München
im Januar 2016

IT-Sicherheit und Haftungsrisiken im Unternehmen

Natalie Wall
Fachanwältin für Informationstechnologierecht

Wall&Kollegen Rechtsanwälte

IT-Sicherheit und Haftungsrisiken im Unternehmen

Gliederung

- Zulässiger Umgang mit personenbezogenen Daten nach BDSG
- Rechte und Pflichten des Datenschutzbeauftragten
- Direktmarketing zur Datenbeschaffung - Einwilligungserfordernisse
- Datenschutz in verbundenen Unternehmen (kein Konzernprivileg!)
- Grenzüberschreitende Datenverarbeitung
- Anforderungen an technische und organisatorische Maßnahmen nach § 9 BDSG

IT-Sicherheit und Haftungsrisiken
im Unternehmen

Zulässiger Umgang mit personenbezogenen Daten nach BDSG

Personenbezogene Daten (Art. 2 a RL 95/46/EG, § 3 BDSG)

- Alle Informationen über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürliche Person.
- Eine Person ist bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Schutzumfang

- Geschützt sind Angaben zu Einzelpersonen:
  - Vor- und Familienname
  - Anschrift
  - Staatsangehörigkeit
  - Beruf

- Kein Schutz von jur. Personen (GmbH, AG, e. V., e. G.) und Personengesellschaften (OHG, KG)

Haftungsrisiken bei personenbezogenen Daten:

- Verschuldensunabhängige Haftung nach BDSG für öffentliche Stellen, Bußgeld bis 250.000,- EUR

- Im privatwirtschaftlichen Bereich:
  - Beseitigungs- und Unterlassungsansprüche
  - Schadensersatz und Schmerzensgeld
  - Bußgeld von 25.000,- EUR bis 250.000,- EUR

Zulässigkeit der Erhebung, Verarbeitung u. Nutzung personenbezogener Daten

- Grds. nur zulässig, wenn nach Gesetz erlaubt oder Einwilligung des Betroffenen vorliegt (Verbot mit Erlaubnisvorbehalt)
- Gesetzliche Erlaubnis liegt insb. vor, soweit Verarbeitung zur Durchführung oder Abwicklung des Vertrages notwendig (§ 28 BDSG)
- Schriftliche Erlaubnis des Betroffenen nach eingehender Information über Art u. Umfang der Speicherung; klauselmäßiges Einverständnis reicht nicht. Es bedarf einer freien Entscheidung des Betroffenen

Benachrichtigungspflicht § 19a BDSG

Datenerhebung ohne Kenntnis des Betroffenen:

- Betroffener ist über die erstmalige Speicherung, die Art der erhobenen Daten, den Zweck, die Verarbeitung und Nutzung und die Identität der verantwortlichen Stelle zu benachrichtigen
- Ausnahmen:
  - Betroffener hat schon Kenntnis erlangt
  - Speichern ist gesetzlich erlaubt
  - Daten sind für eigene Zwecke gespeichert und aus allgemein zugänglichen Quellen entnommen (z.B. Telefonbuch)

Auftragsdatenverarbeitung, 11 BDSG

- Nach § 11 BDSG zulässig
- Auftragnehmer übernimmt nur die Speicherung und ggf. die Strukturierung der Daten (verlängerter Arm)
- Auftraggeber behält Bestimmungsrecht darüber, welche Daten gespeichert oder verarbeitet werden. Er erteilt Auftragnehmer Weisungen hinsichtlich Verarbeitung und Nutzung von Daten
- Eine Weitergabe von Daten an außenstehende Dritte (sog. Funktionsübertragung) ist nur mit Einwilligung des Betroffenen erlaubt

Keine Generaleinwilligung zulässig

Unzulässig:

- „Ich bin damit einverstanden, dass meine oben stehenden Angaben sowie meine erhobenen personenbez. Umsatz-, Einlöse- und Teilnahmedaten durch die Fa. XY, die jeweiligen Partnerunternehmen u. die beauftragten Dienstleistungsunternehmen im Rahmen der geltenden Datenschutzgesetze zur Abwicklung des Programms sowie zu Werbe- und Marktforschungszwecken verarbeitet und genutzt werden.“

  LG München I, Urt. v. 01.02.2001 – 12 O 13009/00

Vermeidung von Haftung durch interne Datensicherung:

