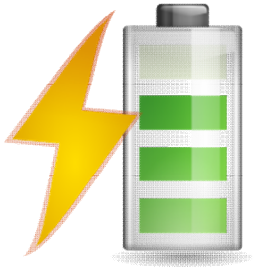
Fälle aus der Datenschutz-Praxis – Ausgabe 2011-9

Überblick über die wichtigsten Änderungen im BDSG



Durch die zum 1. September 2009, 1. April 2010 sowie 11. Juni 2010 in Kraft getretenen Novellen ist eine Reihe von Änderungen eingetreten. Nachfolgend soll nur schlagwortartig eine kurze Übersicht gegeben werden:

- präzisere Definition der Grundsätze der Datenvermeidung und Datensparsamkeit, § 3a
- Stärkung der betrieblichen Datenschutzbeauftragten, § 4f
- Regelungen, unter welchen Voraussetzungen personenbezogene Daten an Auskunfteien übermittelt werden dürfen, § 28a, einschließlich in Teilbereichen Regelungen, inwieweit personenbezogene Daten für die Bonitätsbewertung herangezogen werden dürfen, § 6, 28a Absatz 2 Satz 4, 28 Absatz 3
- Regelungen, unter welchen Voraussetzungen Scoreverfahren im Rahmen von Vertragsverhältnissen eingesetzt werden dürfen, § 28b
- mehr Transparenz:
    - Im Falle automatisierter Einzelfallentscheidungen muss der Betroffene zukünftig umfassender informiert werden, bei ihn beeinträchtigenden Entscheidungen auf Verlangen auch über die wesentlichen Gründe aufgeklärt werden (§ 6a).
    - Bei Ablehnung eines Verbraucherdarlehensvertrages aufgrund von Bonitätsauskünften einer Auskunftei muss der Verbraucher über diese Auskunft unterrichtet werden (§ 29 Absatz 7).
    - Einmal im Jahr müssen insbesondere Auskunfteien auf Antrag kostenlos Auskunft zu den bei ihnen gespeicherten personenbezogenen Daten geben (§ 34 Absatz 8).
    - Beim Einsatz von Scoringverfahren hat der Betroffene einen Anspruch darauf, dass ihm das Zustandekommen seines Scorewertes einzelfallbezogen und nachvollziehbar erläutert wird (§§ 28 b, 34).
    - Informationspflicht bei Datenschutzpannen (§ 42 a).
- schärfere Anforderungen bei der Auftragsdatenverarbeitung (§ 11).
- Einschränkungen bei postalischer Werbung und Adresshandel (§ 28 Absatz 3). Grundsätzlich soll vom Betroffenen eine Einwilligung eingeholt werden. Es gibt jedoch zahlreiche Ausnahmen.
- Verbot der Koppelung des Abschlusses eines Vertrages mit der Einwilligung in die Datenverarbeitung zu Werbezwecken, (§ 28 Absatz 3 b).
- Privilegierung der Markt- und Meinungsforschung bei der Nutzung von Adressdaten (§ 30 a). Eine Datenerhebung, -verarbeitung und -nutzung ist grundsätzlich auch ohne Einwilligung des Betroffenen möglich.
- Einführung einer eigenen Norm zum Arbeitnehmerdatenschutz, (§ 32) einschließlich einer Definition des Begriffs „Beschäftigte“ (§ 3 Absatz 11).
- bessere Sanktionsbefugnisse:
    - die Bußgeldtatbestände wurden erweitert, die Bußgelder erhöht (§ 43).
    - Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich können bei materiell-rechtlichen Verstößen Anordnungen erlassen, etwa Auflagen oder sogar Verbote aussprechen (§ 38 Absatz 5).

Quelle: Bundesbeauftragter für den Datenschutz, Info 1, 15. Auflage vom Januar 2011.

Link: www.datenschutz.bund.de, oder weiterführende Informationen unter www.dbsc.de > Datenschutz > Quick Intro.

