it.sec
security for your information

Die neuen Pflichten aus dem BDSG

Seit 1. September 2009 ist das neue Bundesdatenschutzgesetz (BDSG) in Kraft, welches für die Unternehmen in Deutschland zahlreiche neue Pflichten mit sich bringt. Wir haben Ihnen die wesentlichen Änderungen kurz zusammengestellt und beraten Sie gerne bei der Umsetzung der neuen Aufgaben. Das neue BDSG stellt vor allem hinsichtlich der Auftragsdatenverarbeitung, neuer Informationspflichten und erweiterten Überprüfungsvorgaben wichtige Anforderungen, die ein Unternehmen unbedingt beachten sollte.

Mehr Vorgaben zur Auftragsdatenverarbeitung

Für nahezu alle Unternehmen sind die beschlossenen Verschärfungen zur Auftragsdatenverarbeitung relevant. Waren bisher im schriftlichen Auftrag lediglich die vorgesehene automatisierte Verarbeitung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen, so sind nunmehr nach § 11 Abs. 2 BDSG (neu) im Einzelnen (!) neben Gegenstand und Dauer des Auftrags, die vom Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen und etwaige Befugnisse für Unterauftragsverhältnisse auch der Umfang, die Art und der Zweck der vorgesehenen automatisierten Verarbeitung, die Art der Daten und der Kreis der Betroffenen sowie gegenseitige Verpflichtungen zu Meldungen und Kontrollen zu treffen. Dies erfordert in der Praxis für viele Auftragsarbeiten detaillierte und spezifische Datenschutzverträge und damit erst mal zusätzlichen Aufwand, bestehende Vertragsverhältnisse entsprechend anzupassen.

Desweiteren wurde im neuen BDSG der Auftraggeber dazu verpflichtet, sich sowohl vor Beginn der Datenverarbeitung (bisher vor allem im Rahmen der Vertragsverhandlung geschehen) als auch im laufenden Betrieb (bisher i.d.R. nur bei grundlegenden Auftragstätigkeiten erfolgt) regelmäßig (!) von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und entsprechende Ergebnisse zu dokumentieren. Derartige Auftragskontrollen werden daher selbst ohne ausdrückliche Anpassung von § 4g BDSG in der Praxis überwiegend dem Datenschutzbeauftragten obliegen, zumal nur dieser die erforderliche Fachkunde aufweist, um bestehende Maßnahmen im Sinne des BDSG sachgerecht bewerten zu können. Da nunmehr unzureichende Verträge zu Auftragsarbeiten bzw. unzureichende Auftragskontrollen nach § 43 Abs. 1 Nr. 2b BDSG (neu) ordnungswidrig sind und mit einer Geldbuße bis zu 50.000 € nach § 43 Abs. 3 BDSG (neu) bestraft werden können, wird der Auftragskontrolle jetzt eine hohe Bedeutung beigemessen. Die damit verbundene Formalisierung erzeugt jedoch einigen Mehraufwand.

Neue Informationspflichten und Bußgeldregelungen

Wenn von einer verantwortlichen Stelle – versehentlich oder durch Missbrauch einzelner Personen – unrechtmäßig schützenswerte personenbezogene Daten übermittelt wurden, hat sie dies unverzüglich nach § 42a BDSG (neu) sowohl der zuständigen Aufsichtsbehörde als auch den Betroffenen mitzuteilen. Dabei hat die Information der Betroffenen erst zu erfolgen, sobald angemessene Maßnahmen zur Datensicherung ergriffen wurden und die betreffende Strafverfolgung nicht mehr gefährdet wird. Sofern die Betroffenen z.B. aufgrund der Vielzahl der betroffenen Fälle nicht direkt informiert werden können, sind halbseitige Anzeigen in zwei bundesweit erscheinenden Tageszeitungen zu schalten oder hat eine ebenso wirksame Veröffentlichung in anderer Form zu erfolgen (z.B. bei einem Online-Portal auf den beim Zugang aufzurufenden Web-Seiten).

Diese neue Informationspflicht ist ebenfalls strafbewährt: Nach § 43 Abs. 3 i.V.m. Abs. 2 Nr. 7 BDSG (neu) kann dies mit einer Geldbuße bis zu 300.000 € bestraft werden. Kann aus dem Vergehen gar ein wirtschaftlicher Vorteil erwachsen, der oberhalb der Geldstrafen anzusetzen ist, kann neuerdings auch ein höheres Bußgeld verhängt werden. Wenn eine verantwortliche Stelle dem Auskunftsersuchen von Betroffenen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig nachkommt, ist dieses nunmehr auch (wenn auch mit dem geringeren Satz) bußgeldrelevant nach § 43 Abs. a Nr. 8a bis 8c BDSG (neu).

Umfassende Überarbeitungen und Überprüfungen nötig

Im § 28 Abs. 1 Nr. 1 BDSG (neu) wurde bei der automatisierten Verarbeitung personenbezogener Daten zu eigenen Geschäftszwecken (analog zum öffentlichen Bereich) ausdrücklich auf den Erforderlichkeitsgrundsatz verwiesen und zugleich die bestehenden Termini („Vertragsverhältnis“ und „vertragsähnliches Vertrauensverhältnis“) auf entsprechende Termini aus dem Schuldrecht („rechtsgeschäftliches Schuldverhältnis“ und „rechtsgeschäftsähnliches Schuldverhältnis“) angepasst.

