

Wer darf was?

Das dritte Gebot: Die Zugriffskontrolle

Die Zugriffskontrolle soll erreichen, dass Mitarbeiter und befugte Dritte nur im Rahmen ihrer Rechte auf Daten zugreifen können. Weiterhin soll sie verhindern, dass personenbezogene Daten unbefugt gelesen, kopiert, verändert oder entfernt (gelöscht) werden können. Ein alltägliches, jedoch nicht einfaches Thema für den Datenschutzbeauftragten.

► Waren die beiden vorhergehenden Gebote aus dem § 9 BDSG und Anlage, die Zutritts- und die Zugriffskontrolle, noch relativ grobe Einzelmaßnahmen, um den Schutz von personenbezogenen Daten sicherzustellen, ist das dritte Gebot weitaus feingliedriger.

Fokussierung auf die Echtdaten

Der Datenschutzbeauftragte hat jetzt bereits personenbezogene Datenfelder und Datenkategorien im Fokus seiner

Empfehlungen für den Umgang mit vertraulichen Dokumenten

Selbst Microsoft stellt die Frage, wie Sie vertrauliche Dokumente vor unbefugtem Zugriff schützen, und bietet Strategien, damit vertrauliche Dokumente auch vertraulich bleiben. Hier ein Auszug der Empfehlungen:

1. Vernichten Sie Ausdrucke. Wenn Sie vertrauliche Dokumente zum Austeilen bei Besprechungen drucken, sammeln Sie sie anschließend wieder ein und vernichten Sie sie bzw. fordern Sie die Teilnehmer auf, dies zu tun.
2. Beschriften Sie Dokumente. Gelegentlich sind sich Mitarbeiter nicht bewusst, dass bestimmte Dokumente vertraulich sind, und ergreifen daher nicht die nötigen Vorsichtsmaßnahmen. Fordern Sie die Verfasser auf, die Kopf- oder Fußzeile der Dokumente mit dem Vermerk „Vertraulich“ zu kennzeichnen. Es ist auch möglich, ein Wasserzeichen mit dem Vermerk „Vertraulich“ zu erstellen.

Bemühungen, die Rechte der Betroffenen nach dem BDSG sicherzustellen. Es geht nun primär um die Frage, wer was mit diesen Daten anfangen darf.

Hier beginnt nun die diffizile Aufgabenstellung für den DSB, die entsprechenden Weichen für den befugten Zugriff zu stellen.

Zentraler Begriff: „unbefugt“

Beschränken wir uns zunächst auf den Begriff der Unbefugtheit, ohne dabei in das juristische Deutsch abzuschweifen. Kurzum: Der Datenschutzbeauftragte muss sicherstellen, dass niemand, der die personenbezogenen Daten nicht für sein Aufgaben- und Tätigkeitsfeld benötigt, auf diese Information in irgendeiner Form Zugriff erhält.

Erster Ansatz: Zugriffsberechtigung aus Tätigkeitsbeschreibung ableiten

Die Information, wer was darf, könnte sich z.B. bereits aus der Funktions- oder Tätigkeitsbeschreibung der Mitarbeiter auslesen lassen. Dass ein Beschäftigter aus dem Finanz- und Rechnungswesen nicht Zugriff auf das Informationstableau der Zeiterfassung für alle Angestellten erhält, sollte sich z.B. von selbst verstehen.

Zweiter Schritt: Feintuning innerhalb des Funktionsbereichs

Innerhalb eines Funktionsbereichs oder einer Abteilung sind in der Regel mehrere Beschäftigte aktiv. Hier gilt es, ein gewisses Feintuning zu betreiben:

- Wer darf grundsätzlich im Rahmen seiner Tätigkeit auf personenbezogene Daten zugreifen?
- Wer erhält die Berechtigung zur Neuerfassung, Änderung oder gar Löschung von Daten mit Personenbezug?



Die Zugriffskontrolle soll sicherstellen, dass kein Unbefugter Zugriff auf personenbezogene Daten erhält

Grundprämisse ist ein sauberes Berechtigungskonzept

Um die notwendigen Zugriffsbefugnisse umzusetzen, hat sich in der Praxis immer wieder ein sauberes Berechtigungskonzept bewährt. Nur wer die Struktur seiner Daten wirklich kennt und mit Unterstützung des Verantwortungsträgers die Mitarbeiter entsprechend ihrer Aufgabenstellung zuordnet, kann sich sicher auf der datenschutzkonformen Seite fühlen.

Einen ausführlichen Beitrag dazu, wie Sie solche Konzepte am besten erstellen, lesen Sie in der November-Ausgabe der Datenschutz PRAXIS („Schritt für Schritt zum effektiven Benutzer- und Rollenkonzept“).

Ist die Rechtevergabe nachvollziehbar und dokumentiert?

