Datenschutzrechtliche Anforderungen im Unternehmen: Notwendiges Wissen für Entscheider und Verantwortliche

Forum 7-it

RA Rainer Friedl

München, 16. Januar 2010

Historie und Sinn und Zweck des Datenschutzes

Historie des Datenschutzes

- Erstes Datenschutzgesetz: Hessisches Datenschutzgesetztes vom 30.09.1970
- 1978: das erste BDSG in Kraft
- 1984: Volkszählungsurteil
- 1995: „EG-Datenschutzrichtlinie“
- Jetziges BDSG in der Fassung von 1.9.2009
- Datenschutzrecht bis heute nicht zeitgemäß, teils „chaotisch“ und unpraktikabel
  -> ABER GÜLTIGES GESETZ!

Zweck des Datenschutzes

- Schutz vor **Missbrauch** personenbezogener Daten.
- Wahrung der Grundrechte von Personen beim Umgang mit ihren Daten, insbesondere das **Recht der informationellen Selbstbestimmung**: Das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

Die gesetzlichen Regelungen

Gesetzliche Grundlagen

- Zentrales Gesetz ist das **Bundesdatenschutzgesetz (BDSG)**
- Daneben haben einige andere Gesetze, Verordnungen und internationale Verträge auch Regelungen zum Datenschutz, insbesondere:
  - Betriebsverfassungsgesetz (BetrVG)
  - Telekommunikationsgesetz (TKG)
  - Telemediengesetz (TMG)
  - Europäische Datenschutzrichtlinie (Richtlinie 951461EG) und Standardvertragsklauseln (EU-Kommission)
  - Jugendschutzgesetz (JuSchG)
  - Landesdatenschutzgesetze (LDSG)
  - Sozialgesetzbuch (SGB)
  - (Safe Harbor-Abkommen (USA))
- U.v.m.

Wichtige Begriffsbestimmungen im Datenschutz (1)

- **Personenbezogene Daten** sind Einzelangaben über **persönliche oder sachliche Verhältnisse** einer **bestimmten oder bestimmbaren** natürlichen Person (Betroffene) (siehe § 3, I BDSG). Also **alle Angaben**, die einer **identifizierbaren Person zugeordnet** werden können, wie z.B. Geburtsdatum, Familienstand, Staatsangehörigkeit, Konfession, Adresse, Telefonnummer, Beruf, Foto, Arbeitgeber, Gehalt, Einkommen, Vermögen, Besitz, Urlaubsplanung, Arbeitsverhalten, Arbeitsergebnisse, Zeugnisnoten, Beurteilungen, Krankheiten, Vorstrafen, Steuern, Versicherungen, etc.

- **Betroffener** kann jede natürliche Person sein, z.B. Kollegen, Kunden, Interessenten, Bewerber, Lieferanten oder deren Ansprechpartner, etc.

- Für eine **Bestimmbarkeit** reicht es aus, wenn unter Zuhilfenahme mehrerer Datenquellen, eine konkrete Person ermittelt werden kann, z.B. durch Zuhilfenahme einer Liste zur Auflösung von Pseudonymen.

Wichtige Begriffsbestimmungen im Datenschutz (2)

- **Die Datenverarbeitungsvorgänge (Verwendung von Daten)**

  Das BDSG unterscheidet drei verschiedene Vorgänge bei der Verwendung von Daten:

  - **Erheben**: ist das Beschaffen von Daten über den Betroffenen
  - **Verarbeiten**: ist das Speichern, Verändern, Übermitteln, Sperren oder Löschen von Daten
  - **Nutzen**: ist jede Verwendung von Daten, die nicht Erheben oder Verarbeiten ist

  Grundsätzlich kommt es dabei nicht darauf an, ob die Daten elektronisch/digital (z.B. Datenbanken, Dateien, IT-Systemen/-Applikationen, etc.) oder analog (Karteikarten, Akten, etc.) verarbeitet werden.

- **Die verantwortliche Stelle** ist die, die zur **Erfüllung ihres Geschäftszwecks** personenbezogene Daten verwenden muss und für die **Einhaltung des Datenschutzes** verantwortlich ist. Sie muss daher durch entsprechende **Maßnahmen** die **Einhaltung des Datenschutzes sicherstellen**, z.B. dass die benötigten Daten nur für den jeweiligen Zweck verwendet, rechtzeitig gelöscht /gesperrt oder Daten nicht unerlaubt an Dritte weitergegeben werden.

