Audit des internen Datenschutzmanagements

Beschäftigtendatenschutz auf dem Prüfstand

Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen
Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel

Hier lesen Sie

- wie Interessenvertreter das Datenschutzmanagement überprüfen können
- welche Fragen sie stellen und wie sie ein solches Audit vor Ort gestalten sollten
- welche Handlungsfelder und Probleme dabei in der Praxis häufig auftreten

Betriebs- und Personalräte haben den Arbeitnehmerdatenschutz und die Arbeit der Datenschutzbeauftragten zu überwachen. Für diese verantwortungsvollen Aufgaben benötigen sie einen Leitfaden, der sie beim Überprüfen des internen Datenschutzmanagements in Unternehmen und Behörden unterstützt. Dieser Beitrag gibt Interessenvertretern eine Checkliste an die Hand, mit der sie die betriebliche Organisation des Datenschutzes sowie auch die Qualität der Aufgabenerfüllung des Datenschutzbeauftragten einfach kontrollieren können. So ausgerüstet ist ein Audit des Datenschutzmanagements gemeinsam mit den Verantwortlichen ohne größeren Aufwand möglich.

Ein nicht sachgemäßer Umgang mit Daten in Betrieben und Dienststellen kann weitreichende Folgen wie die Demotivation der Mitarbeiter, Bußgelder, Reputationsschädigungen oder der Verlust von Kundenbindung haben. Hier kann ein Audit durch Arbeitnehmervertretungen präventiv wirken und bei der praktischen Umsetzung des Datenschutzes unterstützend wirken. Sollten bei der Überprüfung Defizite im Datenschutzmanagement erkennbar werden, können konkrete Maßnahmen wie beispielsweise Beratung durch die Aufsichtsbehörde, Nachschulung des Datenschutzbeauftragten, die Schaffung neuer Strukturen, Änderung der Prozesse oder gegebenenfalls die Einschaltung externer Berater unternommen werden.

Überprüfen des Datenschutzmanagements

Betriebsräte und betriebliche Datenschutzbeauftragte sind verantwortlich für die Umsetzung des Beschäftigtendatenschutzes.[1] Sie bilden zwei Säulen einer internen Datenschutzkontrolle. Betriebsräte haben das Recht, den Stand des Beschäftigtendatenschutzes zu überprüfen, auch wenn es sich dabei um eine Kontrolle der Arbeit des betrieblichen Datenschutzbeauftragten handelt.

Das hier vorgeschlagene Audit soll grundsätzlich dazu dienen, mit dem Datenschutzbeauftragten und weiteren Verantwortlichen für den Datenschutz im Unternehmen ins Gespräch zu kommen und die vom Bundesdatenschutzgesetz (BDSG) gewollte Kooperation zu praktizieren. Bei fehlenden oder nicht ordnungsgemäßen Bestandteilen des Datenschutzmanagements kann zudem eine Unterstützung für den Datenschutzbeauftragten durch die Interessenvertretung nur hilfreich sein. Das gilt etwa dann, wenn eine Prüfung durch die Aufsichtsbehörde für den Datenschutz ansteht.

Die Audit-Checkliste lässt sich beispielsweise für schriftliche Anfragen an die Leitung der verantwortlichen Stelle oder an den Datenschutzbeauftragten nutzen. Sie kann auch für mündliche Befragungen des Beauftragten, der Leitung oder der Mitarbeiter der IT- und Perso-

1 Nachfolgend wird Bezug auf Betriebsräte und das Betriebsverfassungsgesetz genommen.

nalabteilung, des Rechnungswesens, von Vertrieb/Marketing oder der Revision eingesetzt werden.

Das Audit sollte sich zunächst auf die jeweilige Datenschutzorganisation konzentrieren, das heißt auf vorhandene Strukturen und formalisierte Prozesse, die zur Umsetzung der gesetzlichen Anforderungen des Datenschutzes eingerichtet sind. Im Sinne eines Regelkreises ist der jeweilige betriebliche Ist-Stand des Beschäftigtendatenschutzes festzustellen, mit dem geforderten rechtlichen Soll-Zustand zu vergleichen und das Datenschutzmanagementsystem kontinuierlich zu verbessern. Bei der Nutzung der Checkliste ist festzuhalten, ob die jeweilige Anforderung, Rahmenbedingung oder Aufgabe erfüllt ist oder für das Unternehmen nicht zutrifft. An jeder Beantwortung der Fragen sollten sich Bemerkungen anschließen, die auf weiterführende Maßnahmen verweisen. Die vorgeschlagene Checkliste ab Seite 29 beschränkt sich auf wesentliche Problemfelder des Beschäftigtendatenschutzes.

Prioritäten einer Audit-Planung

Für ein gelingendes Datenschutzmanagement sind schriftliche Unterlagen unverzichtbar. Insofern ist in einem Audit nachzufragen, welche zum Datenschutzmanagement vorhanden und im Betrieb bekanntgemacht gemacht worden sind. Hierzu gehören unter anderem eine Datenschutzrichtlinie, ein Datenschutzkonzept und Jahresberichte des Datenschutzbeauftragten. Es ist von einer Berichtspflicht des Beauftragten auszugehen, da dieser bei einer Kontrolle durch die Aufsichtsbehörde nachweisen muss, dass er seine gesetzlichen Aufgaben erfüllt.[2]

Betriebsräte haben nach § 80 Abs. 2 BetrVG ein Recht, die genannten Unterlagen zu erhalten. Ihre klare Zuständigkeit für den Beschäftigtendatenschutz und ihre Aufgabe, technische Kontrolleinrichtungen gleichberechtigt mitzubestimmen, begründen ihren Anspruch.

