Datenschutz
für die betriebliche Praxis

Erfüllung datenschutzrechtlicher
Anforderungen in der Privatwirtschaft

- Informationsbroschüre -

procedo Unternehmensberatung GmbH
Ammerländer Heerstraße 231
D-26129 Oldenburg

Oldenburg, den 04.08.2009

INHALTSVERZEICHNIS

1. ANFORDERUNGEN ZUR EINHALTUNG DES DATENSCHUTZES

1.1. Gesetzliche Verpflichtung der Unternehmung

Das Bundesdatenschutzgesetz (BDSG) verpflichtet Unternehmen zum Schutz personenbezogener Daten bei EDV-mäßiger Verarbeitung (nutzen, speichern, verändern, weitergeben) und Erhebung. Verantwortlich für die Umsetzung des Datenschutzes ist die Geschäftsführung oder ein von dieser bestellter Beauftragter. Die Einhaltung des Datenschutzrechtes wird von den Aufsichtsbehörden kontrolliert, Verstöße können mit einem Bußgeld von derzeit bis zu 250 T€ geahndet werden.

1.2. Personenbezogene Daten im Fokus des Datenschutzes

Zu den personenbezogenen Daten zählen unter anderem Adresse, Telefonnummer, Geburtsdatum, Foto, Video, Gehalt, Vermögen, Besitz, Lebenslauf, Arbeitgeber, Arbeitsverhalten, Arbeitsergebnisse, Personalnummer, PC Benutzerkennung, Telefonverbindungsdaten, Nutzerverhalten im Internet, Konsumentenverhalten.

Besonders schützenswerte personenbezogene Daten sind Informationen über ethnische Herkunft, politische Meinungen, Gesundheit, Sexualleben, religiöse Überzeugungen und Gewerkschaftszugehörigkeit. Personenbeziehbare Daten (z.B. IP-Adresse eines Internetnutzers) sind vergleichbar zu schützen wie personenbezogene Daten.

1.3. Erfordernis des Datenschutzes durch den Auftraggeber/Kunden

Eine wachsende Anzahl von Unternehmen, die gesetzlich zur Einhaltung des Datenschutzes verpflichtet sind, verpflichten auch ihre Auftragnehmer durch eine Integration von Datenschutzklauseln in die allgemeinen Lieferbedingungen zur Einhaltung des Datenschutzes. Auftraggeber sind unter bestimmten Voraussetzungen zur Kontrolle der Datenschutzorganisation der Auftragnehmer verpflichtet.

Die Erwartung der Endkunden an Unternehmen, vertrauensvoll mit ihren personenbezogenen Daten umzugehen, hat in den vergangenen Jahren dazu geführt, dass viele Unternehmen Datenschutz in Form einer Privacy Policy oder Datenschutzerklärung kommunizieren, um das Vertrauen der Endkunden zu bestärken.

1.4. Mitarbeitererwartungen an den Schutz ihrer Persönlichkeitsrechte

Mitarbeiter und Arbeitnehmervertreter erwarten einen adäquaten Schutz ihrer Privatsphäre durch den Datenschutzbeauftragten während der Erfüllung eines Arbeitsvertrages. Insbesondere bei Video- und Telefonüberwachungen, der Nutzung von Personalinformationssystemen, der Nutzung von Internetdiensten am Arbeitsplatz sowie bereits beim Bewerbungsprozess wird Datenschutz relevant.

2. AKTUELLE HERAUSFORDERUNGEN IM DATENSCHUTZ

2.1. Teilweise mangelnde Sensibilität und interne Kontrollen

Mangelnde Sensibilität für Datenschutzbelange sowie die Vernachlässigung von internen Kontrollen bei im Auftrag datenverarbeitenden Stellen führten zu einer zunehmenden Anzahl von gravierenden Verstößen gegen das Datenschutzrecht.

2.2. Klage und Beschwerden bei Verletzung von Persönlichkeitsrechten

Einzelfälle belegen, dass Arbeitnehmer oder Arbeitnehmervertretungen bei gravierender Verletzung ihrer Privatsphäre durch Videoüberwachung oder Telefonüberwachung inzwischen bereit sind, gegen die Verletzung ihrer Privatsphäre zu klagen. Hohe Aufwendungen für Rechtsanwälte und Imageschäden können infolge eines öffentlichen Gerichtsverfahrens entstehen. Am häufigsten werden Bußgeldverfahren eingeleitet.

2.3. Forderung nach mehr Regulierung und staatlicher Kontrolle

Eine stärkere Regulierung für den Bereich der Verarbeitung personenbezogenen Daten ist neben der Forderung nach mehr staatlicher Kontrolle durch die Aufsichtsbehörden zentrale Forderung von Medien, Datenschützern und Politik. Eine signifikante Erhöhung der Bußgelder wird ebenfalls angestrebt. Sogar das Wirtschaftsministerium unterstützt die Forderungen nach stärkerer Regulierung.