Die Systematik des Datenschutzrechts und das Prinzip der Datensparsamkeit

- Der Datenschutz ist als **Verbot** mit **Erlaubnisvorbehalt** konstruiert (§ 4 Abs. 1 BDSG)

- Die Verarbeitung personenbezogener Daten ist nur erlaubt, wenn und soweit sie durch Gesetz erlaubt ist, oder eine Einwilligung des Betroffenen vorliegt.
  - Eine gesetzliche Erlaubnis kann dabei auch indirekt gegeben sein, z.B. Verarbeitung und Weitergabe von Mitarbeiterdaten aus sozialrechtlichen und steuerrechtlichen Gründen
  - Wichtigster Erlaubnisvorbehalt für Unternehmen ist § 28 BDSG: Datenverarbeitung für eigene Geschäftszwecke.

- Prinzip der Datenvermeidung und Datensparsamkeit (§ 3a BDSG)

Das Verhältnis von Datenschutz und Datensicherheit

- **Datensicherheit** : Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität von Daten.
- Die Datensicherheit betrifft alle Daten, nicht nur personenbezogene Daten, sondern zum Beispiel auch technische Daten.
- Die Datensicherheit ist damit auch **Voraussetzung** für effektiven und gesetzeskonformen Datenschutz.
- Datenschutz stellt regelmäßig zusätzliche hohe Anforderungen an die Datensicherheit .

Der Verantwortliche und seine „Aufsicht“

- Verantwortlich ist immer die verarbeitende Stelle. Damit ist der gesetzliche Vertreter, also die Geschäftsführung/Vorstand die verantwortliche Person.
  - Ansprechpartner für den DSB
  - verantwortlich für die Umsetzung des Datenschutzes in „letzter Instanz“
  - Haftung gegenüber Dritten ist nicht delegierbar

- Datenschutzrechtliche Aufsichtsbehörden in Bayern
  - Nicht-öffentlicher Bereich
    Bayerisches Landesamt für Datenschutzaufsicht (Präsident Thomas Kranig)
  - öffentlicher Bereich
    Dr. Thomas Petri, Bayerischer Landesbeauftragte für den Datenschutz

Wer muss den Datenschutz beachten?

- Die datenschutzrechtlichen Regelungen sind prinzipiell von jedermann zu beachten, also auch von selbstständigen oder Kleinst-Firmen.

- Nur rein persönliche oder familiäre Tätigkeiten sind davon ausgeschlossen. Platzierte Werbung auf der Homepage schließt diese Ausnahme i.d.R. schon aus.

Das „Verfahren“ und technisch-Organisatorische Maßnahmen

- Nach dem BDSG sind alle Verfahren, die personenbezogene Daten automatisiert Verarbeiten **vor** ihrer Inbetriebnahme zu melden. Die Meldepflicht kann nach § 4d, Abs. 2, ff. entfallen: z.B. bestellter Datenschutzbeauftragter, für sehr kleine Unternehmen (< 10 Beschäftigte)

- Der DSB ist ggf. bereits bei der Planung zu involvieren, insbes. wenn eine Vorabkontrolle notwendig ist

- Folgende Angaben müssen gemacht werden (in der Regel wird man vom DSB ein Formblatt bekommen)
  - Name oder Firma der verantwortlichen Stelle,
  - Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen
  - Anschrift der verantwortlichen Stelle
  - **Zweckbestimmungen** der Datenerhebung, -verarbeitung oder -nutzung,
  - Eine Beschreibung der betroffenen **Personengruppen** und der diesbezüglichen Daten oder Datenkategorien
  - **Empfänger oder Kategorien** von Empfängern, denen die Daten mitgeteilt werden können,
  - **Regelfristen für die Löschung** der Daten
  - Eine geplante **Datenübermittlung** in Drittstaaten,
  - Eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

- Sind andere als die verantwortliche Stelle an dem Verfahren beteiligt, sind ggf. **zusätzlich** die Vorschriften zur Auftragsdatenverarbeitung zu beachten (§ 11 BDSG)

Der Datenschutzbeauftragte (DSB)

- Der Datenschutzbeauftragte wirkt auf die Einhaltung der datenschutzrechtlichen Bestimmungen hin.

- Die Funktion des Datenschutzbeauftragten kann von einem externen Dienstleister oder von einem Mitarbeiter ausgeübt werden. Die Vor- und Nachteile sind dabei abzuwägen.

