whitepaper Novellierung

Datenschutz 2009

Nach der letzten „großen“ Erneuerung des Bundesdatenschutzgesetzes im Mai 2001 (Datensparsamkeit, CD-ROM, Chipkarten, Videoüberwachung, EU- Datenschutzrichtlinie) sind im Sommer 2009 drei Novellierungen beschlossen worden.

Am 12. Juni 2009 hat der Bundesrat die sogenannte BDSG-Novelle I verabschiedet, sie tritt am 1. April 2010 in Kraft.

- die Zulässigkeit der automatisierten Einzelentscheidungen
- Scoring
- Datenübermittlung an Auskunfteien
- Rechte des Betroffenen erweitert

Am 10. Juli 2009 hat der Bundesrat die sogenannte BDSG-Novelle II verabschiedet.

- Änderung der Zulässigkeit der personalisierten Werbung
- Arbeitnehmerdatenschutz
- Auftragsdatenverarbeitung neu gestaltet
- Informationspflichten der Unternehmen bei Datenschutzpannen
- Verschärfte Straf- und Bußgeldvorschriften und erweiterte Kompetenzen der Aufsichtsbehörden
- Stärkung der Rechtsstellung des betrieblichen Datenschutzbeauftragten

Diese Regelungen treten am 1. September 2009 in Kraft. Für die personalisierte Werbung gibt es eine Übergangsfrist.

Die BDSG-Novelle III ist eine Umsetzung aus den Anforderungen der Verbraucherkreditrichtlinie und soll weitere Transparenz schaffen.

Sie tritt am 11.06.2010 in Kraft.

Akuter Handlungsbedarf

Wie nachfolgend dargestellt, ergibt sich aus den Novellierungen, je nach Art des Unternehmens und der Geschäftstätigkeit, ein konkreter bis akuter Bedarf zum Handeln.

Während die Zulässigkeit der automatisierten Einzelentscheidungen, die Regelungen zum Scoring, die Datenübermittlung an Auskunfteien sowie die Änderungen in der Zulässigkeit der personalisierten Werbung vorwiegend „nur“ die Unternehmen des Handels, die Werbetreibenden und das Kreditgewerbe betreffen, sind die Novellierungen zum Arbeitnehmerdatenschutz und die Neuregelungen zum Outsourcing für fast alle Unternehmen relevant.

Akuter Handlungsbedarf für fast alle Unternehmen besteht aus unserer Erfahrung

- - für den Abschluss und die Gestaltung von Verträgen mit externen Dienstleistern (Outsourcing)
- - die Regelungen zur Auskunft Betroffener
- - im Bereich des Arbeitnehmerdatenschutzes
- - die Erhebung von Daten zu Werbezwecken

Besonders relevant sind diese Punkte, da Verstöße jetzt mit einem erhöhten Bußgeld geahndet werden können und im Fall von Datenschutzpannen eine Informationspflicht besteht.

Auf den folgenden Seiten sind die Änderungen, die sich aus der Novellierung ergeben, dargestellt.

Automatisierte Einzelentscheidungen

§ 6a Automatisierte Einzelentscheidung
(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. *Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.*
(2) Dies gilt nicht, wenn
1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder
2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert. Als geeignete Maßnahme gilt insbesondere die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist verpflichtet, ihre Entscheidung erneut zu prüfen.

Z.B. dürfen Kredit- oder Ratenkaufentscheidungen nicht alleine auf dem extern oder intern ermittelten Scorewerte basieren. Die Änderung betrifft die Definition der automatisierten Entscheidung. Diese liegt jetzt immer dann vor, wenn keine inhaltliche Bewertung und Entscheidung durch einen Mitarbeiter stattfindet. Zukünftig reicht es also nicht mehr, die vorgegebenen Scorewerte nur abzusegnen. Entscheider müssen die Entscheidungsgründe inhaltlich bewerten. Das betrifft „nur“ die Negativentscheidungen (Abs. 2).