In der Praxis stellt sich oft die Frage, wann es sich bei der Verarbeitung von Beschäftigtendaten um besondere Arten von Daten gemäß § 3 Abs. 9 BDSG handelt. Damit sind sensible Daten gemeint, die besondere Risiken bei der Datenerhebung, -verarbeitung und -nutzung mit sich bringen können. Im Bereich des Beschäftigtendatenschutzes sind es etwa Daten aus Videoüberwachungen, Psychotestdaten, Daten aus dem betrieblichen Eingliederungsmanagement oder aus Krankenrückkehrgesprächen und medizinische Daten des Betriebsarztes.

Besondere Risiken für Beschäftigte

Bei der Planung, Einrichtung, dem Betrieb und der Außerbetriebnahme von automatisierten Verfahren, in denen derartige Daten verarbeitet werden, ist der betriebliche Datenschutzbeauftragte präventiv heranzuziehen und von ihm eine Vorabkontrolle durchzuführen. Dies gilt auch dann, wenn es um die Einführung neuer Technologien wie Chipkarten oder Smartphones geht, die besondere Risiken für das informationelle Selbstbestimmungsrecht der Beschäftigten mit sich bringen.[3]

Es kommt wiederholt vor, dass die Brisanz der Verarbeitung besonderer Arten von Daten – speziell von Gesundheitsdaten – bei der Aufnahme in das Verfahrensverzeichnis nicht erkannt, die Vorabkontrolle als wichtiger Schritt der Zulässigkeitsprüfung von automatisierten Verfahren nicht durchgeführt wird und dem Datenschutzbeauftragten für diese Aufgabe keine geprüften Formulare zur Verfügung stehen.[4]

Die Entscheidung darüber, ob eine Vorabkontrolle zum Beispiel bei der Einführung von dienstlichen Tablets oder der Nutzung von privaten Smartphones durchgeführt werden muss, ist oft schwierig. Deshalb gehen Unternehmen dazu über, generell bei neuen IKT-Verfahren eine Vorabkontrolle durchzuführen.

2 Gesellschaft für Datenschutz und Datensicherheit (GDD), Datensicherheit im Unternehmen, 4. Auflage 2010, 136: Der Tätigkeitsbericht ist der Aufsichtsbehörde vorzulegen; Caster, Datenschutzaudit nach BSI Grundschutz, CD-ROM – Version 1.0, 2011, Einführungstext, 40; ablehnend: Jaspers/Greif, Der betriebliche Datenschutzbeauftragte nach der geplanten EU-Datenschutz-Grundverordnung – ein Vergleich mit dem BDSG, in: RDV 2012, 78 ff. (82)

3 Simitis-Petri, BDSG, 7. Auflage, § 4d Rn. 35

4 Brink, Der betriebliche Datenschutzbeauftragte – eine Annäherung, in: ZD 2012, 55 ff. (58)

In diesem Zusammenhang müssen Datenschutzbeauftragte in Unternehmen der Privatwirtschaft Richtlinien für Datenabflüsse und Datenpannen nach § 42 a BDSG erlassen, da seit 2009 eine Veröffentlichungspflicht besteht, wenn bei einer Datenpanne sensible Daten betroffen sind.[5]

IKT-Mitbenutzung durch externe Dritte

Interessenvertretungen müssen wissen, inwieweit Dritte die Hard- und Software des Unternehmens nutzen und/oder gegebenenfalls personenbezogene Daten der Beschäftigten erheben, verarbeiten und nutzen. Hier geht es um die Verarbeitung von Daten durch Dritte. Dabei kann es sich um Auftragsdatenverarbeitung, gegebenenfalls um Funktionsübertragung oder um Fernwartung handeln, für die es Verträge geben muss. Oftmals handelt es sich um die ausgelagerte IT-Abteilung, externe Personaldienstleister für die Lohn- und Gehaltsabrechnung, Berater, Fernwartungsfirmen etwa für die TK-Anlage oder Auskunfteien und Detektive.

Zur Kontrolle der einschlägigen Betriebsvereinbarungen sind Belegschaftsvertretern die Verträge zur Auftragsdatenverarbeitung nach § 11 BDSG vorzulegen. Kontrollmöglichkeiten des Arbeitgebers, des Datenschutzbeauftragten oder des Betriebsrats sind darin in der Regel jedoch nicht vorgesehen.

Betriebsräte benötigen die Verträge, um ihre Aufgabenerfüllung nach § 80 Abs. 1 Nr. 1 und § 87 Abs. 1 Nr. 6 BetrVG wahrzunehmen. Ihre Kontrollmöglichkeiten dürfen durch die Datenverarbeitung bei Dritten nicht eingeschränkt werden. Sie müssen überprüfen können, ob die gesetzlichen Vorgaben unter anderem des § 11 BDSG eingehalten werden. Interessenvertretungen sollten zudem wissen, dass es für derartige ausgelagerte Datenverarbeitungen Musterverträge gibt.