- Nicht möglich ist die Ausübung durch Personen, die ggf. in einen Interessenkonflikt geraten können (Mitglieder der Geschäftsführung, Personalverantwortliche, IT verantwortliche, etc.).

Der Datenschutzbeauftragte (DSB): Notwendigkeit der Bestellung

- Alle nicht-öffentlichen stellen müssen ein Datenschutzbeauftragten bestellen, insbesondere wenn eine der folgenden Voraussetzungen erfüllt ist:
  - Mehr als neun Beschäftigte verarbeiten ständig personenbezogene Daten automatisiert
  - 20 oder mehr Beschäftigte verarbeiten personenbezogene Daten auf andere Art und Weise (praktisch unbedeutend)
  - Geschäftsmäßige automatisierte Verarbeitung zum Zwecke der Übermittlung oder Markt- oder Meinungsforschung
  - besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden
  - Verarbeitung personenbezogener Daten vorgenommen werden, die die Persönlichkeit des Betroffenen bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens

Der Datenschutzbeauftragte (DSB): Die wesentlichen Aufgaben

- Hinwirkung auf die Einhaltung und Verbesserung des Datenschutzes
- Erstellung eines Sicherheitskonzept
- Erstellen einer Datenschutzrichtlinie; ggf. Vorbereiten einer Betriebsvereinbarung
- Prüfung von Telemediendiensten
- Betriebsanweisungen prüfen, anpassen, erarbeiten
- Mitarbeiterverpflichtungen prüfen, anpassen, erstellen und dokumentieren
- Mitarbeitereinweisung durch mündliche und/oder schriftliche Schulungen
- Prüfung und/oder Führen des Verfahrensverzeichnisses
- Kontrollieren ggf. auch die Erstellung eines öffentlichen Verfahrensverzeichnisses
- Dokumentation des Berechtigungskonzeptes
- Prüfung und Kontrolle des Trennungsgebotes sowie der Datenvermeidung und Datensparsamkeit
- Übermittlung der personenbezogener Daten ins Ausland prüfen
- Erhebung, Verarbeitung oder Nutzung personenbezogenen Daten im Auftrag prüfen
- Dokumentation schriftlicher Einwilligungen
- Betroffenen-Auskunft
- Erstellung des Datenschutz-Handbuchs
- Durchführung interner Audits und Audits bei externen Dienstleistern

Der Datenschutzbeauftragte (DSB): Stellung und Bestellung des DSB

- Im Rahmen seiner Tätigkeit als DSB weisungsfrei.
- Nur dem Leiter der verantwortlichen Stelle unterstellt (also meist dem gesetzlichen Vertreter).
- Keine Weisungsbefugnisse im Unternehmen.
- DSB und Kenntnis aller Daten?
- Die Bestellung muss schriftlich erfolgen.

Qualifikation des Datenschutzbeauftragten

Das Gesetz schweigt weitgehend zu den Voraussetzung („Fachkunde und Zuverlässigkeit“). Empfehlungen:

- Ausbildung

  Hochschul- oder Fachhochschulabschluss (z.B. Rechtswissenschaft, Informatik, Wirtschaftswissenschaft)

  oder

  Kaufmännische, technische oder verwaltungsrechtliche Ausbildung und mehrjährige Berufspraxis auf datenschutz-relevantem Gebiet

- Nachgewiesene Zusatzqualifikation als DSB durch entsprechende Ausbildung (z.B. TÜV, Dekra, Hochschulen)

- Ständige datenschutzrechtliche Fortbildung

Qualifikation des Datenschutzbeauftragten: Die wichtigsten Merkmale (angelehnt an „Ulmer Urteil“)

- Rechtliche Kenntnisse und Fähigkeiten: Der Datenschutzbeauftragte muss die datenschutzrechtlichen Regelungen kennen und anwenden können. Bei schwierigen rechtlichen Fragen und Verträgen ist ggf. Rechtsrat einzuholen.
- Technische Kenntnisse: Der Datenschutzbeauftragte muss mit Begriffen der Informationsverarbeitung vertraut und technisch versiert sein. Bei komplexen Strukturen ist ggf. die Beratung durch Spezialisten erforderlich.
- Organisatorische Kenntnisse: Kenntnis des Ablaufs und der Prozesse im Unternehmen; Vorschlagen geeigneter Maßnahmen
- Didaktische und kommunikative Fähigkeiten: Vermittlung der datenschutzrechtlichen Anforderungen, Durchführung von Schulungen
- Organisatorische Fähigkeiten: Erarbeitung von Maßnahmen mit Einfluss auf Geschäftsprozesse
- Zuverlässigkeit und Fähigkeit zur Konfliktbewältigung