TIPP! Unternehmen müssen den Betroffenen auf deren Verlangen die wesentlichen Gründe für die Entscheidung erläutern. Hier sollten Sie Ihre internen Prozesse anpassen. Lassen Sie sich beraten, wenn Sie bislang (interne oder externe) Scoringwerte oder automatisierte Einzelfallentscheidungen nutzen.

Datenübermittlung an Auskunfteien

§ 28a Datenübermittlung an Auskunfteien
(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und
1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,
2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,
3. der Betroffene die Forderung ausdrücklich anerkannt hat,

4.a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,
b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,
c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und d) der Betroffene die Forderung nicht bestritten hat oder
5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung
unterrichtet hat.
Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.
(2) Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und
Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten.
Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauens-verhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.
(3) Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

Hier wird die Übermittlung von Negativinformationen an Auskunfteien geregelt. Die Übermittlung von Positivdaten richtet sich nicht nach §28a BDSG.

TIPP! Informationen über vorherige Mahnungen durch andere Unternehmen (sog. Frühindikatoren) werden in Zukunft nicht mehr möglich sein. Sie sollten bedenken, dass externe Scorewerte zukünftig wohl „positiver“ ausfallen werden. Die in Abs. 3 beschriebene Nachberichtspflicht sollten Sie bereits jetzt als Prozess mit den Auskunfteien erarbeiten.

Scoring

§ 28b Scoring
Zum Zwecke der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn
1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,
2. im Falle der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29, und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,
3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,
4. im Falle der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist. Die Unterrichtung ist zu dokumentieren.

Diese Verpflichtung betrifft alle Unternehmen, die Entscheidungen aufgrund von Scoring treffen. TIPP! Den Nachweis für die Nutzung eines wissenschaftlich anerkannten mathematisch- statistischen Verfahrens müssen Sie als Anwender erbringen. Das sollten Sie dokumentieren. Beim Geoscoring (Ziffer 3) dürfen für die Berechnung von Wahrscheinlichkeitswerten nicht nur auf Grundlage der Adressdaten erfolgen. Der Betroffene ist vor der Berechnung von Scorewerten über die Nutzung von Anschriftendaten zu informieren. Auch das müssen Sie dokumentieren.

Rechte des Betroffenen

Beispielhaft für die Erweiterung der Rechte des Betroffenen werden hier die Änderungen im §34 Auskunft an den Betroffenen erläutert. Auf den Abdruck des Gesetztexts wurde aufgrund der Länge verzichtet.

TIPP! Im Bereich des Scorings wird der Anspruch auf Auskunft erheblich erweitert. So müssen Sie Auskunft erteilen über die innerhalb der letzten sechs Monate erhobenen Wahrscheinlichkeitswerte, die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten sowie die Berechnungsgrundlagen sowie deren Bedeutung für den Einzelfall (nachvollziehbar und allgemein verständlich). Die Auskunft ist unentgeltlich und auf Verlangen in Textform zu erteilen. Verstöße gegen den Auskunftsanspruch sind in den Bußgeldkatalog (§43 BDSG) aufgenommen worden.

Änderung der Zulässigkeit der personalisierten Werbung

Die Änderungen sind in dem §28 BDSG dokumentiert. Auswirkungen sind insbesondere die geforderte Schriftform, im Falle der elektronischen Zustimmung zur Nutzung von personenbezogenen Daten (z.B. im Internet) muss dieses dokumentiert werden, jederzeit einsehbar und jederzeit widerrufbar sein. Listenmäßig erfasste Daten dürfen auch zukünftig ohne Zustimmung der Betroffenen weitergegeben werden (sog. Listenprivileg), allerdings nur stark eingeschränkt. So sind die Weitergabe und Herkunft für einen Zeitraum von zwei Jahren zu dokumentieren. Für Daten, die ab dem 1. September 2009 erhoben werden gelten die Regelungen ab sofort- für sog. Altdaten gilt eine Übergangsfrist bis zum 1. August 2010 (Meinungsforschung) oder bis zum 31. August 2012 (Werbung).

