn sie mit einem datenschutzrechtlichen Problem konfrontiert werden, müssen sie es zumindest erkennen können. **Datenschutzschulungen** sollten das hierfür nötige Grundwissen vermitteln (z. B.: Was sind personenbezogene Daten?) und typische Bereiche aufzeigen (z. B. das Beauftragen externer Dienstleister). Vorrangig sind die Mitarbeiter der Abteilungen zu schulen, die am intensivsten mit personenbezogenen Daten umgehen (z. B. Personal, IT, Marketing und Kundenservice). Wenn diese ein Gespür dafür entwickelt haben, wann sie den Datenschutzbeauftragten konsultieren sollten, können viele Risiken von vornherein reduziert werden.

45 Auch für die **Verpflichtung auf das Datengeheimnis gemäß § 5 BDSG** sollte ein Prozess eingerichtet werden. Nach dieser Vorschrift sind mit der Datenverarbeitung beschäftigte Personen bei der Aufnahme ihrer Tätigkeit entsprechend zu verpflichten. Hintergrund dieser Vorgabe ist, dass zwar das Unternehmen selbst in erster Linie in der Verantwortung steht, ein datenschutzkonformes Verhalten aber nur dann möglich ist, wenn auch die einzelnen Mitarbeiter sich daran halten. Der formelle Akt der Verpflichtung nach § 5 BDSG soll ebenfalls sensibilisieren. Da die Verpflichtung „bei der Aufnahme der Tätigkeit" erfolgen muss, wird sie meist in den Prozess für neue Mitarbeiter eingebunden, den dieser an seinen ersten Tagen im Unternehmen durchläuft. Noch besser ist jedoch die Anbindung an eine Datenschutzschulung, da hier die entsprechenden Hintergründe vermittelt werden können. Dieser Ablauf sollte jedoch in den ersten Monaten der Tätigkeit erfolgen, um eine rechtzeitige Verpflichtung zu gewährleisten.

IV. Weitere Prozesse

46 Um die Einhaltung datenschutzrechtlicher Vorschriften im laufenden Betrieb sicherstellen zu können, sollten im Rahmen eines Datenschutzmanagements noch weitere Prozesse eingerichtet werden, deren weitere Erläuterungen jeweils an anderer Stelle zu finden sind:

---

[22] Ein ausführlicheres Prüfungsschema findet sich bei Leupold/Glossner/*Scheja/Haag,* Münchener Anwaltshandbuch IT-Recht, Teil 4, Rn. 66.

– **Beschwerdemanagement:**[23] Für einen optimierten Umgang mit Beschwerden zum Thema Datenschutz, aber auch zur Bearbeitung von Auskunftsersuchen gemäß § 34 BDSG;
– **Data Breach Notification:**[24] Notfallplan für den Fall schwerwiegender Datenschutzverstöße und Prüfung einer Selbstanzeigepflicht nach § 42a BDSG;
– **Archivierungs- und Löschungskonzepte;**[25]
– **IT-Sicherheitskonzepte**[26] und Notfallpläne für das Vorgehen beim Ausfall von IT-Systemen.

---

[23] Ausführlich hierzu s. *Schoof/ Spies* und *Kosmides,* XII.
[24] Checkliste für eine Selbstanzeigepflicht bei Leupold/Glossner/*Scheja/Haag,* Münchener Anwaltshandbuch IT-Recht, Teil 4, Rn. 350.
[25] Ausführlich hierzu s. *Conrad/Hansen,* III.
[26] Nach den Vorgaben der Anlage zu § 9 BDSG, ausführlich hierzu s. *Schmieder* XI.