Datenschutzregelungen für IT-Abteilung

Administratoren haben die technischen Mittel und das Know-how, heimliche Überwachungen durchzuführen. Betriebsräte befürchten oft, dass Administratoren sich nicht an Betriebsvereinbarungen und Datenschutzregelungen halten, wenn sie von Vorgesetzten eine nichtmitbestimmte Anweisung zur Kontrolle erhalten.

Berichte über Datenschutzskandale und Kündigungsschutzprozesse von Administratoren[6] zeigen, dass für die Prävention unzulässiger Kontrollen Vorkehrungen erforderlich sind. Insofern sollte im Audit gefragt werden, welche Maßnahmen vorbeugend im Hinblick auf die IT-Abteilung ergriffen worden sind, um Administratoren vor solchen Zwangslagen, Abmahnungen, Kündigungen und unbedachtem Handeln zu schützen.

Überblick über Hard- und Software

Datenschutz und Datensicherheit gehören untrennbar zusammen. Insofern sind Regelungen für die Beschaffung und Verfügbarkeit von Hard- und Software im Datenschutzmanagement unerlässlich.

Sowohl der Datenschutzbeauftragte als auch der Betriebsrat müssen den Überblick haben, welche Geräte und welche Programme eingesetzt werden. Das kann unter anderem durch ein Bestandsverzeichnis geschehen und im Verfahrensverzeichnis nach den §§ 4 e und 4 g Abs. 2 BDSG dokumentiert werden.

Erforderlich ist eine klare Positionierung der Betriebsparteien, inwieweit private Geräte mitgebracht und für dienstliche Zwecke genutzt werden dürfen (»BYOD«: Bring Your Own Device).[7]

Anforderungen an Datenschutzbeauftragte

Der Düsseldorfer Kreis hat im Jahr 2010 rechtliche Anforderungen für die Privatwirtschaft aufgestellt[8], welche Rahmenbedingungen erfüllt und konkreten Eigenschaften und Fähigkeiten Datenschutzbeauftragte mitbringen müssen, damit sie die gesetzlichen Vorgaben zur Zuverlässigkeit und Fachkunde erfüllen.[9] Unternehmen müssen zum Beispiel einen Datenschutzbeauftragten bestellen, wenn es mehr als neun Personen mit der automatisierten Datenverarbeitung oder 20 oder mehr Personen bei der nichtautomatisierten Datenverarbeitung beschäftigt.[10]

In der Einleitung des Beschlusses weisen die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich daraufhin, dass Fachkunde und Rahmenbedingungen für den Datenschutzbeauftragten in den verantwortlichen Stellen »nicht durchgängig den Anforderungen des BDSG genügen«. Das bedeutet, dass vielfach klar gegen gesetzliche Vorgaben des BDSG verstoßen und deshalb eine Konkretisierung der rechtlichen Anforderungen durch den Düsseldorfer Kreis notwendig wurde.

Ausgewiesene Fachkunde

Die notwendige Fachkunde ist abhängig von der Art und dem Umfang der Datenverarbeitung und vom Schutzbedarf der personenbezogenen Daten.

In Beratungen fragen Betriebsräte oft, wann die rechtlichen, technischen und organisatorischen Mindestkenntnisse als angemessene Fachkunde des Datenschutzbeauftragten vorhanden sein müssen. Nach dem Beschluss müssen diese grundsätzlich bereits zum Zeitpunkt seiner Bestellung in ausreichendem Maße vorliegen.

Interne Datenschutzbeauftragte müssen zudem Fortbildungsmaßnahmen besuchen und gegebenenfalls vorhandene Wissens- und Informationsdefizite nach ihrer Bestellung abbauen. Darauf haben sie seit 2009 einen durchsetzbaren Rechtsanspruch. Der Arbeitgeber hat die anfallenden Kosten zu tragen und ihn dafür freizustellen. Bei externen Datenschutzbeauftragten kann die Fortbildung Bestandteil der Vergütung sein.[11]

5 Gliss, Datenabfluss und Datenschutzpannen: Veröffentlichungspflicht nach § 42a BDSG, in: DSB 12/2009, 11

6 LAG Köln vom 14.5.2010, Az.: 4 Sa 1257/09, dazu Pröpper, EDV-Admin – kein Schnüffeln!, in: CuA 12/2010, 11 ff.

7 Siehe dazu Brandt, BYOD – Handlungsbedarf für die Belegschaftsvertretung, in: CuA 10/2011, 8 ff.

8 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 24./25.11.2010): Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 BDSG, www.datenschutz.rlp.de

9 Zur Zuverlässigkeit von Betriebsräten Schierbaum, in: CuA 2/2013, 32 ff.; zu den rechtlichen Voraussetzungen einer Bestellung Hoeren, Der betriebliche Datenschutzbeauftragte, in: ZD 2012, 355

10 Wybitul, Anforderungen an betriebliche Datenschutzbeauftragte, in: MMR 2011, 372

11 Düsseldorfer Kreis, aaO., III. 3

Interessenvertretung: Audit-Checkliste für das interne Datenschutzmanagement (Auszug)

