CB-BEITRAG

Brigitte Jordan

Step-by-step: Wie verankere ich das Bundesdatenschutzgesetz praxisnah und zum Vorteil des Unternehmens?

Der nachfolgende Beitrag gibt einen Überblick über die komplexen und vielfältigen Fragestellungen und Herausforderungen, vor denen Datenschutzbeauftragte im Unternehmen regelmäßig stehen. In diesem Zusammenhang erläutert die Autorin insbesondere auch die technischen und organisatorischen Maßnahmen, die geeignet sind, den besonderen Anforderungen des Datenschutzrechtes gerecht zu werden.

Einleitung

Aus heutigen Unternehmensstrukturen sind leistungsfähige IT-Systeme zur Verarbeitung und Auswertung personenbezogener Daten, v. a. Kundendaten, nicht mehr wegzudenken. Moderne ERP-, CRM- und Data Warehouse Systeme bieten nahezu unbegrenzte Möglichkeiten, Daten zu verwerten und zu analysieren. Diesen Möglichkeiten hat der Gesetzgeber das Bundesdatenschutzgesetz (BDSG) und andere rechtliche Vorschriften entgegengesetzt, um das informelle Selbstbestimmungsrecht des Einzelnen in seinem Persönlichkeitsrecht zu schützen. Das BDSG schützt vor Beeinträchtigungen der Persönlichkeitsrechte durch unsachgemäßen Umgang mit personenbezogenen Daten und bietet darüber hinaus dem Unternehmen eine zweckdienliche und immer aktuelle Transparenz seiner schützenswerten Geschäftsprozesse, Abläufe und Daten. Solche Daten sind neben Personalstammdaten, Buchhaltungsdaten, Kundenstammdaten auch Forschungs- und Entwicklungsdaten. Jedes Unternehmen ist daran interessiert, seine Unternehmenswerte wie bspw. Erfindungen, Entwicklungen und Verkaufsstrategien vor dem Zugriff ungebetener Dritter zu schützen. Das BDSG in seiner aktuellen Form gibt wichtige Grundsätze im Umgang mit personenbezogenen Daten vor:

Es ist alles verboten, was nicht explizit erlaubt ist
Dieser Grundsatz soll gewährleisten, dass im Zuge neuer technischer Entwicklungen keine Möglichkeiten genutzt werden können, die dem Sinn des Gesetzes und den Interessen der Unternehmen widersprechen. Daher dürfen personenbezogene Daten nur so genutzt werden, wie es im BDSG ausdrücklich gestattet ist.

Die Speicherung und Verarbeitung von Daten bedarf einer Erlaubnis
Ein Unternehmen darf Daten nur erheben und verarbeiten, wenn eine ausdrückliche Erlaubnis vorliegt. Diese kann durch die Betroffenen oder durch eine Rechtsvorschrift erteilt werden.

Datenvermeidung und Datensparsamkeit
Es dürfen nur solche personenbezogenen Daten gespeichert werden, die für den Nutzungszweck absolut erforderlich sind. So wird der unkontrollierten Erhebung und Nutzung von Daten vorgebeugt.

Daten dürfen nur zweckgebunden verwendet werden
Die Vermischung personenbezogener Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist im BDSG untersagt. So wird vermieden, dass aus den gespeicherten Daten Analysen erstellt werden, die detaillierte Rückschlüsse auf Eigenschaften oder persönliche Verhältnisse der Betroffenen zulassen.
Wenn ein Unternehmen dem Datenschutz keine angemessene Aufmerksamkeit widmet, kann dies weitreichende Folgen haben:
- Empfindliche Geldstrafen bis zu 300 000 Euro
- Freiheitsentzug bis zu zwei Jahren
- Imageverlust bei Kunden und Kooperationspartnern
- Nichterfüllung von Anforderungen aus dem Qualitätsmanagement
- Rating-Nachteile bei der Kreditvergabe (IT-Sicherheit ist ein Rating Faktor in den Vorgaben nach Basel II)

Für die Folgen eines mangelnden Datenschutzes gilt der Grundsatz der Geschäftsführer- bzw. Vorstandshaftung, es handelt sich also um ein Ordnungsmäßigkeitsverschulden.