Mitarbeiter-Screening

Datenschutzrechtliche Aspekte des Mitarbeiter-Screenings in international tätigen Unternehmen:

Viele Unternehmen sind dazu übergegangen, ihre Mitarbeiter gegenüber Listen abzugleichen, die terrorverdächtige Personen und Organisationen enthalten. Insbesondere Unternehmen, die internationalen Konzernen angehören, werden von ihren teilweise in Drittländern ansässigen Muttergesellschaften hierzu aufgefordert.

Letztere stellen auch darüber hinaus gehende Listen z.B. mit gesuchten Personen zur Verfügung, die aufgrund nationaler Vorschriften in den Drittländern einzusetzen sind. Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zwar kann § 28 Abs. 1 BDSG eine Rechtsgrundlage im Sinne des BDSG sein, diese Vorschrift kann jedoch für ein Screening nicht herangezogen werden.

Der Abgleich mit den Listen dient nicht dem Vertragsverhältnis. Eine Abwägung der Unternehmens- und Betroffeneninteressen führt zu überwiegenden schutzwürdigen Interessen der Betroffenen. Dies gilt insbesondere vor dem Hintergrund, dass die Rechtsstaatlichkeit des Zustandekommens der Listen nachvollziehbar und gesichert sein muss, sowie Rechtsschutzmöglichkeiten bestehen müssen. Angesichts der fehlenden Freiwilligkeit einer solchen Erklärung im Arbeitsverhältnis kann auch das Vorliegen einer Einwilligung eine konkrete Rechtsgrundlage nicht ersetzen.

Feststellung: Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen daher fest, dass im Geltungsbereich des Bundesdatenschutzgesetzes lediglich solche Listen verwendet werden dürfen, für die eine spezielle Rechtsgrundlage im Sinne des § 4 Abs. 1 BDSG vorliegt. In diesem Zusammenhang weisen die obersten Aufsichtsbehörden für den Datenschutz im nicht- öffentlichen Bereich auch auf die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg hin.

Quelle: Tätigkeitsbericht 2009/2010 der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Saarlandes.

BSI Studie zur Cloud Computing Sicherheit

Das Thema Cloud Computing ist derzeit eines der am meisten diskutierten Themen in der Informationstechnik (IT). Hinter dem Begriff Cloud Computing stehen aber weniger neue Technologien, sondern deren Kombination und konsequente Weiterentwicklung ermöglichen neue IT-Services und neue Geschäftsmodelle.

Wie bei vielen neuen Techniken und Dienstleistungen werden auch beim Cloud Computing die Aspekte Informationssicherheit und Datenschutz intensiv diskutiert und durchaus kritischer beleuchtet als bei schon länger vorhandenen Angeboten . Viele Umfragen und Studien zeigen, dass potentielle Kunden Bedenken bezüglich Informationssicherheit und Datenschutz beim Cloud Computing haben, die einem verstärkten Einsatz entgegenstehen. Bei den Nutzern von Cloud – Angeboten muss noch das notwendige Vertrauen aufgebaut werden.

Das BSI hat daher Empfehlungen für sicheres Cloud Computing erstellt, die sich zunächst an Cloud Service Provider (CSP) richten. CSPs haben die Möglichkeiten und die Pflicht, Informationssicherheit in einem angemessenen Umfang umzusetzen.

Das bereitgestellte Eckpunktepapier kann von CSPs als Richtschnur für die Umsetzung von Sicherheitsmaßnahmen genutzt werden. Andererseits können Cloud-Nutzer, die sich mit den vorliegenden Empfehlungen beschäftigen, die CSPs nach deren Umsetzung fragen. Der erste Schritt für einen Cloud-Kunden sollte es jedoch immer sein, sich über die Schutzbedürftigkeit der eigenen Daten und Anwendungen klar zu werden. Davon hängt im Wesentlichen ab, ob und unter welchen Rahmenbedingungen geschäftsrelevante Daten und Anwendungen in die Cloud verlagert werden können.

Quelle: BSI, Bundesamt für Sicherheit in der Informationstechnik 2011.

Link: https://www.bsi.bund.de/DE/Themen/CloudComputing/CloudComputing_node.html