Verstöße gegen diese Vorschriften werden mit Bußgeld geahndet.

TIPP! Passen Sie umgehend >Ihre Prozesse und Abläufe sowie die Dokumentation an!

Arbeitnehmerdatenschutz

Die Neuregelungen zum Arbeitnehmerdatenschutz finden sich in §32.

§ 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.
(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.
(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

Neu ist die Regelung, die zur Aufdeckung von Straftaten führt. Hier sind der Anfangsverdacht und das Vorgehen im Einzelfall zu dokumentieren. Hiermit soll das Massenscoring verhindert werden. Die Regelungen gelten auch für nicht-elektronische Unterlagen, wie Akten und handschriftliche Aufzeichnungen.

TIPP! Etablieren Sie hier Verfahren und Abläufe, die eine rechtssichere Dokumentation gewährleisten!

Auftragsdatenverarbeitung

Die Änderungen zur Auftragsverarbeitung sind in dem schon bestehenden §11 BDSG dokumentiert.

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.
(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im
Einzelnen festzulegen sind:
1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden
Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.
Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
Das Ergebnis ist zu dokumentieren.

TIPP! Die für das Outsourcing notwendigen zu dokumentierenden Verfahren und Kontrollen sind jetzt definiert. Hier ergibt sich aus unserer Erfahrung für fast jedes Unternehmen ein konkreter Handlungsbedarf. Bei Verstößen drohen auch hier Bußgelder.

Informationspflichten der Unternehmen bei Datenschutzpannen

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nicht öffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte
1. besondere Arten personenbezogener Daten (§ 3 Absatz9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
4. personenbezogene Daten zur Bank- und Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlung für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungs-pflichtigen verwendet werden.

Bei Datenschutzverstößen, bei denen sensible personenbezogene Daten (Gesundheit, politische Überzeugungen,…), Daten, die einem Berufsgeheimnis unterliegen oder Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten beziehen sowie bei Bank und Kreditkartendaten ist das Unternehmen verpflichtet, die Betroffenen umgehend zu informieren, ggf. auch durch halbseitige Zeitungsanzeigen in bundesweit erscheinenden, überregionalen Zeitungen.

TIPP! Wenn Sie mit genannten Daten umgehen, so empfiehlt es sich dringend für den „Ernstfall“ Prozesse und Abläufe definiert zu haben.

Verschärfte Straf- und Bußgeldvorschriften und erweiterte Kompetenzen der Aufsichtsbehörden

Die Tatbestände, die zur Verhängung von Bußgeldern und Strafen führen können, sind erheblich ausgeweitet worden. Die Höhe der Bußgelder ist bei als leichter eingestuften Ordnungswidrigkeiten auf 50.000 € verdoppelt worden. In schweren Fällen drohen sogar Bußgelder bis 300.000€. Aus Datenschutzverstößen erzielte Gewinne können zukünftig abgeschöpft werden.

Zusätzlich zur Verhängung von Bußgeldern ist es den Datenschutzaufsichtsbehörden nunmehr auch erlaubt, Geschäftspraktiken zu untersagen.

Stärkung der Rechtsstellung des betrieblichen Datenschutzbeauftragten

Der betriebliche Datenschutzbeauftragte genießt in Zukunft einen erweiterten Kündigungsschutz (§4f BDSG). Er ist während seiner Berufung und ein Jahr nach Beendigung der Tätigkeit nur aus wichtigem Grund kündbar. Der Anspruch auf Fort- und Weiterbildung ist jetzt gesetzlich festgeschrieben.

Wichtiger Hinweis:

Diese Zusammenstellung und die enthaltenen Tipps und Handlungsempfehlungen erheben nicht den Anspruch auf Vollständigkeit und können / sollen in keinem Fall eine Rechtsberatung ersetzen!

edsb.de
Bernd H. Sievers

sievers@edsb.de

fon +49-(0)2205-947 69 50