Ausgangssituation

Im heutigen digitalen Zeitalter werden Massendaten verarbeitet, archiviert und sollen möglichst in kürzester Zeit vorgehalten werden können, um Unternehmensentscheidungen kurzfristig daraus ableiten zu können. Allein zur Gewährleistung der eigenen Ordnungsmäßigkeit, Nachvollziehbarkeit, Sicherheit und mit dem Ziel der Revisionssicherheit ist es erforderlich, im Unternehmen die schützenswerten Daten zunächst zu ermitteln. Jedes Unternehmen ist anders aufgestellt und arbeitet nach anderen Wertvorstellungen. Dies muss im Zusammenhang mit dem BDSG besonders beachtet werden.

Das Gesetz betrachtet ausschließlich Daten über persönliche oder sachliche Verhältnisse einer bestimmten bzw. bestimmbaren natürlichen Person. Innerhalb dieses Rahmens ist der Datenkranz sehr weit gefasst. Er bezieht sich sowohl auf alle Merkmale zur Identifikation von Personen wie Name, Alter, Größe, Gewicht, Familienstand, als auch auf Merkmale über seine persönlichen und geschäftlichen Verhältnisse, wie bspw. Vermögen, Grundbesitz, Mitgliedschaften, Automarken, Umsätze, Kosten, Wohnsitze und Ähnliches. Fügt man beide Komponenten, also die Beschreibung über die personenbezogenen Daten sowie die Vorschrift über die natürliche Person zusammen, lässt sich schnell erkennen, dass in einem Unternehmen mit komplexer IT-Landschaft eine Vielzahl von Daten zu den unterschiedlichsten Personenkreisen betroffen ist.

Zunächst trifft dies für das in einem Unternehmen beschäftigte Personal zu. Gleiches gilt allerdings auch für eine größere Anzahl von Lieferanten und Kunden. Betroffen sein können ferner Angehörige oder Personen, über die man schreibt oder Dossiers sammelt. Ebenso betrifft es Informationen über externe Zuarbeiter, soweit deren Daten für Abrechnungs- oder Kostenrechnungszwecke benötigt werden. Allein in dieser kleinen Zusammenstellung sind unterschiedlichste Applikationen aus dem Personal- und Lohnbereich, der Auftragsabwicklung, der Finanzbuchhaltung, der Produktionsplanung und -steuerung, dem Vertrieb, dem Einkauf sowie dem Marketing involviert.

Darüber hinaus verlangt § 4f BDSG – sofern mindestens zwanzig Personen in die automatisierte Verarbeitung personenbezogener Daten involviert sind – schriftlich einen Beauftragten für den Datenschutz zu bestellen. Dieser Person müssen nicht nur seitens des Unternehmens die notwendigen Arbeitsmittel zur Verfügung gestellt werden, sie muss auch über die notwendige Arbeitszeit verfügen, die für diesen Aufgabenbereich notwendigen Prüfungen selbst durchzuführen. Bei der Beurteilung der Fachkunde ist insbesondere darauf zu achten, dass der Datenschutzbeauftragte EDV-technische Sachverhalte unter juristischem Blickwinkel interpretieren und den jeweiligen gesetzlichen Tatbeständen zuordnen kann. Nützlich ist daher eine juristische Vorbildung oder die Erarbeitung solcher Kenntnisse in entsprechenden weiterführenden Seminaren.

Die organisatorische Zuordnung sollte – soweit Datenschutzbelange betroffen sind – direkt unterhalb der Unternehmensleitung erfolgen, Interessenskonflikte sind möglichst zu vermeiden. So ist ein der IT-Abteilung zugehöriger (nebenamtlicher) Datenschutzbeauftragter kritischer zu beurteilen, als bspw. der Justitiar des Unternehmens, auch wenn letzterem detaillierte Kenntnisse über IT-technische Zusammenhänge fehlen. Er kann sich sachkundige Hilfe einholen, bspw. bei der IT-Revision. Die oftmals anzutreffende Übertragung der Funktion des Datenschutzbeauftragten auf den Leiter oder einen Mitarbeiter der Internen Revision kann dann zu Interessenskonflikten führen, wenn im Rahmen dieser Tätigkeit zu Kontroll- und Nachweiszwecken eine Speicherung und Verarbeitung personenbezogener Daten, die das Gesetz ausschließt, als wünschenswert erachtet wird.