1. Schriftliche Regeln und Unterlagen zum Beschäftigtendatenschutz

- Liegen dem Datenschutzbeauftragten alle Betriebsvereinbarungen zur Einführung und Anwendung technischer Kontrolleinrichtungen vor und sind diese auf dem aktuellen Stand geführt?
- Gibt es Arbeits-/Verfahrensanweisungen für den Prozess der Einführung und Änderung automatisierter Verfahren, die sich unter anderem an die IT-Abteilung, den Vertrieb oder an die Personalabteilung richten?
- Existiert für alle Mitarbeiter und Führungskräfte eine verbindliche Datenschutzrichtlinie (oft auch Datenschutzordnung genannt)?
- Liegt eine Datenschutzanweisung – gegebenenfalls in Einzelregelungen – vor, die ein umzusetzendes Datenschutzkonzept beschreibt?
- Sind Strukturen und Prozesse im betrieblichen Datenschutzmanagement unter Berücksichtigung des Beschäftigtendatenschutzes beschrieben?
- Liegen konkrete Arbeitsanweisungen/Richtlinien/Merkblätter/Konzepte zum Datenschutz und zur Datensicherheit vor?
- Ist das Verfahrensverzeichnis von der IT-Abteilung vollständig erstellt, wird es vom Datenschutzbeauftragten aktuell geführt und überprüft dieser jährlich die Aktualität des Verfahrensverzeichnisses?
- Liegt eine schriftliche Richtlinie für den rechtskonformen Umgang mit »Datenabfluss und Datenpannen« nach § 42a BDSG vor und ist der Datenschutzbeauftragte dabei eingebunden?

2. Sensible personenbezogene Daten, Vorabkontrolle

- Werden sensible Daten der Beschäftigten gemäß § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt und automatisierte Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Mitarbeiter oder der Kunden des Unternehmens aufweisen, vorab vom Datenschutzbeauftragten kontrolliert?
- Ist die Bedeutung von besonders sensiblen Daten zum Beispiel in der IT-Abteilung, Personalabteilung, im Rechnungswesen oder im Vertrieb bekannt?
- Sind Vorabkontrollen durchgeführt und ausreichend dokumentiert worden?
- Ist die Notwendigkeit einer Vorabkontrolle in bestimmten Fällen der Datenverarbeitung allen Verantwortlichen bekannt und ein Meldewesen an den Datenschutzbeauftragten eingerichtet, damit er die Zulässigkeit prüfen kann?
- Ist schriftlich festgehalten worden, wann eine Vorabkontrolle erforderlich und durchzuführen ist?
- Erhält der Datenschutzbeauftragte rechtzeitig, das heißt zur Beginn der Planungsphase eines IT-Projekts, alle erforderlichen Unterlagen für eine eventuell erforderliche Vorabkontrolle nach § 4d BDSG?
- Kann der Datenschutzbeauftragte in Zweifelsfällen bei der Vorabkontrolle die zuständige Aufsichtsbehörde kontaktieren?
- Ist der Umgang mit »Datenpannen« nach § 42a BDSG als Verfahrensanweisung geregelt und der Datenschutzbeauftragte eingebunden?

3. Mitbenutzung der Informations- und Kommunikationstechniken durch Fremdfirmen

- Gibt es eine Liste der Auftragnehmer nach § 11 BDSG »Auftragsdatenverarbeitung«?
- Liegen Auftragsdatenverarbeitung, Funktionsübertragung an Fremdfirmen oder Fernwartung vor?
- Gibt es für Fernwartung interne schriftliche Regeln?
- Sind Drittfirmen vor Aufnahme ihrer Tätigkeit anhand von Zertifikaten sorgfältig überprüft und unter Einbindung des Datenschutzbeauftragten ausgewählt worden?
- Werden Kontrollen der Datenverarbeitung in Form eines Audits während der Auftragsdatenverarbeitung vom Arbeitgeber durchgeführt, dokumentiert und an den Kontrollen der Datenschutzbeauftragten und die Belegschaftsvertretung beteiligt?
- Sind in den Verträgen mit Drittfirmen auch das Einhalten von Betriebsvereinbarungen, die Vorlage eines Datensicherheitskonzepts, die Zustimmung zum Einschalten von Unterauftragnehmern und jederzeitige Kontrollmöglichkeiten vereinbart?

4. Regelungen für die IT-Abteilung

- Sind in besonderen Fällen, zum Beispiel Überprüfung eines E-Mail-Accounts oder Auswertung einer Videoaufzeichnung, mindestens ein Vier-Augen-Prinzip und damit die Hinzuziehung gegebenenfalls des Datenschutzbeauftragten und des Betriebsrats vorgeschrieben?
- Sind Zugriffsberechtigungen von Administratoren nach Erforderlichkeit vergeben?
- Sind für die IT-Abteilung Stellenbeschreibungen erstellt und regelmäßig aktualisiert?
- Ist eine Administrationsrichtlinie erlassen worden?
- Sind alle Administratoren auf das Datengeheimnis und gegebenenfalls Fernmeldegeheimnis vom Datenschutzbeauftragten verpflichtet worden?