2.4. Bekenntnis der Unternehmen zu stärkerer Selbstverpflichtung

Eine Initiative deutscher Großunternehmen zur stärkeren Selbstverpflichtung im Bereich Datenschutz unter Begleitung des für den Datenschutz zuständigen Bundesinnenministeriums versucht den gegenwärtigen Forderungen nach stärkerer Regulierung entgegenzuwirken.

2.5. Novellierung des Bundesdatenschutzgesetzes

Im Juli 2009 wurde das BDSG in zwei Stufen umfassend novelliert. Die Neuregelungen treten bereits im September 2009 in Kraft. Diese betreffen den Arbeitnehmerdatenschutz, die personalisierte Werbung, Änderungen in Bezug auf die Auftragsdatenverarbeitung und die Bußgeldhöhe (bis 300 T€).

Im April 2010 tritt die zweite Stufe der Novellierung des BDSG in Kraft. Diese regelt die Rechte der Betroffenen, Scoringverfahren und die Anforderungen an die automatisierte Einzelentscheidung neu.

3. WAS FÄLLT UNTER DATENSCHUTZ?

3.1. Schutz personenbezogener und personenbeziehbarer Daten

Personenbezogene Daten sind durch die Implementierung entsprechender organisatorischer und technischer Maßnahmen zu schützen. Unter personenbezogenen Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zu verstehen.

3.2. Praxisbeispiel Videoüberwachung

Die Geschäftsführung einer GmbH entscheidet sich, eine Videoanlage auf dem Betriebsgelände zu installieren. Nachdem die Videokameras in Betrieb genommen wurden, wendet sich eine Mitarbeiterin an den Betriebsrat und Geschäftsführung, weil die Kamera mit dem 180° Erfassungsumfeld Bilder von ihrem Arbeitsplatz aufnimmt und diese für mehr als eine Woche gespeichert werden. Die Geschäftsführung erklärt, sie wolle durch die Videoaufzeichnungen Diebstahl entgegenwirken.
Da das Unternehmen keine Datenschutzbeauftragten bestellt hat, wird ein externer Datenschutzexperte kontaktiert. Dieser stellt fest, dass weder die nach dem Bundesdatenschutzgesetz vorgeschriebene Vorabkontrolle durchgeführt, noch die Hinweispflicht auf die Videoüberwachung erfüllt, noch eine ordnungsgemäße Dokumentation der Videoüberwachung erstellt wurde. In der Regel ist auch nur eine Speicherung von bis zu zwei Werktagen erlaubt.

3.3. Praxisbeispiel Auftragsdatenverarbeitung

Eine Vertriebsgesellschaft mit größerem Kundenstamm, die Wert auf den vertrauensvollen Umgang mit ihren Kundendaten legt, beauftragt einen EDV-Dienstleister mit der Fernwartung ihrer EDV-Systeme. Dieser erhält vollen Zugriff auf die EDV-Systeme und die Kundendaten. Weil die Vertriebsgesellschaft gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, nimmt dieser die Kontrollpflichten bei der Auftragsdatenverarbeitung durch den EDV-Dienstleister wahr.
Der Datenschutzbeauftragte stellt eine mangelnde Verpflichtung der Mitarbeiter des EDV-Dienstleisters auf das Datengeheimnis gemäß Bundesdatenschutzgesetz fest. Organisatorische und technische Maßnahmen zur Einhaltung des Datenschutzes und der Datensicherheit existieren beim EDV-Dienstleister nicht. Die Vertriebsgesellschaft verlangt die Einhaltung des Datenschutzes wie in den Lieferbedingungen vereinbart und droht mit dem Entzug des Auftrags. Daraufhin beruft der EDV-Dienstleister einen externen Datenschutzbeauftragten.

4. BESTELLUNG EINES DATENSCHUTZBEAUFTRAGTEN

4.1. Gesetzliche Verpflichtung zur Bestellung

Die gesetzliche Verpflichtung zur Bestellung eines Datenschutzbeauftragten liegt vor, wenn in einem Unternehmen mehr als neun Mitarbeiter mit der Verarbeitung personenbezogener Daten beschäftigt sind (§ 4 f BDSG).

4.2. Bestellung zur Reduzierung von Meldepflichten

Eine Bestellung unabhängig von der Anzahl der Mitarbeiter, die personenbezogene Daten verarbeiten, erfolgt in der Praxis häufig, um der Meldepflicht bei den Aufsichtsbehörden für Verfahren automatisierter Verarbeitung personenbezogener Daten zu entgehen.

4.3. Bestellung zur Erfüllung von Kundenerwartungen

Aus der vertraglichen Verpflichtung zur Einhaltung des Datenschutzes durch einen Auftraggeber (u.a. öffentliche Institutionen, größere Unternehmen) resultiert in der Regel als erster Schritt zur Erfüllung der Lieferbedingungen der Nachweis der Bestellungsurkunde des Datenschutzbeauftragten gegenüber dem Auftraggeber.