Während bei Letzterem in der Praxis „nur“ davon auszugehen ist, dass zahlreiche textuelle Überarbeitungen nötig werden, bedeutet Ersteres, dass jetzt strengere Kriterien anzulegen sind, ob eine vorgesehene automatisierte Verarbeitung im geplanten Umfang noch zulässig ist oder nicht. Dies setzt nunmehr ein positives Prüfergebnis (Verifikation) voraus. Bisher reichte eine Feststellung über fehlende Nichterforderlichkeit (Falsifikation) aus. Die bei vielen verantwortlichen Stellen insofern nachzuziehenden Detailprüfungen werden somit ebenfalls einigen Mehraufwand erzeugen.

it.sec
security for your information

Bei jeder Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Allgemeinen und bei der Verwendung personenbezogener Daten zum Zweck der Werbung ohne vorliegende Einwilligung der Betroffenen im Besonderen wurde der Grundsatz der Datenvermeidung und Datensparsamkeit verankert. Dies ist zwar weiterhin nicht strafbewährt, stellt jetzt aber nicht mehr nur eine besondere Anforderung an DV-Systeme dar.

Das Widerspruchsrecht der Betroffenen bezieht sich nach dem novellierten BDSG nicht mehr nur auf Nutzung oder Übermittlung, sondern auch auf die anderen Phasen der Verarbeitung gemäß § 28 Abs. 4 BDSG (neu), weiterhin jedoch nicht auf die Erhebung. Die Nichteinhaltung des Widerspruchsrechts kann nunmehr auch mit einem höheren Bußgeld geahndet werden nach § 43 Abs. 2 Nr. 5b BDSG (neu). Die Herkunft listenmäßig übermittelter Datensätze ist nach § 34 Abs. 1a BDSG (neu) zwei Jahre lang zu speichern und Betroffenen im Rahmen des Auskunftsrechts mitzuteilen.

Sonstiges

Für den Umgang mit Beschäftigtendaten (inkl. der Daten von Bewerbern und ausscheidenden Mitarbeitern) wurde ein eigener Paragraph geschaffen (§ 32 BDSG), welcher ebenfalls ausdrücklich auf das Erforderlichkeitsprinzip abhebt und Kontrollen einer entsprechenden Verhältnismäßigkeitsprüfung unterwirft. In diesem Zusammenhang wurde eine Legaldefinition über „Beschäftigte“ eingefügt (§ 3 Abs. 11 BDSG).

Fortbildungskosten des Datenschutzbeauftragten hat die verantwortliche Stelle nunmehr durch unmittelbaren Gesetzeswortlaut (und nicht mehr nur aufgrund ihrer Unterstützungspflicht) zu tragen. Interne Datenschutzbeauftragte erhalten i.d.R. einen Kündigungsschutz auch über die Tätigkeitsdauer als Datenschutzbeauftragter hinaus. Schließlich wurden zur Datenübermittlung an Auskunfteien (§ 28a BDSG) und zum Scoring (§ 28b BDSG) neue Paragraphen verabschiedet, rundet die Verpflichtung zur inhaltlichen Bewertung automatisierter Einzelentscheidungen anstelle einer reinen Überprüfungsverpflichtung (§ 6a Abs. 1 BDSG) bzw. zur Begründung der Entscheidung gegenüber dem Betroffenen (§ 6a Abs. 2 Nr. 2 BDSG) und die strenge Zweckbindung von Daten, die im Rahmen der Gewährleistung von Betroffenenrechte anfallen (§ 6 Abs. 3 BDSG), die umfassende Novelle ab.

Bernhard C. Witt
Berater für Datenschutz und IT-Sicherheit

[Berater für Datenschutz und IT-Sicherheit bei der it.sec GmbH & Co. KG, Diplom-Informatiker, geprüfter fachkundiger Datenschutzbeauftragter (UDIS), Lehrbeauftragter für Datenschutz und IT-Sicherheit an der Universität Ulm (seit 2005), Autor der Bücher "IT-Sicherheit kompakt und verständlich" (2006) und "Datenschutz kompakt und verständlich" (2008), Sprecher der GI-Fachgruppe Management von Informationssicherheit und Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit]

it.sec
security for your information

Über it.sec

Die it.sec ist auf Sicherheitsberatungen und Komplettlösungen rund um das Thema der Informationssicherheit spezialisiert. Das Unternehmen wurde 1996 von Holger Heimann in Ulm gegründet und realisiert seitdem ganzheitliche Security-Konzepte für namhafte Unternehmen im In- und Ausland. Das Portfolio umfasst umfassende Beratungsleistungen rund um das Thema der IT-Sicherheit und Verfügbarkeit. Die Schwerpunkte bilden die Themen: Informationssicherheit, Datenschutzberatungen, IT-Risk-Management, Security Governance/Risk- & Compliance Consulting, Penetrationstest, IT-Forensics, Security Architecture Design und Reviews, ISO/IEC 2700x, BCM, BSI Grundschutzkataloge, Security GRC in SCADA Systems, Web-Application Security, Data Integrity, Hardening, PCI-Security, SOA and Web Services Security, Security Products: Web Application Firewall, IDS/IPS, SIEM, Content Security, Authentication & Authorization, PKI, Verschlüsselung, Firewall, HSM (Application & Transaction Security)

Kontakt

Hauptsitz

it.sec GmbH & Co. KG
Einsteinstrasse 55
D-89077 Ulm

Fon +49(0)731-20589-0
Fax +49(0)731-20589-29

Office München

Trimburgstrasse 2
D-81249 München

Fon +49(0)89-680940-30
Fax +49(0)89-680940-31

eMail info@it-sec.de
http:// www.it-sec.de