5. Regelungen zur Beschaffung und Verfügbarkeit von Hard- und Software

- Gibt es ein schriftliches Programmfreigabeverfahren?
- Gibt es aktuelle und vollständige Verzeichnisse der eingesetzten Hard- und Software?
- Sind eingesetzte webbasierte Software-Lösungen, Sicherheits-Software und Datensicherungs- und Fernwartungs-Tools ausreichend dokumentiert?
- Ist die Nutzung von mitgebrachten Privatgeräten (»BYOD«: Bring Your Own Device) geregelt?

6. Rechtsstellung und Fachkunde des betrieblichen Datenschutzbeauftragten

- Ist ein Datenschutzbeauftragter nach § 4f BDSG ordnungsgemäß und schriftlich bestellt?
- Liegt eine Begründung vor, wenn keine Bestellung vorgenommen worden ist?
- Handelt es um eine freiwillige Bestellung?
- Wird in der Bestellung Weisungsfreiheit, Unterstützung, rechtzeitige Information über neue Vorhaben, ausreichendes Zeit- und Mittelbudget und ein Meldewesen zum Verfahrensverzeichnis zugesichert?

7. Verfahrensverzeichnis

- Liegt ein aktuelles internes Verfahrensverzeichnis beim Datenschutzbeauftragten vor, das von der IT-Abteilung erstellt ist?
- Entspricht das Verfahrensverzeichnis den Vorgaben nach §§ 4e und 4g BDSG?
- Sind alle wesentlichen »Verfahren« dokumentiert?
- Benutzt das Unternehmen eine normgerechte Vorlage?
- Steht ein Jedermann-Verzeichnis nach § 4g Abs. 2 Satz 2 BDSG für Anforderungen bereit?
- Ist eine Prozedur bei Nachfragen zur Jedermann-Verfahrensübersicht eingeführt worden?
- Ist ein regelmäßiges Meldewesen von den Verfahrensverantwortlichen an den Datenschutzbeauftragten für die Aktualisierung des Verfahrensverzeichnisses eingerichtet, beispielsweise im Intranet?

8. Datenschutzmanagementsystem

- Existiert ein Datenschutzmanagementsystem, das die Zuständigkeiten, Ansprechpartner und die Zusammenarbeit der beteiligten Stellen im Datenschutz regelt?
- Sind die Inhalte der Datenschutzanweisung/-ordnung allen Beschäftigten aufgrund von Schulungsmaßnahmen bekannt?
- Wie wird sichergestellt, dass die Beschäftigten nach den schriftlichen Vorgaben des Datenschutzbeauftragten handeln?
- Wird der Datenschutzbeauftragte bei jeder Einführung oder Änderung von IKT-Systemen und bei allen datenschutzrelevanten Vorgängen rechtzeitig eingebunden und hat er dabei stets ein Anhörungsrecht?
- Prüft der Datenschutzbeauftragte Tests von Software mit nicht-anonymisierten Originaldaten der Beschäftigten vorab auf Zulässigkeit?
- Existiert für Testverfahren in der IT-Abteilung eine vom Datenschutzbeauftragten erstellte Richtlinie?
- Kontrolliert der Datenschutzbeauftragte regelmäßig gemäß § 4g Abs. 1 Nr. 1 BDSG die ordnungsgemäße Anwendung von IKT-Systemen?
- Führt der betriebliche Datenschutzbeauftragte angekündigte und nicht-angekündigte Kontrollen an Arbeitsplätzen durch?

9. Schulungsmaßnahmen nach § 4g Abs. 1 BDSG

- Liegen Nachweise über durchgeführte Mitarbeiterschulungen im Datenschutz vor?
- Für welche speziellen Zielgruppen sind (regelmäßige) Schulungsmaßnahmen vorgesehen?
- Existiert ein aktueller Schulungsplan und ein Schulungskonzept?
- Ist das Schulungskonzept mit der Interessenvertretung abgestimmt worden?
- Weisen die Schulungsinhalte einen konkreten Praxisbezug auf?

10. Verpflichtung gemäß § 5 BDSG und § 88 TKG

- Liegen Nachweise über Verpflichtungen auf das Datengeheimnis oder das Fernmeldegeheimnis vor?
- Werden neue Mitarbeiter zeitnah verpflichtet und unterrichtet aufgeklärt?
- Ist das Formular für die Verpflichtung auf das Datengeheimnis rechtskonform?
- Ist die Verpflichtung der Mitarbeiter an einer Unterrichtung des Datenschutzbeauftragten gekoppelt?
- Wird die Verpflichtung auf das Datengeheimnis regelmäßig aktualisiert?

11. Information und Beratung

- Wird der Datenschutzbeauftragte von der Geschäftsleitung über alle datenschutzrelevanten Vorhaben unterrichtet?
- Erhält der Datenschutzbeauftragte die Unterlagen zu allen geplanten IKT-Verfahren und bei wesentlichen Änderungen (Neuanlage, Änderung, Löschung) bestehender IKT-Verfahren vor dem Produktivstart?
- Sind Melde-, Abstimm-, Freigabe- und Kontrollverfahren für neue IKT-Verfahren und Änderungen bestehender IKT-Verfahren schriftlich geregelt, in denen der Datenschutzbeauftragte eingebunden ist, und funktionieren diese Prozesse?
- Werden neue IKT-Verfahren erst dann produktiv, wenn die Rückmeldung des Datenschutzbeauftragten vorliegt und seine Anforderungen umgesetzt worden sind?
- Ist die Aufbewahrung und Auswertung aller maschinell erzeugten Protokolle in einer Prozessbeschreibung geregelt?