Das BDSG muss zunächst verstanden und von dem jeweils bestellten Datenschutzbeauftragten so gut und praxisnah wie möglich vermittelt werden. Das setzt eine gewisse Praxiserfahrung voraus, um dieser Anforderung gerecht zu werden.

Im Wesentlichen gibt es zwei Kategorien im Datenschutz, sie lauten „Dokumentationspflicht“ und „technische und organisatorische Maßnahmen (TOM)“. Bei der Dokumentationspflicht geht es bspw. darum, alle Mitarbeiter auf die Geheimhaltung gem. § 5 BDSG zu verpflichten. Bei den technischen und organisatorischen Maßnahmen werden zudem einzelne Schutzmaßnahmen im Unternehmen nicht nur durch die Datenschutzbrille sondern auch durch die Sicherheitsbrille betrachtet und beide Aspekte besonders mit Praxisbezug zum Unternehmen aufgenommen.

Durchführung

Die wertvollste aller Dokumentationspflichten ist die Aufnahme eines internen Verfahrensverzeichnisses nach § 4g i. V. m. § 4e BDSG. Die meisten Datenschützer werden spätestens jetzt aufschreien, da es die größte Herausforderung darstellt, die das Gesetz vorgibt. Allerdings wissen sie auch, wie hilfreich und essenziell diese Aufnahme für sie selbst und das Unternehmen im Einzelnen ist. Es wird eine transparente, eindeutige und verständliche erste Bestandsaufnahme schützenswerter Unternehmensdaten erstellt. Dabei werden alle schützenswerten Verfahren (DV-Anwendungen) gemäß Gesetzesvorlage erfasst, beschrieben und aktuell gehalten. Diese Aufnahme ist zwar eine Fleißarbeit, bietet dem Unternehmen jedoch mehrere Vorteile. Das Miteinander wird gefördert, ebenso die interne Kommunikation und das Verständnis gegenüber dem Schutz sensibler, personenbezogener Daten im Unternehmen. Nach Abschluss der Verfahrensbestandsaufnahme werden im zweiten Schritt die Verantwortlichen pro Verfahren ermittelt und dokumentiert. Um bei automatischer Übermittlung personenbezogener Daten Herkunft und Empfänger zu erkennen und die Sicherheit der Übertragung beurteilen zu können, bedarf es transparenter Schnittstellen. Damit zugriffsberechtigte Personengruppen oder allein zugriffsberechtigte Personen erkennbar werden, wird ein Organigramm mit der Beschreibung der Verantwortlichkeiten zumindest für den IT- und Personalbereich erstellt.

Hilfreich bei der ersten Bestandsaufnahme sind:

- Dateiverzeichnisse/Softwareinventar
- Schnittstellenübersichten
- Organigramme und Stellenbeschreibungen

Bereits nach der ersten Bestandsaufnahme erhalten Geschäftsführung und Betriebsrat eine verständliche und transparente Übersicht aller sensiblen IT-Verfahren mit den jeweiligen Verfahrensverantwortlichen. Je nach Größe eines Unternehmens kann es sich um bis zu 200 Anwendungen mit 300 integrierten Verfahren handeln. Ein Beispiel bietet ein ERB-System mit mehreren Modulen wie bspw. FI, PP, WWS oder HR. Unter dem ERP-Hauptsystem müssen die im Einsatz befindlichen Module mit ihren integrierten Verfahren wie bspw. Zeitwirtschaft und Bewerbungsverfahren jeweils einzeln anhand der Verfahrensbeschreibung aufgenommen und dokumentiert werden. Dies ist in der Tat eine aufwendige Fleißarbeit, die sich jedoch bezahlt macht.

Es werden neben den grundsätzlichen Angaben zum Verfahren die jeweils berechtigten Personenkreise erfasst und damit die einzelnen Berechtigungen systemseitig geprüft. Dies lässt sich auch als Säuberungsaktion deklarieren. Dabei wird meistens schnell erkannt, ob innerhalb der Verfahren noch „alte“ Berechtigungen von Mitarbeitern bestehen, die bereits das Unternehmen verlassen haben oder Mitarbeiter Berechtigungen besitzen, die innerhalb des Unternehmens die Position gewechselt und keine Zugriffsrechte mehr haben. So wird eine effektive Bereinigung der Berechtigungen erzeugt.

