

Anfang Juli wurde vom Bundestag eine Änderung des Bundesdatenschutzgesetzes mit **z. T. nicht zu unterschätzenden Auswirkungen auf die Unternehmen beschlossen**. Folgende Änderungen wurden u. a. vorgenommen und gelten weitgehend ab September 2009:

- **Marketing / Werbung**

- **Weitergabe von Adressdaten nur nach Einwilligung**

Personenbezogene Daten wie Adressen dürfen künftig nur weitergegeben werden, wenn der Kunde darin einwilligt. Die entsprechende Textpassage, z. B. in den vertraglichen Vereinbarungen, ist dabei **optisch hervorzuheben**.

- **Listenprivileg/ Herkunftsangabe für Adressdaten**

Listenmäßig erfasste Daten wie Name, Beruf, Adresse, Geburtsjahr oder Titel dürfen auch ohne Einwilligung weitergegeben werden, wenn die Betroffenen über die Herkunft der Angaben informiert werden. Den Betroffenen soll damit ermöglicht werden, einer Weitergabe und Nutzung ihrer Daten wirksam zu widersprechen.

- **Das Verschicken von Eigenwerbung an eigene Kunden bleibt von der Novelle unberührt.**

>> Konkrete Anforderungen an Unternehmen (Werbung/Marketing):

Der Datenbestand muss geprüft und den möglichen Nutzungen zugeordnet werden. Die Quelle/ Herkunft der Daten muss zusätzlich gespeichert werden, vorhandene Einwilligungen sind entsprechend zu dokumentieren. Bei übernommenen Adressdaten ist deren Herkunft im Werbebrief anzugeben. Die Weitergabe von Adressdaten muss mindestens zwei Jahre lang dokumentiert werden. Für Zwecke der Werbung gelten Übergangsregelungen bis 2012.

- **Auftragsdatenverarbeitung (Outsourcing, IT-Dienstleistungen)**

In § 11 BDSG ist die Datenverarbeitung im Auftrag detailliert geregelt. Der **Auftrag muss schriftlich erfolgen** und im Einzelnen sind **zehn Punkte festzulegen**, u. a. die technischen und organisatorischen Maßnahmen des Auftragnehmers, Kontrollrechte des Auftraggebers, vom Auftragnehmer mitzuteilende Verstöße, Begründung von Unterauftragsverhältnissen oder Rückgabe überlassener Datenträger und Löschung der gespeicherten Daten nach Beendigung des Auftrags.

Die Verantwortung des Auftraggebers wird durch die neuen Regelungen verschärft. Er muß den Auftragnehmer **regelmäßig kontrollieren und die Ergebnisse dokumentieren**.

>> Konkrete Anforderungen an Unternehmen (Einsatz Dienstleister):

1. Die Beauftragung von Dienstleistern hat grundsätzlich schriftlich mit den entsprechenden Datenschutzfestlegungen lt. § 11 BDSG zu erfolgen (z.B. Datenschutzstandardvertrag).

2. Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Massnahmen auszuwählen. (z.B. Vorlage Sicherheitskonzeption durch den Dienstleister).

3. Der Auftraggeber muss den Auftragnehmer regelmässig kontrollieren und die Ergebnisse dokumentieren (z.B. Vorlage eines Datenschutz-Prüfungsberichts durch Dienstleister).

4. Datenschutzrelevante Auftragsdatenverarbeitungen (Beispiele):

Lohnabrechnung, Archivierung, Aktenvernichtung, Kundenservice, Direktmarketing

oder spezielle IT-Dienstleistungen, z.B. Outsourcing RZ, Installation und Wartung von Netzwerken oder Hardware, Pflege von Software (Betriebssystem, Anwendungen) oder Durchführung von Migrationen im Produktivsystem, wenn bei diesen Dienstleistungen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Datenschutzrelevante Auftragsdatenverarbeitungen sind auch die entsprechenden Dienstleistungen (siehe oben) innerhalb eines Unternehmensverbundes durch ein anderes Verbundunternehmen.

• **Anforderungen an die Sicherheit der personenbezogenen Daten**

1. Der **Grundsatz der Datensparsamkeit und Datenvermeidung** wird erweitert. Wenn möglich müssen personenbezogene Daten anonymisiert und pseudonymisiert werden, um Rückschlüsse auf Personen zu verhindern. **Nur wirklich notwendige Daten dürfen gespeichert sein.** Wenn die Zusammenfassung mit vielen anderen Daten oder die Unkenntlichmachung des Namens möglich ist, ist dies durchzuführen.