12. Organisatorische Verfahren zur Sicherstellung der Rechte der Beschäftigten

- Hat der Datenschutzbeauftragte ein Verfahren zur Sicherstellung der Rechte von Betroffenen gemäß § 33 ff. BDSG schriftlich dokumentiert?
- Ist zum Beispiel bei einem Auskunftsersuchen eine schnelle und zweckmäßige Bearbeitung gewährleistet?
- Ist der Prozess der Bearbeitung und Beantwortung einer Datenschutzbeschwerde geregelt?
- Inwieweit wird der Datenschutzbeauftragte beim Bewerberdatenschutz tätig?
- Ist im Unternehmen die Schweigepflicht des Datenschutzbeauftragten und gegebenenfalls seines Hilfspersonals allen Beschäftigten erklärt worden?
- Wird im Jahresbericht vom Datenschutzbeauftragten anonymisiert über die Beschwerden, Datenschutzprobleme und Eingaben der Beschäftigten berichtet?

13. Umsetzung von § 9 und Anlage zu § 9 BDSG

- Gibt es eine aktuelle Übersicht zu den Maßnahmen nach § 9 BDSG im Unternehmen?
- Hat der Datenschutzbeauftragte diese technisch-organisatorischen Maßnahmen abgenommen oder sind (zertifizierte) Audits durchgeführt worden?
- Inwieweit werden mobile Datenträger verschlüsselt und ist der Datenschutzbeauftragte am Prozess beteiligt?
- Sind konkrete Maßnahmen zum Trennungsgebot besonders bei der Verarbeitung sensibler Daten umgesetzt worden?
- Inwieweit existieren für die IT-Verfahren mit personenbezogenen Daten der Beschäftigten schriftliche Berechtigungskonzepte und wird die Einhaltung und Notwendigkeit von Berechtigungen stichprobenartig überprüft?
- Existieren ein Datenträgerverzeichnis und Richtlinien zur Datenträgerentsorgung, Vernichtung von Papier und Entsorgung von Hardware?

Die komplette Checkliste gibt es auf der CuA-Website zum Download:

» **www.cua-web.de**

Die erforderlichen Mindestkenntnisse werden von den Aufsichtsbehörden wie folgt unterteilt:

- umfassende allgemeine Kenntnisse im Datenschutzrecht,
- branchenspezifische Kenntnisse,
- Kenntnisse einschlägiger spezialgesetzlicher Vorschriften und der Informations-/Kommunikationstechnik,
- Kenntnisse im betrieblichen Datenschutzmanagement und der technischen und organisatorischen Struktur des Unternehmens sowie betriebswirtschaftliche Grundkenntnisse.

Von besonderer Bedeutung ist der Hinweis, dass Datenschutzbeauftragte über Kenntnisse in Bezug auf die Zusammenarbeit mit dem Betriebsrat verfügen müssen. Kenntnisse im Arbeitsrecht sind erforderlich, weil die Datenschutzbeauftragten auf die Mitbestimmungsrechte bei der Einführung und Änderung von IKT-Systemen hinweisen und zum Beschäftigtendatenschutz beraten sollen.

Kenntnisse über die mittelbare Wirkung von Grundrechten sind erforderlich, wenn es um die Verhältnismäßigkeits- und Zulässigkeitsprüfung bei IKT-Systemen geht. In einer Umfrage von 2011 des Landesdatenschutzbeauftragten von Rheinland-Pfalz gaben etwa 40 Prozent der befragten Datenschutzbeauftragten aus der Privatwirtschaft an, dass sie über keinerlei arbeitsrechtliche Kenntnisse verfügen und somit im Beschäftigtendatenschutz keinerlei Kompetenz haben.[12]

Weisungsfrei und unabhängig

Seit 2009 ist die Unabhängigkeit des Datenschutzbeauftragten erheblich gestärkt worden. Er ist:

- weisungsfrei,
- hat einen gesetzlichen Sonderkündigungsschutz und
- ist dem Leiter der verantwortlichen Stelle direkt zu unterstellen.

Diese Unabhängigkeit ist durch organisatorische und vertragliche Regelungen sicherzustellen.

Seine Unabhängigkeit ist nach außen und innen darzustellen. Dazu gehört auch das Bekanntmachen seiner Kontaktdaten und die sichtbare Verankerung des Beauftragten in einer Stabsstelle, zum Beispiel im betrieblichen Organigramm.

Unterstützende Rahmenbedingungen

Die verantwortliche Stelle muss den Datenschutzbeauftragten in seiner Aufgabenerfüllung unterstützen. Für seine Prüfpflichten sind ihm alle erforderlichen Zutritts- und Einsichtsrechte für alle betrieblichen Bereiche einzuräumen.[13] Betriebliche Datenschutzbeauftragte sind in alle wichtigen Planungs- und Entscheidungsabläufe einzubinden. Damit sie das Verfahrensverzeichnis aktuell führen können, müssen sie alle erforderlichen Unterlagen dafür erhalten.