Kapitel 3. Selbstkontrolle und Datenschutzaufsicht

Übersicht

Literatur: *Büllesbach,* Transnationalität und Datenschutz – Die Verbindlichkeit von Unternehmensregelungen, Baden-Baden 2008 (Diss.); *Dzida/Schütt,* Arbeitnehmerdatenschutz: Rechte und Pflichten des Betriebsrats, ArbRB 2012, 21; *Ehmann,* Datenschutzkontrolle beim Betriebsrat, CR 1998, 331; *Gola,* Aus den aktuellen Tätigkeitsberichten der Aufsichtsbehörden, RDV 2012, 136; *Gola/Schomerus,* Kommentar zum BDSG, 11. Aufl., München 2012; *Grapentin,* Datenschutz und Globalisierung – Binding Corporate Rules als Lösung?, CR 2009, 693; *Heil,* Privacy Policies, Binding Corporate Rules (BCR) und verbindliche Unternehmensregelungen, DuD 2009, 228; *Hornung,* Informationen über „Datenpannen“ – Neue Pflichten für datenverarbeitende Unternehmen, NJW 2010, 1841; *Jaspers,* Die EU-Datenschutz-Grundverordnung, DuD 2012, 571; *Jaspers/Reif,* Der betriebliche Datenschutzbeauftragte nach der geplanten EU-Datenschutz-Grundverordnung – ein Vergleich mit dem BDSG, RDV 2012, 78; *Kort,* Die Stellung des Betriebsrats im System des Beschäftigtendatenschutzes, RDV 2012, 8; *Roßnagel,* Datenschutz in globalen Netzen, DuD 1999, 253; *Schröder,* Die Haftung für Verstöße gegen privacy policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, Baden-Baden 2007; *Simitis* (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011 (zit. Simitis/*Bearbeiter*); *Simonet,* Die Implementierung interner Whistleblowingsysteme im Rahmen der Corporate Governance, Berlin 2012; *Thüsing,* Beschäftigtendatenschutz auf der Zielgeraden?, BB 2013, Heft 5 I; *Wybitul,* Beschäftigtendatenschutz 2013 – und wenn er nicht gestorben ist, ZD 2013, 97; *ders.,* Whistleblowing – datenschutzkonformer Einsatz von Hinweisgebersystemen?, ZD 2011, 118.

A. Allgemeines, Aufgaben

1 Der **betriebliche Datenschutzbeauftragte** (Beauftragter für den Datenschutz gemäß § 4f BDSG), s. *Haag,* II.1, ist als ein wichtiges Element der sog. **Selbstkontrolle**[1] des Unternehmens, das als datenverarbeitende Stelle dem BDSG unterliegt, zu sehen. In gewissem Sinne das Gegenstück dazu oder die **zweite Stufe** der Kontrolle, nun von außen, stellt die Aufsicht durch die Datenschutzaufsichtsbehörden als Fremdkontrolle, geregelt in § 38 BDSG, dar.

[1] Simitis/*Simitis,* BDSG, Einleitung Rn. 109 ff.

Ziel ist es, „an der Quelle", also dort, wo die Datenverarbeitung geschieht und wo Kenntnisse über deren Gründe und Umfang vorhanden sind, eine niederschwellig operierende, ***interne Kontrolle*** einzuführen. **2**

Die Idee ist derzeit weder europarechtlich vorgegeben noch flächendeckend verbreitet: Die **RL 95/46/EG** kennt das Institut nicht als Verpflichtung und schon in Österreich ist es (weiterhin) unbekannt. Veränderungen mögen mit der Datenschutzgrundverordnung eintreten[2], die das Institut des Datenschutzbeauftragten vorsieht, allerdings – insoweit schon kritisiert[3] – evtl. (s. auch Rn. 30) erst ab einer Unternehmensgröße von mehr als 250 Mitarbeitern (Art. 35 Abs. 1 DS-GVO (E)). **3**

Nach dem BDSG ist das Konzept relativ klar und nachvollziehbar, wonach es eine „interne" Kontrolle durch den Beauftragten für den Datenschutz gibt, darüber hinaus die nächste Stufe mit externer Kontrolle durch die Aufsichtsbehörde. Gemäß DSRL 95/46/EG erfolgt die Kontrolle primär und allein durch eine Kontrollstelle (Art. 28), ergeben sich jedoch Erleichterungen bei Meldepflichten und Vorabkontrolle durch Bestellung eines „Datenschutzbeauftragten" (Art. 18 Abs. 2 und Art. 20 Abs. 2). Durch die **DS-GVO** würde dieses Prinzip bis zu einem gewissen Grade aufgegeben. Zum einen sind die Bestellungsvoraussetzungen andere. Insbesondere ist ein Beauftragter erst ab einer Größenordnung vorgesehen, die deutlich über den Bestellungsvoraussetzungen des bislang geltenden BDSG liegt. Zum anderen erhält die Aufsichtsbehörde und insbesondere dann die Kommission als zusätzliche Aufsicht erheblich weiter gefasste Kompetenzen bzw. Eingriffsmöglichkeiten. Insofern wird die Aufsicht erheblich gestärkt, die Selbstkontrolle wohl eher abgebaut. **4**