2. Die **Nutzung von Verschlüsselungstechniken nach Stand der Technik ist künftig eine gesetzliche Standard-Sicherheitsanforderung (BDSG Anlage zu § 9).**

>> Konkrete Anforderungen an Unternehmen (Datensicherheit):

1. Das Unternehmen hat die Pflicht, ihren Datenbestand auf die folgenden Kriterien hin zu überprüfen und ggf. umzusetzen:

Fragestellungen: sind alle Daten tatsächlich notwendig ? Ist die Nutzung der Daten auch anonym oder unter Pseudonym möglich ? Ist eine Zusammenführung von Daten möglich und sinnvoll? Dies gilt nur für Bestände mit personenbezogenen Daten und soweit dies nach dem Verwendungszweck möglich ist.

2. Die Einsatzmöglichkeiten von Verschlüsselungstechniken sind für die folgenden Einsatzgebiete abzu prüfen und ggf. umzusetzen:

Zugangskontrolle (Autorisierung, Authentifizierung), Zugriffskontrolle (Datei-, Datenträger) und Datenweitergabe (Transport, Übertragung, E-Mail).

3. Erforderlich sind Massnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.

• **Arbeitnehmerdatenschutz**

Im neu aufgenommenen § 32 BDSG wird die "Datenerhebung, -verarbeitung und -nutzung für **Zwecke des Beschäftigungsverhältnisses**" geregelt. Die Verarbeitung und Nutzung ist erlaubt, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung eines Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Der Anwendungsbereich des BDSG auf nicht dateibezogene Informationen, z. B. Schriftstücke, Dokumentationen, Personalakten wurde erweitert.

Zur **Aufdeckung von Straftaten** können diese Daten nur erhoben, verarbeitet oder genutzt werden, wenn ein Verdacht vorliegt, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Hier ist aber immer der Grundsatz der Verhältnismäßigkeit zu beachten.

- **Informationspflicht bei Datensicherheitsverletzungen**

Erlangt ein Dritter unrechtmäßig Kenntnis von sensiblen Daten, z.B. durch Datendiebstahl oder durch Verlust eines Laptops, und besteht dadurch ein erhebliches Missbrauchsrisiko, so sind die Betroffenen, die Aufsichtsbehörde und ggf. die Öffentlichkeit zu informieren.

- **Bußgelder bei Verstößen**

Die möglichen Bußgelder für Verstöße gegen Datenschutzbestimmungen wurden deutlich angehoben **bis 300.000 €**. Aufsichtsbehörden können künftig bei Verstößen gegen Datenschutzregelungen auch anordnen, dass der entsprechende Verstoß eingestellt wird.

- **Übersicht weiterer Regelungen**

- **Datenschutzaudit verschoben**

Die ursprünglich geplanten Regelungen zur Einführung eines Datenschutzaudits sind gestrichen worden. Hier soll nach dem Willen der Koalition zunächst ein dreijähriges Pilotprojekt für eine Branche erfolgen.

- **Kündigungsschutz für Datenschutzbeauftragte**

Weiterhin sieht das neue Datenschutzgesetz eine **Stärkung der Position des betrieblichen Datenschutzbeauftragten** vor, u. a. durch einen verbesserten Kündigungsschutz und Verpflichtung des Unternehmens zu Fortbildungsmassnahmen.

- **Automatisierte Einzelentscheidung (§ 6a BDSG)**

Konkretisierung des Anwendungsbereichs und erweiterte Transparenzpflichten

- **Zulässigkeit des Scorings (§ 28b BDSG)**

Anwendungsbereich (Kredit, Werbung, Bewerbung)
Zulässigkeitsvoraussetzungen und Auskunftspflichten

- **Datenübermittlung an Auskunftsteien (§ 28a BDSG)**

Zulässigkeitsvoraussetzungen, Übermittlung für Bankgeschäfte, Informationspflichten
Übermittlung an unternehmensübergreifende Warnsysteme

- **Gültigkeit / Übergangsfristen**

Die meisten Regelungen des neuen Gesetzes treten bereits zum **1. September 2009** in Kraft, die erweiterten Bußgeldbestimmungen gelten ab April 2010. Für Zwecke der Werbung gelten Übergangsregelungen bis 2012.

Georg Osner, Datenschutzbeauftragter

Für Rückfragen: E-Mail: Osner@datenschutz-osner.de