Die Auftragsdatenverarbeitung (ADV):

- Die ADV trifft immer zu, wenn personenbezogene Daten einer verantwortlichen Stelle durch eine andere Stelle im Auftrag verarbeitet werden.
- Der Auftrag muss immer schriftlich nach einer sorgfältigen Auswahl erfolgen und mindestens die Voraussetzungen des § 11 mit § 9 BDSG enthalten und erfüllen.
- Regelmäßige Kontrolle des Auftragnehmers.
- Die ADV ist Privileg!
- ADV nicht ohne Datenschutzbeauftragten oder anwaltliche Hilfe.

Sanktionen und Konsequenzen bei fehlender oder mangelhafter Implementierung des Datenschutzes

- Bußgeld bei Nichtbefolgung datenschutzrechtlicher Vorschriften, ggf. strafbar bei vorsätzlichen Verstößen (§§ 43 f BDSG)
  - Z.B. Nichtbestellung eines DSB (bis zu € 50.000)
  - Z.B. fahrlässig unbefugte Datenerhebung (bis zu € 300.000)
- Verbot des Verfahrens; Löschungsverpflichtung unrechtmäßig erworbener Daten
- Schadensersatzansprüche, insbes. § 7 f BDSG
- Persönliche Regresshaftung der gesetzlichen Vertreter ggü. dem Unternehmen
- Vermögensschaden-Haftpflicht übernimmt Schäden i.d.R. nicht, auch nicht die D&O-Versicherung
- Arbeitsrechtliche Konsequenzen bei mangelnder Verpflichtung der Beschäftigten
- Image- und Vertrauensverlust des Unternehmens

Stolpersteine im Datenschutz (1)

» Sie erhalten ein Schreiben mit folgendem Inhalt:

Sehr geehrte Damen und Herren,

Ich bitte Sie, mir schriftlich Auskunft zu folgenden Punkten zu geben:

- Welche personenbezogenen Daten über mich werden bei Ihnen gespeichert.
- Zu welchem Zweck werden diese Daten erhoben, verarbeitet und genutzt.
- Wie wurden die Daten erhoben , bzw. aus welcher Quelle haben Sie diese Daten erhalten.
- Mitteilung über alle weiteren Empfänger meiner Daten.

Ich erwarte Ihre Antwort bis zum ….

Stolpersteine im Datenschutz (2)

Im Datenschutz gibt es einige „Stolpersteine“, die von Unternehmen gerne übersehen werden.

- Ahndung von Datenschutzverstößen: nicht nur, wenn „etwas passiert“ ist.
- Keine Rückwirkende Heilung von Verstößen, wie z.B. Bestellung des DSB.
- Arbeiten mit Einverständniserklärungen (Jederzeit-Widerruf mit Folgen der Löschung/Sperrung).
- Nichteinhaltung von Kontrollpflichten => Datenschutzvorgaben nicht erfüllt.
- Weitergabe von Daten in Drittstaaten (außerhalb EU / EWR).
- Gefahr des „wilden Datensammelns“ (Dokumentationspflicht in Verfahrensverzeichnissen, Angabe in ADV, Gebot der Datensparsamkeit, fehlende Zweckbindung => keine Erlaubnis).
- Kein Konzernprivileg.
- Informationspflicht bei „Unfällen“ (§ 42a).

Die wichtigsten „ToDo‘s“ im Datenschutz

- Website: Datenschutzerklärung (§ 13 TMG), Impressum, falls Dienstleister ggf. Vorgaben der DLInfoV
- Erstellung einer individuellen IT-Richtlinie, insbesondere Regelung von privatem Gebrauch und Einsatz privater Geräte
- Verpflichtung auf das Datengeheimnis und ggf. Fernmeldegeheimnis (z.B. falls private Telefonate erlaubt sind)
- Sicherstellung der Bearbeitung von Auskunftsanfragen
- Bestellung eines DSB
- Öffentliches Verfahrensverzeichnis

Vielen Dank …

… für Ihre Aufmerksamkeit!

Noch Fragen?