Die Kontrolle durch die Aufsichtsbehörde greift bei solchen Stellen, die personenbezogene Daten automatisiert verarbeiten oder die die Verarbeitung oder Nutzung in oder aus nicht automatisierten Dateien vornehmen (§ 38 Abs. 1 Satz 1 BDSG).[4] Damit ist ein gewisser Unterschied im Geltungsbereich der beiden Kontrollen festzustellen. Nach § 4f BDSG ist der Beauftragte für den Datenschutz durch die Stellen zu bestellen, die personenbezogene Daten automatisiert verarbeiten.[5] In der Praxis dürften diese Unterscheidungen aber kaum eine Rolle spielen, vielmehr von einer gewissen Deckungsgleichheit des Bereichs der Selbstkontrolle und auch der Datenschutzaufsicht anzugehen sein. **5**

Die Pflicht zur Bestellung eines Beauftragten für den Datenschutz besteht für **nichtöffentliche Stellen** bei automatisierter Verarbeitung personenbezogener Daten ab einer Zahl von neun Personen, die ständig mit der automatisierten Verarbeitung beschäftigt sind, ansonsten, wenn mindestens zwanzig Personen in der Regel mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind. Der Beauftragte für den Datenschutz ist schriftlich zu bestellen (§ 4f Abs. 1 Satz 1 BDSG). Bestellt werden darf nur, wer die erforderliche **Zuverlässigkeit** und **Fachkunde** besitzt (§ 4f Abs. 2 Satz 1 BDSG). Es muss sich nicht zwingend um einen Beschäftigten der verantwortlichen Stelle handeln, die Aufgabe kann auch auf einen externen Datenschutzbeauftragten ausgelagert werden. **6**

---

[2] Entwurf v. 25.1.2012; s. auch *Forgó*, I.3.

[3] S. auch Stellungnahme des BITKOM unter http://www.bitkom.org/de/themen/50792_62145.aspx (Stand: 8/2013); *Jaspers/Reif*, RDV 2012, 8.

[4] Zu den Aktivitäten der Aufsichtsbehörden und deren Themen s. *Gola*, RDV 2012, 136.

[5] S. zur Bestellung *Haag*, II.1.

7 **Selbstkontrolle** heißt hinsichtlich des betrieblichen Datenschutzbeauftragten nicht, dass nur wirklich Angestellte diese Aufgabe erfüllen können. Vielmehr können zum einen dies Angestellte ohnehin als Nebentätigkeit ausüben, sodann aber auch Externe, wie das BDSG ausdrücklich klarstellt (§ 4f Abs. 2 Satz 3, 1. Hs. BDSG). Allerdings wird bei Externen besonderes Augenmerk auf die Wahrung deren Unabhängigkeit und auch auf die Einhaltung des Benachteiligungsverbots § 4f Abs. 3 Satz 3 BDSG zu legen sein.

8 Nach § 4d BDSG bestehen **Meldepflichten** hinsichtlich automatisierter Verarbeitungen vor Inbetriebnahme an die zuständige Aufsichtsbehörde, deren Inhalt § 4e BDSG festlegt. Diese entfallen, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat (§ 4d Abs. 2 BDSG).

9 Nach § 4d Abs. 6 BDSG ist der Beauftragte für den Datenschutz zudem für die **Vorabkontrolle zuständig,** was bedeutet, dass solche Unternehmen, die eine Vorabkontrolle durchzuführen haben, unabhängig von der Zahl der Mitarbeiter einen Datenschutzbeauftragten zu bestellen haben. Die Vorabkontrolle ist vorzunehmen, „soweit automatisierte Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen" **(§ 4d Abs. 5 Satz 1 BDSG).** Dies ist insbesondere bei der Verarbeitung von **„besonderen Arten personenbezogener Daten"** i. S. d. § 3 Abs. 9 BDSG sowie bei Verarbeitung zu Zwecken der Bewertung oder Fähigkeiten, der Leistung oder des Verhaltens des Betroffenen anzunehmen (§ 4d Abs. 5 Satz 2 BDSG). Auch diese Vorabkontrolle ist ein Teil der „Selbstkontrolle".

B. Verhältnis der beiden Einrichtungen zueinander

I. Unterstützung des Beauftragten

10 Die beiden Ebenen Selbstkontrolle und Datenschutzaufsicht arbeiten nach dem Willen des Gesetzgebers **„Hand in Hand".** Das Gesetz drückt dies so aus, dass nach § 4g Abs. 1 Satz 2 BDSG der Beauftragte für den Datenschutz in *Zweifelsfällen* sich an die für die Datenschutzkontrolle zuständige Behörde wenden kann.