Hinzu kommt, dass oftmals nicht bekannt ist, ob externe Dienstleister für ihre Systempflege und Wartung sogar noch zusätzlich unnötige und teilweise unberechtigte Zugriffsberechtigungen besitzen. Auch dieser Aspekt wird geprüft, und die betreffenden Dienstleister/Auftragnehmer werden gem. § 11 BDSG im Rahmen der Auftragsdatenverarbeitung verpflichtet. In diesem Zusammenhang werden die bestehenden

Rahmen-/Hauptverträge überprüft, da das BDSG einen Anforderungskatalog von zehn zu erfüllenden Vertragsvorgaben- und Kriterien vorgibt. Sollten diese nicht in dem bestehenden Vertrag mit dem jeweiligen Dienstleister/Auftragnehmer abgehandelt sein, ist eine zusätzliche Verpflichtungserklärung zu vereinbaren. Auch ist es die Aufgabe eines Datenschutzbeauftragten, sich bei den Dienstleistern/Auftragnehmern selbst von der Einhaltung des BDSG zu überzeugen. An dieser Stelle sei erwähnt, dass durch eine solche Datenschutzmaßnahme dank dieses Gesetzes auch ein Unternehmensmehrwert geschaffen wird.

Dazu bietet die Anlage zu § 9 S. 1 des BDSG mit ihren **acht technischen und organisatorischen Maßnahmen (TOM)** einen weiteren transparenten und zweckgebundenen Praxisbezug. Diese Maßnahmen sind innerhalb des internen Verfahrensverzeichnisses ebenfalls pro Verfahren auf die jeweils tatsächliche Ist-Situation zu prüfen und zu dokumentieren.

Es handelt sich um

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Trennungsgebot

Erfahrungsgemäß aus der Praxis empfiehlt es sich der Vollständigkeit halber und in diesem Kontext, diese Kontrollmaßnahmen um drei weitere zu ergänzen.

Dabei handelt es sich um den

9. Zweckbindungsgrundsatz
10. Organisationskontrolle
11. Verhältnismäßigkeits-Grundsatz

1 Zutrittskontrolle

Gemäß BDSG-Anlage (zu § 9 S. 1) ist zu gewährleisten, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle).

Es wird bspw. nach Regelungen zum Gebäudezutritt und auch nach den berechtigten Personen zu einzelnen Bereichen/Abteilungen gefragt. Dies schützt das Unternehmen vor fremdem Eindringen und minimiert das Risiko von Diebstahl oder Vandalismus. Ein Beispiel für eine mögliche Maßnahme kann der Pförtner sein, bei dem sich jeder Besucher an- und abmelden muss. Dabei wird ein Besucherbuch geführt, in dem alle Besucher dokumentiert werden, sodass niemand vergessen und nach Feierabend alleine zurückgelassen werden kann. So lässt sich schnell erkennen, ob ein erforderliches Maß an Sicherheitsmaßnahmen bereits eingerichtet wurde, fehlende Maßnahmen können punktuell im Unternehmen optimiert werden.

2 Zugangskontrolle

Gemäß BDSG-Anlage (zu § 9 S. 1) ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle).

