www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT

Ausgabe April 2013 | 12 € zzgl. MwSt.

Quelle: Thinkstock

Alles, aus jedem Grund, zu jeder Zeit?

Welche Auskünfte darf die Datenschutzaufsicht fordern?

Die Datenschutzaufsicht hat Anspruch auf „die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte" (§ 38 Abs. 3 BDSG). Was heißt das genau? Muss der Datenschutzbeauftragte immer Gewehr bei Fuß stehen und auf Anfrage sofort alles sagen können? Der Fall „Unister" hat für den Bereich von Internet-Dienstleistern gezeigt, welche Brisanz hier steckt. Aktionen der Datenschutzaufsicht aus der jüngsten Zeit gegenüber Banken und Kliniken werfen weitere Fragen auf. Vergewissern Sie sich, welche neuen Tendenzen in der Kontrollpraxis bestehen und was das für Sie bedeutet!

Der Klinik-DSB war verblüfft. Vor ihm lag ein Schreiben des Thüringer Landesbeauftragten für Datenschutz, mit dem er sich an alle Krankenhäuser in Thüringen wandte, die sich in öffentlicher Trägerschaft befinden. Gefragt wurde nach Größe, Beteiligungsverhältnissen und verwendeten Krankenhausinformationssystemen.

Anlasslose Auskunft jederzeit?

Gewiss, alles keine wirklichen Geheimnisse. Aber es kam dem DSB doch der Gedanke, ob das alles der Behörde ohne jeden erkennbaren Anlass mitgeteilt werden muss.

Strukturprüfung bei Krankenhäusern

Worum es dem Landesbeauftragten bei seiner flächendeckenden Aktion ging, zeigt ein Blick in seinen Tätigkeitsbericht 2010/2011 (siehe *http://kurzlink.de/Bericht_Thueringen*, S. 98–100, hier S. 98): „Dabei wurde festgestellt, dass insgesamt sechs verschiedene Krankenhausinformationssysteme zum Einsatz kommen. Jedes dieser Systeme sollte einer datenschutzrechtlichen Prüfung unterzogen werden. Daher wurden datenschutzrechtliche Kontrollen

Fortsetzung auf Seite 14

ISSN-Nr. 1614-6867

Datenträger datenschutzkonform entsorgen

Datenträgervernichtung nach der neuen DIN SPEC 66399-3

Ein Umzugsunternehmer war bei einer Krankenkasse damit beauftragt, das Archiv aus- und wieder einzuräumen. Er hatte während der Umzugsarbeiten Zugriff auf alle Karteikarten von Versicherten, die Aktenschränke waren nicht abgeschlossen. Er konnte nach Familienmitgliedern und Freunden suchen. Jahre später kam er erneut zur Versicherung, um die Karteikarten zum Schreddern zu transportieren. Der abschließbare Container stand offen im Hof und wurde dort nach und nach befüllt, bevor er zum Recyclinghof gefahren wurde. Diese Zustände sind in der Praxis kein Einzelfall. Die neue DIN SPEC 66399-3 hilft, solche Pannen zu vermeiden.

Seit dem 1. Februar 2013 gibt es erstmals eine DIN-Spezifikation, die den vollständigen Prozess der Datenträgervernichtung abbildet, so wie er in der Praxis idealerweise gestaltet sein sollte: die DIN SPEC 66399-3.

Erstmals wird nach Datenträgerart unterschieden

Die Besonderheit der neuen DIN 66399, die der DIN-Spezifikation zugrunde liegt und seit Oktober 2012 gilt, ist, dass sie bei der Vernichtung erstmals nach Datenträgern differenziert, angefangen vom Papier bis hin zu hochverdichteten Speicherplatinen. Da Daten auf Papier weniger verdichtet sind als auf einem Speicherchip, bedarf es bei identischer Schutzklasse jeweils anderer Verfahren der sicheren Datenträgervernichtung. Dies stellt die DIN 66399-2 tabellarisch dar und legt je nach Sicherheitsstufe und Art des Datenträgers unterschiedliche Größen von Materialteilchenflächen fest.

DIN SPEC 66399-3 standardisiert den kompletten Vernichtungsprozess

Das Eingangsbeispiel macht jedoch deutlich, dass die Materialteilchenfläche allein völlig unerheblich für die Sicherheit sein kann, wenn Personen während des Transports Zugriff auf die noch nicht entsorgten Daten haben. Für die datenschutzgerechte Entsorgung der Datenträger ist also nicht nur die Vernichtung an sich wichtig, sondern der gesamte Prozess von der Anfallstelle bis zur umweltfreundlichen Verwertung und Beseitigung. Diesen Prozess standardisiert die DIN SPEC 66399-3.

Auftraggeber bleibt Verantwortlicher

In der DIN SPEC heißt es unter 3.1.: „In der Regel läuft der Prozess vom Anfall der zu vernichtenden Datenträger bis zur umweltverträglichen Vernichtung arbeitsteilig ab. Werden Dienstleister in den Prozess einbezogen, so ist die Aufgabenabgrenzung zwischen der verantwortlichen Stelle und dem Dienstleister klar zu regeln. Aufgrund von Rechtsvorschriften sind in diesem Prozess vor allem technische und organisatorische Maßnahmen zu ergreifen.“*

Damit verweist die Spezifikation sowohl auf die technischen und organisatorischen Maßnahmen nach § 9 BDSG Anlage 1 als auch auf die Auftragsdatenverarbeitung (§ 11 BDSG). Sie macht deutlich: Der Auftraggeber, der für die Datenträgervernichtung einen Dienstleister einschaltet, ist für den gesamten Prozess (extern und intern) datenschutzrechtlich weiterhin verantwortlich, und zwar so lange, bis der Datenträger vernichtet ist.

Drei Varianten der Vernichtung

Der Dienstleister ist nach den Vorgaben des § 11 BDSG schriftlich zu beauftragen und vor Auftragsvergabe hinsichtlich der von ihm getroffenen technischen und organisatorischen Maßnahmen unter die Lupe zu nehmen. Die DIN-Spezifikation hilft dabei und enthält standardisierte Kriterien, die im Vorfeld zu prüfen sind. Sie unterscheidet drei Varianten der Datenträgervernichtung:

1. direkt durch die verantwortliche Stelle
2. Datenträgervernichtung vor Ort durch einen Dienstleister
3. Datenträgervernichtung extern durch einen Dienstleister

Welche Prozessschritte sind zu prüfen?

Bei der Variante 1 gliedert die Norm den Vernichtungsprozess zeitlich in:

- „Organisation und Personal“
- „Anfallstelle zur Datenträgervernichtung“
- „Sammeln und gegebenenfalls Lagern“
- „Datenträgervernichtung direkt“

Variante 2 enthält zusätzlich den Prozessschritt „Transport vor Ort“, und

Fragen an das Sicherheitskonzept

Das interne Sicherheitskonzept sollte nach der DIN-Spezifikation folgende Fragen beantworten:

1. Welche Informationen sind schutzwürdig und in welche Schutzklassen einzuordnen?
2. In welcher Sicherheitsstufe wird vernichtet?
3. Wer vernichtet die Datenträger: die verantwortliche Stelle direkt oder ein Dienstleister?
4. Wo vernichtet ein Dienstleister: vor Ort oder extern?
5. Welche technischen und organisatorischen Maßnahmen sind am Anfallort, beim Transport und beim Dienstleister zu beachten?