11 Diese **Zweifelsfälle** liegen nicht nur in jenen Fällen vor, in denen der Datenschutzbeauftragte die Vertretung datenschutzrechtlicher Vorschriften vermutet. Der Gesetzgeber sieht die Aufsichtsbehörde hier vor allen Dingen auch in einer **unterstützenden Funktion.** Zwar muss der Datenschutzbeauftragte über ein hinreichendes Maß an **Fachkunde** verfügen (§ 4f Abs. 2 Satz 1 und 2 BDSG), um die ihm gesetzlich obliegenden Aufgaben erfüllen zu können. Gleichwohl geht auch das Gesetz davon aus, dass sich der Datenschutzbeauftragte vor allen Dingen in der Querschnittsmaterie von Recht und Informationstechnologie im Einzelfall auf **externe Kompetenzen** stützen können muss.[6]

12 Nach § 4g Abs. 1 Satz 3 BDSG kann er die **Beratung** nach § 38 Abs. 1 Satz 2 BDSG durch die Aufsichtsbehörde in Anspruch nehmen. Diese Beratung nach § 38 Abs. 1 Satz 2 BDSG sieht vor, dass die Aufsichtsbehörde die Beauftragten für den Datenschutz und die verantwortliche Stelle mit Rücksicht auf deren Bedürfnisse „berät und unterstützt". Die Informationspflicht bei Datenpannen (§ 42a BDSG, s.

[6] Nachdem sogar insgesamt ein Externer ausdrücklich als Datenschutzbeauftragter bestellt werden darf, § 4f Abs. 2 Satz 3 BDSG; s. auch Simitis/*Simitis,* BDSG, § 4f Rn. 742 ff. hinsichtlich der Unterstützungspflicht der verantwortlichen Stelle.

Schoof, XII.1 Rn. 2 ff.) kann man als Schnittstelle für das Verhältnis zur Aufsichtsbehörde sehen.[7]

II. Befugnis der Aufsichtsbehörde zu Anordnungen

Es ist gleichzeitig festzuhalten, dass die Aufsichtsbehörde ganz erhebliche Befugnisse hat, die im Laufe der Zeit – zuletzt im Jahr 2009 – im BDSG noch verstärkt wurden. **13**

Nach § 38 Abs. 5 BDSG kann die **Aufsichtsbehörde** zur Gewährleistung der Einhaltung des BDSG und anderer Vorschriften über die Datenschutzmaßnahmen die **Beseitigung festgestellter Verstöße** bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel **anordnen**. Bei schwerwiegenden Verstößen oder Mängeln kann dies auch zu einer **Untersagung** der Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren führen, „wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 oder trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden" (§ 38 Abs. 5 Satz 2 BDSG). **14**

III. Abberufung

Die Aufsichtsbehörde kann sogar die **Abberufung** des Beauftragten für den Datenschutz verlangen, wenn dieser die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt (§ 38 Abs. 5 Satz 3 BDSG). Die Befugnisse der Aufsichtsbehörde richten sich naturgemäß nicht gegen den Beauftragten für den Datenschutz, sondern die der Kontrolle unterliegenden Stellen, also gegen das zu kontrollierende Unternehmen. Etwaige Auskunftsverlangen, wie sie nach § 38 Abs. 3 BDSG vorgesehen sind, beantwortet demnach nicht der Datenschutzbeauftragte, sondern die datenverarbeitende Stelle (Unternehmen) selbst. **15**

IV. Betretungsrechte

Der Aufsichtsbehörde stehen zudem nach § 38 Abs. 4 BDSG **Betretungsrechte** in Verbindung mit **Prüfungs- und Besichtigungsrechten** – während der Betriebs- und Geschäftszeiten[8] – zu. **16**

Eine sehr wichtige Funktion übt die Aufsichtsbehörde insofern noch aus, als sie der Adressat der verpflichtend zu erteilenden Informationen bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a BDSG ist (**data breach notification**). **17**

Diese Informationspflicht setzt voraus, dass schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des Betroffenen drohen. Das Verfahren, nach dem vorzugehen ist, ist in § 42a Satz 2 bis 5 BDSG geregelt. Satz 1 sieht insoweit vor, dass unverzüglich der zuständigen Aufsichtsbehörde sowie dem Betroffenen das Vorliegen eines solchen Falles mitzuteilen ist.[9] **18**

Allerdings hat die Benachrichtigung des Betroffenen erst dann unverzüglich zu erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden **19**

[7] Informationspflichtig ist die verantwortliche Stelle, der bDSB wird die Beachtung zu organisieren und zu prüfen haben; s. auch Rn. 17 f.