Die Zugangskontrolle beginnt beim Anmelden des Arbeitsplatzrechners. Die Passwörter sollten nicht auf dem Schreibtisch unter der Tastatur liegen. Dies beinhaltet die Verhinderung des physischen Zugangs zu Anlagen, auf denen die Verarbeitung personenbezogener Daten erfolgt. Sie dürfen weder allgemein noch innerhalb der Unternehmen nicht autorisierten Mitarbeitern zugänglich sein. In Großrechnerumgebungen mit einem hermetisch abgeriegelten Rechenzentrum ist dies weitgehend selbstverständlich. Problematischer wird es in netzwerkbasierten Client-Server-Umgebungen. Hier müssen die entsprechenden Serverlaufwerke in einem gesondert abgeschlossenen Raum geschützt sein. Zu beachten ist in diesem Zusammenhang, dass nicht nur mit der Verarbeitung beschäftigte Rechner, sondern ebenfalls Serverlaufwerke mit Sonderfunktionen, bspw. der Druckdienst (Print-Server) oder der Datenaustausch (Kommunikationsserver) betroffen sind. Dies gilt gleichermaßen für Personal Computer, wenn personenbezogene Daten aus dem Serverbereich auf die Arbeitsplatzstationen der Mitarbeiter transferiert werden können oder ausschließlich dort verarbeitet werden. Auch in diesem Fall muss – den Vorschriften dieses Gesetzes entsprechend – der Zugang zu den Geräten befugten Mitarbeitern vorbehalten bleiben.

3 Zugriffskontrolle

Gemäß BDSG-Anlage (zu § 9 S. 1) ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).

Innerhalb eines integrierten IT-Systems werden nicht ausschließlich personenbezogene Daten verarbeitet. Zumeist wirken hier eine Reihe unterschiedlicher Applikationen, bspw. zur Finanzbuchhaltung, zum Materialbereich, zur Produktionsplanung und -steuerung sowie zum Personalbereich zusammen. In diesen Fällen muss sichergestellt sein, dass ausschließlich Berechtigte Zugriff auf die personenbezogenen Daten haben. Dies muss mit einem differenzierten Zugriffsberechtigungssystem geregelt werden.

Aus der Sicht des Datenschutzes ist es wichtig, dass das Zugriffsberechtigungssystem auf der Grundlage eines schriftlich formulierten, durchdachten und nachvollziehbaren Konzepts entwickelt wurde. Weiterhin muss es ausreichend transparent, dokumentiert und für den Datenschutzbeauftragten in einer angemessenen Zeit prüfbar sein. Daneben muss eine gut funktionierende Benutzerverwaltung dafür sorgen, dass nur aktive Mitarbeiter mit angemessenem Berechtigungsumfang im EDV-System zugelassen sind.

4 Weitergabekontrolle

Gemäß BDSG-Anlage (zu § 9 S. 1) ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle).

Die Weitergabe von Daten über Einrichtungen zur Datenübertragung wie Modems oder Kommunikationsserver muss überprüf- und nachvollziehbar sein. Das Gesetz verlangt an dieser Stelle, dass erkennbar ist, an wen personenbezogene Daten übermittelt wurden.
Um dieser Forderung gerecht zu werden, bedarf es für die Übermittlung der Daten einer schriftlichen Dokumentation. Darüber hinaus ist durch geeignete Maßnahmen sicherzustellen, dass nicht unbefugt, z. B. über Modemverkehr, Daten weitergeleitet und abgerufen werden. Auch hier gilt es, ein geeignetes Verfahren zu finden, bei dem Daten ausschließlich über eine vorher festgelegte, definierte Kommunikationsschnittstelle, z. B. über einen gesondert hierzu festgelegten Kommunikationsserver, übertragen werden. Begleitend hierzu sollte die Datenübertragung in einem automatischen Aufzeichnungsverfahren festgehalten werden.

5 Eingabekontrolle

Gemäß BDSG-Anlage (zu § 9 S. 1) ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).
Die besondere Sensibilität personenbezogener Daten macht es notwendig, dass deren Verarbeitung durch andere Personen prüfbar und nachvollziehbar bleibt. Das Gesetz bestimmt, dass es möglich sein muss, nachträglich zu überprüfen und festzustellen, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind.
Dieser Forderung werden die Unternehmen weitgehend durch technische Maßnahmen gerecht. Zum einen sollte das Verfahren der Dateneingabe und Übernahme ausreichend detailliert und schlüssig beschrieben sein. Darüber hinaus ist es notwendig, dass der Zugriff von Mitarbeitern, die sich mit der Verarbeitung von personenbezogenen Daten beschäftigen, automatisch festgehalten wird. Aus einer solchen automatischen Logdatei sollte u. a. hervorgehen, wer wann mit welcher Funktion auf diese Daten zugegriffen hat. Eine Vielzahl von IT-Systemen erzeugt darüber hinaus automatische Änderungsprotokolle, bspw. bei der Veränderung von Stammdaten. Entsprechende Protokolle sollten auch für die Änderung personenbezogener Daten vorgesehen werden.

