DBSC Infoletter Datenschutz-Praxis ► 2012-06

Werbung - was gilt ab dem 1.9.2012?

Im 6. Abschnitt des BDSG mit der Fassung vom 1.9.2009 sind Übergangsregelungen für das Wirksamwerden der novellierten Einzelvorschriften definiert. So heißt es im § 47 BDSG, dass "*Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 in der bis dahin geltenden Fassung weiter anzuwenden ...*

1. *für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,*
2. *für Zwecke der Werbung bis zum 31. August 2012.*"

In anderen Worten: Unternehmen, die bis 31. August 2009 Kundendaten für persönlich adressierte Briefwerbung erhoben und diese ohne schriftliche Einwilligung genutzt haben (s.g. "Altdatenbestände"), konnten diese Datensätze in unveränderter Form innerhalb der Übergangszeit von drei Jahren, d. h. bis zum 31. August 2012 verarbeiten. Für den gesetzeskonformen Umgang mit Adressmaterial gelten für Werbetreibende ab dem 1. September 2012 verschärfte Auflagen. Folgende Punkte sollten im Vorfeld sichergestellt werden:

- Der Adressat der Werbung hat der Verwendung seiner Daten zu Werbezwecken ausdrücklich zugestimmt. Dies stellt die sicherste Ausgangsbasis für Werbeaktionen dar! Die Zustimmung muss dabei für jede einzelne Form (i.d.R. per Brief, Telefon, E-Mail, SMS, aber auch andere Formen) vorliegen und nachweisbar sein. Bei elektronischen Verfahren zur Zustimmung ist unbedingt das s.g. Double-Opt-In-Verfahren zu verwenden. Die mündliche Zustimmung sollte unbedingt schriftlich rückbestätigt werden, z.B. mit einer kostenfreien Rückantwortkarte des Adressaten. Lediglich die Quittierung einer (angeblichen) Zustimmung ist angreifbar und als sicherer Nachweis wenig tauglich.
- Der Adressat der Werbung hat niemals der Verwendung seiner Daten zu Werbezwecken widersprochen! Der Widerspruch kann jederzeit gänzlich, oder gegen einzelne Formen (Brief, Telefon, Telefax, E-Mail, SMS, Hausbesuch, Wurfsendung) ausgesprochen werden. Einer erteilten Zustimmung kann jederzeit widersprochen werden. In der Wahl der Übermittlung des Widerspruchs ist der Betroffene frei: So kann z.B. per E-Mail der Zustellung von Wurfsendungen widersprochen werden. Der Widerspruch ist unbedingt beim Adressmaterial zu vermerken; eine Missachtung ist ein schwerwiegender Verstoß in erster Linie gegen das Informationelle Selbstbestimmungsrecht, das BDSG und/oder das UWG. Bei Feststellung eines Verstoßes drohen Unterlassungsklage und/oder Ordnungsstrafen.
- Die Adressdaten liegen dem Unternehmen im Rahmen einer Geschäftsbeziehung oder einer vertragsähnlichen Geschäftsbeziehung vor. Der Werbetreibende darf dann für eigene Produkte oder fremde Produkte (Empfehlungswerbung) werben, bis der Empfänger widerspricht oder nach BDSG die Legitimation zur weiteren Speicherung der Daten entfällt, was i.d.R. meist nach 10 Jahren der Fall ist.
- Wenn der Adressat bislang unbekannt ist, sich aber auf einer s.g. Liste öffentlich zugänglicher Daten befindet, dann kann dessen Adresse für Briefwerbung verwendet werden. Vorsicht: Listendaten nach dem BDSG sind aber keine Kommunikationsdaten, wie z.B. E-Mail-Adressen, Telefon- und Telefax-Nummern. D.h., dass die Entnahme von Daten z.B. aus einem öffentlichen Telefonbuch keinesfalls Telefonanrufe zu Werbezwecken legitimiert. Im Gegenteil: Liegt nicht vorab eine Zustimmung für Telefonanrufe vor, stellt dies einen Verstoß gegen §7 UWG dar.
- Listendaten können auch über den Adresshandel bezogen werden. Der Gesetzgeber meint mit Adresshandel und Werbung offensichtlich unterschiedliche Tatbestände, denn nach §29 BDSG ist nach wie vor der Adresshandel mit Listendaten gesetzlich erlaubt, d. h. die Übermittlung dieser Daten zu beliebigen Werbezwecken, sofern die Lieferkette dokumentiert wird. Unternehmen, die listenmäßig zusammengefasste Adressdaten erwerben (Kauf oder Tausch), dürfen an diese Anschriften persönlich adressierte Werbebriefe für eigene und fremde Angebote senden, sofern folgende Voraussetzungen gegeben sind:

  Die erhebende Stelle, d. h. die ursprüngliche Datenquelle, muss eindeutig aus der Werbung hervorgehen. Sind die Daten über mehrere Unternehmen weitergegeben worden, ist im Werbebrief immer das Unternehmen anzugeben, das als Datenquelle erstmalig diese Daten erhoben hat, also die für den Versand verantwortliche Datenquelle.

Mitarbeiter-Screening - Antiterrorlisten

Dürfen Mitarbeiterdaten mit „Antiterrorlisten“ abgeglichen werden?