Die verantwortlichen Stellen haben eine Unterstützungspflicht, indem sie dem Datenschutzbeauftragten gemäß § 4f Abs. 5 BDSG Personal, Räume, Einrichtung, Geräte und Mittel zur Verfügung stellen.

Doch dem Datenschutzbeauftragten wird selten ausreichend Zeit für seine Aufgaben zugestanden, zudem bestehen häufig Interessenkonflikte. Die Aufsichtsbehörden verlangen, dass ihm die erforderliche Arbeitszeit zur Erfüllung seiner Aufgaben und Erhaltung ihrer Fachkunde eingeräumt wird. Konkrete Zahlen für ein Zeitbudget werden nicht genannt, da die Aufsichtsbehörden von einer Einzelfallprüfung ausgehen und einleitend feststellen:

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der Datenschutzbeauftragten maßgeblich beeinflusst werden durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der Datenschutzbeauftragten. Interessenvertretungen sollten darauf drängen, dass ein angemessenes Zeitbudget in der Bestellung des Beauftragten vereinbart wird.

Bei externen Datenschutzbeauftragten muss die verantwortliche Stelle eine bedarfsgerechte Leistungserbringung vertraglich gewährleisten. Diese ist in angemessenem Umfang vor Ort zu erbringen. Da externe Datenschutzbeauftragte als Ansprechpartner für Interessenvertreter oft nicht präsent sind[14], sollten diese überprüfen, inwieweit ein konkretes Zeitbudget und Präsenzzeiten mit dem externen Datenschutzbeauftragten vereinbart worden sind.

Aufgaben der Datenschutzbeauftragten

Oft mangelt es an einer kontinuierlichen Aufgabenerfüllung der nebenamtlichen Datenschutzbeauftragten, weil ihre verfügbare Zeit zu gering bemessen ist. Dies gilt auch für die behördlichen Datenschutzbeauftragten – hier aufgrund der engen Vorgaben der Rechnungshöfe.[15] Insofern sollten Arbeitnehmervertretungen die Kontroll-, Beratungs- und Informationsaufgaben des Beauftragten kennen und den Stand seiner Aufgabenerfüllung regelmäßig mit ihm besprechen.

Verfahrensverzeichnis

Nicht immer wird das interne Verfahrensverzeichnis[16] (§§ 4e und 4g BDSG), das die Datenbasis[17] für die Arbeit des Datenschutzbeauftragten ist, ernstgenommen. Es wird nicht oder nur unzureichend erstellt und nicht nach § 4e BDSG aufgebaut. Die rechtzeitige Meldung von Änderungen durch die Fachabteilungen an den Beauftragten findet vielfach nicht statt. Oft muss dieser zudem das Verfahrensverzeichnis erstellen, wofür ihm die notwendigen Unterlagen und technischen Kenntnisse fehlen.

Betriebsräte können das Verfahrensverzeichnis insbesondere für das Entwickeln und Durchsetzen von Betriebsvereinbarungen nutzen. Das Verfahrensverzeichnis eignet sich auch zum Prüfen, inwieweit bei den eingeführten IKT-Systemen zwischenzeitlich wesentliche Änderungen vorgenommen worden sind.

12 Brink, aaO.,58

13 Düsseldorfer Kreis, aaO., III.1

14 Zu externen und internen Datenschutzbeauftragten Scheja, in: Taeger/Gabel (Hrsg.), BDSG, 2010, § 4 f BDSG Rn. 45 ff. und 73 ff. und Brink, aaO., 57

15 Zum behördlichen Datenschutzbeauftragten Zilkens, Datenschutz in der Kommunalverwaltung, 3. Auflage, Rn. 493 ff.

16 Ausführlich Kiesche/Wilke, Das Verfahrensverzeichnis, in: CuA 10/2011, 27 ff.

17 Caster, aaO., 18

Nachhaltiges Datenschutzmanagement

Für ein systematisches Datenschutzmanagement fehlt es den Datenschutzbeauftragten auch an Zeit. Elemente eines Datenschutzmanagements wie Strategieentwicklung, Kontrollen, Beratung, Dokumentation, Verzeichnisse der eingesetzten Hard- und Software, Log-File-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen und Zusammenarbeit mit dem Betriebsrat[18] sind nur selten anzutreffen. Das qualitätsgesteuerte Datenschutzmanagement bleibt eine wichtige Aufgabe des Datenschutzbeauftragten, bei der Interessenvertretungen Unterstützung leisten können.

Bildungsaufgabe Datenschutz

In der Untersuchung des Landesdatenschutzbeauftragten von Rheinland-Pfalz wird deutlich, dass die Schulungs- und Informationsfunktion des Datenschutzbeauftragten in 32,5 Prozent der teilnehmenden verantwortlichen Stellen nicht wahrgenommen wird.