6 Auftragskontrolle

Gemäß BDSG-Anlage (zu § 9 S. 1) ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle).
Soweit personenbezogene Daten extern, bspw. in einem Dienstleistungsrechenzentrum, verarbeitet werden, muss durch detaillierte vertragliche Verpflichtungen sichergestellt werden, dass dies ausschließlich entsprechend den Weisungen des Auftraggebers geschieht. Der Gestaltung dieser Verträge ist auch unter dem Gesichtspunkt des Datenschutzes erhöhte Aufmerksamkeit zuzuwenden. Der externe Dienstleister muss die gleichen Verpflichtungen für die Einhaltung der Datenschutzbestimmungen übernehmen, die auch den Auftraggeber treffen (Grundsatz der Auftragsbindung). Weiterhin ist bei der Gestaltung der Verträge darauf zu achten, dass ein ausreichendes Zugriffs- und Prüfrecht für den Datenschutzbeauftragten des Auftraggebers formuliert wird.

7 Verfügbarkeitskontrolle

Gemäß BDSG-Anlage (zu § 9 S. 1) ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).
Personenbezogene Daten werden sowohl innerhalb der Rechner auf Datenträger gespeichert und verarbeitet als auch außerhalb der Rechner, etwa zu Archivierungszwecken, auf Bändern, optischen Platten oder zur Übermittlung auf Disketten abgelegt. Hierbei ist zu verhindern, dass diese Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es ist sicherzustellen, dass die Schnittstellen für die Datenauslagerung wie Diskettenlaufwerke nur von Befugten genutzt werden können. Gleiches gilt für die Datenarchivierung. Weiterhin müssen Sicherungsmedien mit besonderer Sorgfalt, etwa in Panzerschränken oder besonders geschützten Räumen, aufbewahrt werden. Eine zusätzliche Sicherung ist die kryptografische Speicherung personenbezogener Daten, sodass kein Unbefugter hierauf zugreifen kann und sie zudem für das Unternehmen jederzeit verfügbar sind.

8 Trennungsgebot

Gemäß BDSG-Anlage (zu § 9 S. 1) ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Ein Testsystem bspw. ist daher grundsätzlich vom Echtsystem zu trennen. Insbesondere sind Verschlüsselungsverfahren nach aktuellem Stand der Technik zu berücksichtigen. Empfehlenswert ist es, in diesem Zusammenhang auch die **Organisationskontrolle** zu beachten. Die innerbetriebliche Organisation muss – soweit der Bereich der Verarbeitung personenbezogener Daten betroffen ist – derart gestaltet sein, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Diese Forderung korrespondiert mit gleichlautenden Anforderungen der Revision und der Wirtschaftsprüfung an ein funktionierendes internes Kontrollsystem. Die Aufbauorganisation sollte klar geregelt und in einem aussagefähigen Organigramm dokumentiert sein. Gleiches gilt für eine klare Regelung und Beschreibung der innerbetrieblichen Abläufe. Wichtig ist darüber hinaus eine schriftlich formulierte, eindeutige Abgrenzung der einzelnen Verantwortlichkeiten. Grundsätze der Funktionstrennung sowie des Vier-Augen-Prinzips sollten in der internen Organisation berücksichtigt werden.
Abschließend sollte **§ 31 BDSG (Besondere Zweckbindung)** in allem zu treffenden technischen und organisatorischen Maßnehmen Beachtung finden. Das bedeutet, dass personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden dürfen.
Für die oben aufgeführten TOMs gilt ein sog. Verhältnismäßigkeitsprinzip. Demnach müssen personenbezogene Daten nicht unendlich

stark geschützt werden, wenn die Umsetzungsmaßnahmen dafür wirtschaftlich unangemessen hoch ausfallen würden.
In diesem Zusammenhang ergeben sich in allen Unternehmensbereichen komplexe und vielfältige Fragestellungen – die täglichen Herausforderungen eines jeden Datenschutzbeauftragten.