Vermutlich will kein Arbeitgeber gerne einen Terroristen oder jemanden beschäftigen, der unter Terrorverdacht steht. Kein Wunder, dass nach den Anschlägen vom 11. September 2001 verstärkte Anstrengungen unternommen wurden, um verdächtigen „Schläfern“ auch in der Arbeitswelt auf die Spur zu kommen. Als Instrument sollen dabei die sogenannten Antiterrorlisten der EU und der Vereinten Nationen zum Einsatz kommen. Ob diese tatsächlich einen nennenswerten Beitrag zur Verhinderung einschlägiger Straftaten leisten können, ist nach wie vor umstritten. Immerhin müssen die Betroffenen mittlerweile aufgrund der Verordnung (EU) 1286/2009 von der EU-Kommission über ihre Aufnahme in die Liste unterrichtet werden und können hierzu auch eine Gegenäußerung abgeben, die dann dem Sanktionsausschuss der Vereinten Nationen zugeleitet wird. Was dort damit geschieht, ist von hier aus ebenso schwer zu beurteilen wie die Frage, wie man überhaupt auf die Liste geraten kann.

In der Praxis besteht unabhängig davon eine erhebliche Unsicherheit, wer unter welchen Voraussetzungen einen Datenabgleich mit den Antiterrorlisten vornehmen darf oder gar muss. In Bezug auf die Arbeitswelt halten die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) einen Abgleich von Mitarbeiterdaten mit „Antiterrorlisten“ durch Unternehmen auf Grundlage von Artikel 2 der Verordnung (EG) Nummer 881/2002 und Artikel 2 der Verordnung (EG) Nummer 2580/2001 für unzulässig. In ihrem Beschluss vom 24. April 2009 begründen sie dies damit, dass Unternehmen für einen automatisierten Abgleich ihrer Mitarbeiter mit Listen, die terrorverdächtige Personen und Organisationen enthalten, nur solche Listen verwenden dürfen, für die eine Rechtsgrundlage vorliegt. Die genannten Verordnungen würden aber dem rechtsstaatlichen Bestimmtheitsgebot nicht genügen. Soweit es auf eine Interessenabwägung ankomme, würden die schutzwürdigen Interessen der von einem Datenabgleich betroffenen Mitarbeiter überwiegen. Nicht zuletzt bestünden Zweifel an der Rechtsstaatlichkeit des Zustandekommens der Listen und unzureichende Rechtschutzmöglichkeiten.

Nach einer mit den übrigen Bundesressorts abgestimmten Mitteilung des Auswärtigen Amts gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sind Unternehmen und andere Wirtschaftsbeteiligte rechtlich nicht zu einem systematischen, anlassunabhängigen Abgleich ihrer Kunden- und Mitarbeiterdaten verpflichtet. Aufgrund des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes bestehe diese Pflicht ausschließlich nach Maßgabe von Sorgfaltspflichten.

Feststellung: Leider sind die sich aus dieser Auskunft ergebenden Konsequenzen für die Praxis weiterhin unklar. Unzulässig dürfte es auf jeden Fall sein, systematisch, flächendeckend und anlassunabhängig die Daten aller Mitarbeiter mit den „Antiterrorlisten“ abzugleichen. Ein Abgleich ist allenfalls dann zulässig, wenn der Dienstherr oder Arbeitgeber im Einzelfall einen konkreten Verdacht hat, dass ein Mitarbeiter zu dem Personenkreis gehört, der in den „Antiterrorlisten“ aufgeführt ist. Soweit Sorgfaltspflichten einen Abgleich gebieten, ist das zu beachten.

Quelle: 30. Tätigkeitsbericht 2010/2011 des LfD Baden-Württemberg

Sichere Nutzung von Web-Angeboten (ISi-Web-Client)

Die Nutzung von Web-Angeboten selbst bringt zahlreiche Gefährdungen mit sich, die spezielle Sicherheitsmaßnahmen erforderlich machen. Über das Web kann es einem Angreifer gelingen, in Systeme einzudringen ("Hacking"), die Benutzer zu täuschen, zu betrügen oder Informationen zu stehlen.

Die Studie ISi-Web-Client gibt Empfehlungen, wie diesen Gefährdungen bei normalem Schutzbedarf zu begegnen ist: durch eine robuste Grundarchitektur des eigenen Netzes, eine geeignete Auswahl der Komponenten, sichere Konfigurationseinstellungen sowie systematische Kontrollmechanismen im Betrieb. Zudem werden Varianten aufgezeigt, die auch einen höheren Schutzbedarf abdecken können. Der Fokus der Studie ISi-Web-Client liegt in erster Linie auf der Anwendungsschicht des TCP/IP-Referenzmodells (Schichten 5-7 im OSI-Referenzmodell) und hier insbesondere auf den beiden Protokollen HTTP und HTTPS. Alle aktuellen Angriffs- und Gefährdungsformen auf dieser Ebene werden von ISi-Web-Client im Detail betrachtet.

Quelle: Bundesamt für Sicherheit in der Informationstechnik, Mait 2012, weiterlesen unter
https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/ISiReihe/ISi-Web-Client/isi-web-client.html