4.4. Bestellung als Kontrollorgan und zur Risikominimierung

Unter Gesichtspunkten der Risikominimierung versuchen Unternehmen, denen Bußgelder, Imageschäden und höhere Schadensersatzforderungen Dritter durch Verstöße gegen den Datenschutz entstehen können, die Verantwortung für den Datenschutz auf externe Datenschutzbeauftragte zu übertragen. Die ordnungsgemäße Einhaltung wird durch den unabhängigen Externen überwacht.

5. AUFGABEN DES DATENSCHUTZBEAUFTRAGTEN

5.1. Übernahme der Verantwortung für den Datenschutz

Die Übernahme der Verantwortung für den Datenschutz umfasst mindestens die Durchführung der gesetzlich vorgeschriebenen Aufgaben.

- Beschreibung der Verfahren automatisierter Verarbeitung und Erstellung von öffentlichen Verfahrensverzeichnissen,
- Durchführung von Vorabkontrollen bei Modifikation bestehender oder Installation neuer Datenverarbeitungsverfahren,
- Verpflichtung der Mitarbeiter auf das Datengeheimnis,
- Schulung der Mitarbeiter zur Sensibilisierung für Vorschriften aus dem Datenschutzrecht,
- Überprüfung technischer Verfahren und organisatorischer Abläufe,
- Vertretung des Unternehmens gegenüber den Aufsichtsbehörden nach Abstimmung mit der Geschäftsführung und
- Beratung der Geschäftsführung in Datenschutzbelangen, um auf die Einhaltung des Datenschutzes hinzuwirken.

5.2. Erarbeitung und Dokumentation eines Datenschutzkonzeptes

Über die derzeit gesetzlichen Verpflichtungen hinaus erarbeiten wir in Abstimmung mit der Geschäftsführung eine Dokumentation aller ablauf-organisatorischer Regelungen mit Bezug zum Datenschutz in Form eines Handbuches, um diese den Mitarbeitern zu kommunizieren. Hierzu zählt:

- Erarbeitung eines firmenindividuellen Datenschutzkonzeptes,
- Zusammenfassung aller ablauforganisatorischer Regelungen im Datenschutzhandbuches,
- Transparente Dokumentation der Durchführung gesetzlich vorgeschriebener Aufgaben im Datenschutzhandbuch und
- Anpassung der Datenschutzorganisation infolge gesetzlicher Novellierungen.

5.3. Überwachung der Einhaltung des Datenschutzes

Um auf die Ordnungsgemäßheit der Datenverarbeitung hinzuwirken, müssen die Verfahren automatisierter Verarbeitung und die gesamte Datenschutzorganisation in regelmäßigen Abständen überprüft werden. Folgende Prüfungen nehmen wir vor:

- Überprüfung technischer Verfahren und organisatorischer Abläufe in Form von Audits (Beleg-, Verfahrens-, und EDV-Prüfungen sowie Sichtkontrollen),
- Auditierung einzelner Funktionsbereiche (EDV, Personal, Einkauf) und Dokumentation ermittelter Schwachstellen,
- Überprüfung der Einhaltung der Anforderungen an Auftragsdatenverarbeitungen bei Auftraggeber und Auftragnehmer sowie
- Empfehlung, Planung, Umsetzung und Überwachung von Korrekturmaßnahmen in Absprache mit den Verantwortlichen.

5.4. Berichterstattung an die Geschäftsführung

Der betriebliche Datenschutzbeauftragte ist nach dem Bundesdatenschutzgesetz bei der Wahrnehmung seiner Tätigkeit der Geschäftsführung direkt unterstellt. Folglich berichten wir laufend an die Geschäftsführung:

- Berichterstattung in Form von Datenschutzprotokollen, die das Ergebnis eines Audits, Empfehlungen zur Sicherstellung der Einhaltung des Datenschutzes und den Status der Maßnahmenumsetzung darstellen,
- Jährliche Erstellung eines umfassenden Datenschutzberichtes zu Beginn eines neuen Kalenderjahres, der Ergebnisse, Tätigkeiten und Maßnahmen des Datenschutzbeauftragten im Berichtszeitraum ausweist.

6. WEITERE INFORMATIONEN UND KONTAKT

Falls Sie weiterhin Interesse an fachlicher Expertise zum betrieblichen Datenschutz besitzen oder offene Fragen zur Notwendigkeit einer Bestellung eines Datenschutzbeauftragten in ihrem Unternehmen verblieben sind bzw. uns und das Vorgehen der Datenschutzbeauftragten der procedo Unternehmensberatung näher kennen lernen möchten, stehen wir Ihnen für Rückfragen und persönliche Gesprächstermine jederzeit gerne zur Verfügung.

procedo Unternehmensberatung GmbH
Ammerländer Heerstraße 231
26129 Oldenburg

Tel.: 0441 – 77 92 945
E-mail: rangosch@procedo-gmbh.de

Mit freundlichen Grüßen

procedo Unternehmensberatung GmbH

Dipl.-Wirtschaftsing. Günter Rangosch
(Datenschutzbeauftragter)

Dipl.-Hdl. Christoph Schultejans
(Datenschutzbeauftragter)