Praxisbeispiel/Exkurs

Datenschutz bedeutet gleichzeitig Datensicherheit und Unternehmenssicherheit. Und aus falsch verstandenem Datenschutz kann plötzlich ein sehr hohes Unternehmensrisiko entstehen. Diese Aussagen lassen sich am besten anhand eines Beispiels aus der Praxis darstellen:
In einem Industrieunternehmen wurde auf Drängen des Betriebsrats der Schutz von personenbezogenen Daten, hier der Mitarbeiterdaten, sehr stark in den Fokus gerückt. Er setzte durch, dass bestimmte Transaktionen und Datenzugriffe in den IT-Systemen nicht mehr protokolliert werden durften. Es sollte damit verhindert werden, dass von den Mitarbeitern ggf. Beschäftigungs- oder auch Zeitprofile angefertigt würden, mit denen möglicherweise Leistungsprofile erstellt werden könnten. Ungeachtet blieb in diesem Bestreben, dass selbst gesetzlich geforderte Aufzeichnungen über rechnungslegungsrelevante Geschäftsprozesse (HGB & AO) nicht mehr nachvollziehbar waren.
Nach einer gewissen Zeit und einem Personalwechsel gerieten die geänderten Prozesse in Vergessenheit. Und dann geschah Folgendes: über Nacht wurden die Unternehmensdaten inklusive der bis dato so vordergründig schutzbedürftigen Mitarbeiterdaten von außen aus dem Internet vom IT-System des Unternehmens abgezogen. Festgestellt wurde der Vorgang am folgenden Arbeitstag von den IT-Mitarbeitern, als sie das Verhalten der IT-Systeme in der vorangegangenen Nacht überprüften. Darüber hinaus konnte nichts kontrolliert und nachvollzogen werden, da die erforderlichen Protokolle, wie oben gefordert, nicht zur Verfügung standen.
Wegen der irgendwann von irgendwem aus falschem Datenschutzgedanken abgeschalteten Kontroll- und Protokollierungssysteme war es nicht möglich nachzuvollziehen, wer in der Nacht welche Unternehmensdaten abgerufen hatte und wohin diese Daten übertragen wurden. Was war der Hintergrund? Handelte es sich um eine klassische moderne Industriespionage? War es nur ein Versehen eines ebenfalls nicht abgesicherten Fremdsystems und gingen die Daten einfach nur ins Nirwana?
Sicher ist jedenfalls, dass falsch verstandener Datenschutz zu einem erheblichen Unternehmensrisiko geführt hat. Das bedeutet, dass richtig und vernünftig eingerichteter Datenschutz gleichzeitig auch die Unternehmenssicherheit erhöht und absolute Chefsache sein muss. Ein korrekt eingerichtetes Datenschutzmanagement gibt Rechtssicherheit und trägt wesentlich zur Unternehmenssicherheit und Wirtschaftlichkeit bei.

Fazit

Sobald man die Ausgangssituation und die Zielsetzung eines jeden Unternehmens mit seinen individuellen Prozessen und Verfahren kennt, der Datenschutz verstanden wird, und die Verantwortlichen stets informiert sind, kann eine praxisnahe Gesetzmäßigkeit zum Vorteil des Unternehmens eingerichtet und auch gelebt werden.
Datenschutzmanagement sichert nicht nur jeden einzelnen Arbeitsplatz im Unternehmen sondern schützt tatsächlich sensible Unternehmensdaten vor fremdem Zugriff und Datendiebstahl. Zusätzlich bietet das gelebte Datenschutzmanagement nach außen gegenüber Kunden und Geschäftspartnern Sicherheit und schafft somit einen enormen Mehrwert. Das zahlt sich für jedes Unternehmen aus. Denn Datenschutz-Kompetenz schafft Vertrauen.

AUTORIN

Brigitte Jordan *ist seit 2004 geschäftsführende Gesellschafterin der REVIDATA GmbH in Düsseldorf. Seit 2007 betreut sie ihre Kunden u. a. als Datenschutzbeauftragte und erhielt darauf aufbauend im Jahr 2009 die geprüfte Qualifikation als zertifizierte Datenschutzauditorin. Brigitte Jordan ist bereits seit 1996 bei dem Traditions- und Familienunternehmen REVIDATA GmbH beschäftigt.*