In der Regel werden Administratoren mit den Einstellungen zur Rechtevergabe beauftragt. Hierbei sollte eine schriftliche Anweisung des Datenverantwortlichen Usus sein. Die noch oft vorherrschende Gewohnheit, kurz te-

lefonisch die Anweisung einer Berechtigungsfreigabe zu erteilen, sollte auf Initiative des Datenschutzbeauftragten unzulässig sein.

Die Zugriffskontrolle geht weit über ein Berechtigungskonzept hinaus

Die Zugriffskontrolle geht jedoch noch weit über die bisher beschriebenen Maßnahmen hinaus. Was ist beispielsweise mit Sicherungsmedien, externen Datenträgern, als vertraulich klassifizierten Dokumenten oder schlicht Müll, sprich: Wie steht es um die datenschutzkonforme Entsorgung?

Mobile Datenträger stets verschlüsseln

Eine dokumentierte Datenträgerverwaltung wäre optimal. Eine grundsätzliche Verschlüsselung beweglicher Datenträger, insbesondere von USB-Speichermedien, ist dagegen unabdingbar. Eine wirkungsvolle Zugriffskontrolle auf verloren gegangene unverschlüsselte Speichermedien ist schlicht nicht umsetzbar.

Zugriffskontrolle auf Datenmüll

Dass auch Datenmüll, sei es in Papierform oder auf Datenträgern, der

Zugriffskontrolle unterliegen muss, sollten Sie als Datenschutzbeauftragter keinesfalls außer Acht lassen. Datenschutzgerechte Entsorgung über entsprechende Schredder verhindert wirkungsvoll unberechtigten Zugriff z.B. durch Reinigungspersonal.

Zur datenschutzkonformen Entsorgung von defekten oder überzähligen Datenträgern finden Sie als Abonnent online unter www.datenschutz-praxis.de verschiedene umfassende und fundierte Fachbeiträge.

Datenabfluss verhindern, Schnittstellen sperren

Zu guter Letzt sei noch auf eine wirkungsvolle Absicherung bzw. Sperre von externen Schnittstellen wie USB-Anschlüssen oder CD-/DVD-Brennern hingewiesen.

Unbeliebt, aber wirksam

Die Zugriffskontrolle verlangt entsprechende Sicherungsmaßnahmen, um das unberechtigte Kopieren von personenbezogenen Daten zu verhindern. Die nach wie vor wirkungsvollste Methode ist dabei schlicht die Deaktivierung der Schnittstellen.

Verkaufen Sie die Zugriffskontrolle als Unternehmensaufgabe

Die vorgestellten Maßnahmen und Empfehlungen lassen sich in den Unternehmen manchmal nicht alle so einfach im Sinne des Datenschutzes umsetzen.

Versuchen Sie es daher einfach mal über eine andere Schiene: Sie werden überrascht sein, was passiert, wenn Sie als DSB Ihre Anregungen nicht ausschließlich für den Schutz personenbezogener Daten, sondern im Rahmen der allgemeinen Datensicherheit vorschlagen.

Jeder Geschäftsführer hat inzwischen von Industriespionage, Datendiebstahl oder über den besonderen Schutz von Unternehmensdaten und Firmen-Know-how gehört. Ob personenbezogene Daten oder zugleich „andere“ Werte geschützt werden, ist letztendlich bedeutungslos. Hauptsache, die Maßnahmen sind wirkungsvoll umgesetzt.

Hermann Keck

Hermann Keck ist externer Datenschutzbeauftragter (www.keck-dsb.de).

Regelung zur Zugriffskontrolle	Erfüllt?	Bemerkung
Bestehen Benutzerprofile hinsichtlich der Zugriffsbefugnisse auf Daten?	<input type="checkbox"/>	
Gibt es differenzierte Berechtigungen für Lesen, Verändern oder Löschen von Daten?	<input type="checkbox"/>	
Ist das Berechtigungskonzept nachvollziehbar in Hinblick auf – die Einrichtung von Administrationsrechten? – die Verwaltung der Zugriffsrechte? – die Erteilung der Rechte?	<input type="checkbox"/>	
Werden die Aktivitäten der Systemadministration kontrolliert?	<input type="checkbox"/>	
Ist eine zeitliche Begrenzung der Zugriffsmöglichkeiten (Nachtabstaltung) implementiert?	<input type="checkbox"/>	
Ist eine datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger sichergestellt?	<input type="checkbox"/>	
Ist eine dokumentierte Datenträgerverwaltung vorhanden?	<input type="checkbox"/>	
Sind externe Schnittstellen wie USB-Anschlüsse und zu sonstigen entnehmbaren Medien (CD-/DVD-Brenner) – sofern nicht für die Aufgabenerfüllung erforderlich – abgesichert?	<input type="checkbox"/>	

Erfüllen Sie die Grundvoraussetzungen für eine datenschutzkonforme Zugriffskontrolle? Die Checkliste finden Abonnenten zum kostenlosen Download unter www.datenschutz-praxis.de/fachwissen/vorlagen/checklisten.