Tatsächlich finden angemessene Schulungsmaßnahmen des Datenschutzbeauftragten kaum statt. Eine PowerPoint-Präsentation mit wenigen Folien im Intranet ist keine angemessene Schulungsmaßnahme. Da Rechte gemäß §§ 96 bis 98 BetrVG[19] zu beachten sind, sollten die Interessenvertretungen mit Hilfe ihrer Mitbestimmung den Anspruch auf Schulungsmaßnahmen für alle Beschäftigten durchsetzen.

Informieren und Unterrichten

Oft wird die Information über den Datenschutz, etwa für neu eingestellte Beschäftigte, und die Verpflichtung auf das Datengeheimnis gemäß § 5 BDSG auf ein Merkblatt und eine Verpflichtungserklärung reduziert. Die Beschäftigten unterschreiben dann die Erklärung, obwohl eine erforderliche Unterrichtung unterbleibt. Das Merkblatt allein genügt nicht. Hier sollten Betriebsräte darauf drängen, dass eine angemessene Unterrichtung stattfindet und daran anschließend eine jederzeitige Beratung der Beschäftigten durch den Datenschutzbeauftragten möglich ist. Die Verpflichtung einschließlich Unterrichtung[20] ist in geeigneten Zeitabständen zu wiederholen.

Beraten und Kooperieren

In vielen verantwortlichen Stellen existiert nur ein prekäres Verhältnis zwischen Datenschutzbeauftragtem und Belegschaftsvertretung, das heißt ein systematischer Austausch einschließlich Beratung findet selten statt. Größte praktische Schwierigkeiten haben Betriebsräte bei dem Versuch, mit externen Datenschutzbeauftragten ins Gespräch zu kommen, da der Arbeitgeber oft aus Kostengründen den Wunsch nach Kooperation schlichtweg ablehnt. Hier sollten die Aufsichtsbehörden in ihrer Kontrollpraxis eine Beratungs- und Kommunikationspflicht des externen Beauftragten anmahnen.

Rechte sicherstellen

Die Rechte auch der betroffenen Beschäftigten sicherzustellen, ist eine wichtige Aufgabe des Datenschutzbeauftragten. In der Regel finden sich auch in größeren Unternehmen keine formalisierten Verfahren, etwa zum Auskunftsersuchen. Datenschutzrechte werden praktisch kaum von den Betroffenen genutzt. Hier sind Interessenvertretungen gehalten, die Einführung vereinfachter Verfahren zu initiieren und ihren Datenschutzbeauftragten dabei zu unterstützen.

Gewährleisten der Datensicherheit

Immer wichtiger werden Risikoanalysen und Maßnahmen der Datensicherheit. In geprüften Verfahrensverzeichnissen wird deutlich, dass die Datensicherheit noch vernachlässigt wird. Insofern wird in der Checkliste ab Seite 29 die Gewährleistung der Datensicherheit – das heißt die Umsetzung von § 9 und Anlage zu § 9 BDSG – als Aufgabe des Datenschutzbeauftragten berücksichtigt.[21] Auch bei dieser Aufgabe sind Informations-, Beratungs- und Mitbestimmungsrechte der Betriebsräte zu beachten.

Fazit

Für Arbeitnehmervertretungen lohnt sich ein systematisches und nachhaltiges Datenschutz-Audit. Datenschutzbeauftragte und Belegschaftsvertretungen können und sollten mit Hilfe eines Audit-Plans kooperativ Gespräche führen, die es ermöglichen, den Stand des betrieblichen und behördlichen Datenschutzes einschließlich des Beschäftigtendatenschutzes zu erheben und im Interesse der Beschäftigten erheblich zu verbessern.[22]

Rückmeldungen zur Anwendbarkeit und Qualität dieser Checkliste, die keinen Anspruch auf Vollständigkeit erhebt und in der Praxis weiter getestet und erprobt wird, sind ausdrücklich erwünscht.

Autoren

Dr. Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen
» eberhard.kiesche@t-online.de
» www.aob-bremen.de

Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel
» info@dtb-kassel.de
» www.dtb-kassel.de

cua-web.de

SERVICE

Voting-Box	✔
Rechtsprechung	
Muster » Checkliste	✔
Arbeitshilfen	
Gesetze	

18 Düsseldorfer Kreis, aaO., I. 2

19 Hallermann, Mitarbeiterschulungen im Datenschutz, in: RDV 2011, 288 ff. (290)

20 Caster, aaO., 25; zur Verpflichtung im öffentlichen Dienst und einem Muster siehe Zilkens, aaO. Rn. 69 ff.

21 Die Audit-Checkliste für Interessenvertretungen baut auf folgenden Mustern und Leitfäden auf: Gesellschaft für Datenschutz und Datensicherheit (Hrsg.), Datensicherheit im Unternehmen, 4. Auflage, 133 ff.; Caster, aaO., Düsseldorfer Kreis, aaO.; Gola (Hrsg.), Datenschutz-Jahrbuch GDD 2013, 438, 495; Seifert, Datenschutzprüfung durch die Aufsichtsbehörden, CD-ROM, 2. Auflage; Oppolzer, Gesundheitsmanagement im Betrieb, 2. Auflage, 38 ff.

22 Für den öffentlichen Bereich Ilbertz/Widmaier, BPersVG, 11. Auflage, § 68 Rn. 59