[8] *Gola/Schomerus,* BDSG, § 38 Rn. 22.

[9] Am 25.8.2013 trat die EU-VO zur Meldepflicht von Datenpannen und Datendiebstahl in Kraft – mit 24-Stunden-Frist für Internet-Provider und Telekommunikationsanbieter.

oder nicht unverzüglich erfolgt sind und die Strafverfolgung durch die Mitteilung nicht mehr gefährdet wird (Satz 2).

20 Diese Vorschrift gilt auch im Falle der Verarbeitung im Auftrag durch einen Auftragnehmer. Der Auftraggeber bleibt für die entsprechende Informationspflicht verantwortlich.[10]

C. Weitere Formen der Selbstkontrolle und der Fremdkontrolle

I. Audit

21 Eine weitere Form von Selbstkontrolle stellt das Datenschutzaudit dar. § 9a BDSG sieht ein freiwilliges Datenschutzaudit vor, ohne jedoch die näheren Regelungen wie dies genau zu vollziehen wäre, anzugeben.[11]

22 Die Frage, die sich bei stärkerer Gewichtung des Datenschutzaudits auch in der Praxis stellen würde, was allerdings bislang regelmäßig nicht der Fall ist, stellt auf das Verhältnis der Funktion des Datenschutzaudits zum betrieblichen Beauftragten einerseits und zur Aufsichtsbehörde andererseits ab. Die Frage ist also, ob es sich hier um eine Art **„Mittelstufe"** zwischen der internen **Selbstkontrolle** und der externen Aufsicht handelt, oder ob nicht in gewissem Sinne die betriebliche **Selbstkontrolle** insoweit **beschränkt** wird.

23 In diesem Zusammenhang ist darauf hinzuweisen, dass man diese zusätzliche Option vereinzelt auch als **„überobligatorischen Datenschutz"** ansieht, nachdem die Gesetzesbegründung ihrerseits das Ziel angibt, „datenschutzfreundliche" Produkte zu fördern.[12] Insoweit besteht einerseits eine gewisse Parallelität zur **Überprüfung von IT-Produkten** im Hinblick auf die Sicherheit durch das BSI. Andererseits wird aber auch das Defizit an Prüfkriterien im Bereich des Datenschutzes deutlich, da weder im Gesetz noch in sonstiger Weise einheitliche und klare Auditkriterien bestehen.

24 Nicht zu übersehen ist das Problem, dass naturgemäß bei einer Auditierung auch **der Datenschutzbeauftragte** mit **auditiert** wird. Dies mag im Hinblick auf die Feststellung von dessen Fachkunde und eventuell auch Zuverlässigkeit durchaus vertretbar sein. Eine solche „Mit-Auditierung" übersieht aber, dass der interne Beauftragte zwar einerseits in der Ausübung seiner Pflichten unabhängig ist, gleichzeitig aber innerhalb des Unternehmens aus seiner Rolle als Datenschutzbeauftragter heraus keine Weisungsbefugnis hat.

25 Bei der Auditierung müsste folglich strikt zwischen dem Ergebnis, wie es die Geschäftsleitung letztlich hergestellt hat, und den Beratungsleistungen des Beauftragten, auch wenn diese nicht umgesetzt wurden, **unterschieden** werden, um der gesetzlichen Stellung des Datenschutzbeauftragten Rechnung zu tragen.

26 Für die Stellung des Datenschutzbeauftragten könnte dies zu einer besonders **misslichen Situation** führen, da die Auditierung zur Offenlegung von Diskrepanzen zwischen dem Datenschutzbeauftragten und der Geschäftsleitung führt.

---

[10] *Gola/Schomerus,* BDSG, § 42a Rn. 2 unter Hinweis u. a. auf *Hornung,* NJW 2010, 1841.

[11] Zum Datenschutzaudit s. auch *Haag,* II.2. Rn. 10 ff. und *Schneider,* II.4 Rn. 12; Simitis/*Scholz,* BDSG, § 9a: Das Ausführungsgesetz ist weiterhin nicht existent.

[12] Hierauf weisen *Gola/Schomerus,* BDSG, § 9a Rn. 7 unter Bezugnahme auf BR-Drs. 461/00, S. 18, hin.