- Kein Zutritt für Unbefugte zu DV-Anlagen
- Keine Nutzung von DV-Systemen durch Unbefugte
- Zugriffskontrolle bei Berechtigten
- Weitergabekontrolle bei Übermittlung oder Speicherung auf Datenträger
- Eingabekontrolle
- Auftragskontrolle

IT-Sicherheit und Haftungsrisiken
im Unternehmen

Rechte und Pflichten des Datenschutzbeauftragten

Pflicht zur (schriftlichen!) Bestellung eines bDSB,

4f BDSG:

- Unabhängig von der Zahl der Beschäftigten, wenn personenbez. Daten geschäftsmäßig zum Zweck der (anonymisierten) Übermittlung erhoben, verarbeitet oder genutzt werden
- unabhängig von der Zahl der Beschäftigten, wenn automatisierte Datenverarbeitungsvorgänge vorgenommen werden (z. B. Scoringverfahren bei Kunden)
- ansonsten, wenn 10 AN mit automatisierter Datenerhebung, -verarbeitung, -nutzung beschäftigt sind, oder bei Verarbeitung auf andere Weise ab 20 AN

Aufgaben des Datenschutzbeauftragten

- Vorabkontrolle risikobehafteter Verarbeitung von personenbezogenen Daten (z. B. bei Erfassen von Profil, Rasse, Religion, Herkunft, Gesundheit, Gewerkschafts-zugehörigkeit)
- Anmeldung des meldepflichtigen Unternehmens in das vom Landeschutzbeauftragten geführte Register (Meldepflicht § 4d BDSG)
- Kontrolle der geplanten Datenverarbeitungssysteme und der ordnungsgemäßen Anwendung der Datenverarbeitungs-programme
- Kein bDSB binnen Monatsfrist ab Tätigkeitsaufnahme: Ahndung mit Bußgeld bis zu 25.000,- EUR

Fazit:

Der Datenschutzbeauftragte soll die Firmenleitung in Datenschutzfragen beraten und auf die Einhaltung der Datenschutzgesetze hinwirken

IT-Sicherheit und Haftungsrisiken
im Unternehmen

Direktmarketing zur Datenbeschaffung - Einwilligungserfordernisse

Direktmarketing zur Datenbeschaffung - Einwilligungserfordernisse

Anforderungen an die Einwilligung, § 28 Abs. 4 BDSG

- Ausdrückliche bewusste Erklärung
- Keine vorangekreuzten Erklärungen, die der Kunde erst wieder streichen muss (soll willentlich selbst ankreuzen)
- Unterrichtung über die jederzeitige Widerrufsmöglichkeit vor der Erklärung der Einwilligung des Kunden

Speichern von Kundendaten

- Zulässig: Speichern der Bestandsdaten: Kundenadressen, die zur Abwicklung des Bestellverhältnisses notwendig sind. Sobald es diese nicht mehr braucht, müssen die Daten gelöscht werden
- Zulässig: listenmäßige Verwendung zu "Marktforschungszwecken„, zB mit Mailings
- Unzulässig **Datatracking:** Nutzungsdaten des Kunden werden mit seiner Adresse zusammengeführt ohne ausdrückliche Erlaubnis des Kunden. Einwilligungsklausel erforderlich. Es reicht nicht, sich die Erlaubnis des Kunden im Rahmen von Allgemeinen Geschäftsbedingungen "zu holen"

Speichern von Kundendaten

Listenmäßige Verwendung zu "Marktforschungszwecken

Zulässige Angaben:

- Zugehörigkeit zu Personengruppen
- Berufs-etc.Bezeichnung
- Namen
- Titel
- Akademische Grade
- Anschrift
- Geburtsjahr

IT-Sicherheit und Haftungsrisiken
im Unternehmen

Grenzüberschreitende Datenverarbeitung

Grenzüberschreitende Datenverarbeitung

Übermittlung personenbezogener Daten

- innerhalb der EU und Vertragsstaaten des EWR-Abkommens (europ. Wirtschaftsraum): Erlaubnistatbestände nach BDSG (§ 4b BDSG)
- außerhalb EU und EWR:
  - beachte § 11 BDSG Auftragsverarbeitung NICHT zulässig, § 3 Abs. 8 BDSG – immer Dritter
  - nur zulässig bei **angemessenem Schutzniveau** beim Übermittlungsempfänger;
  - Maßstab: geltende Rechtsnormen oder speziell geltende Standesregeln oder Sicherheitsmaßnahmen

IT-Sicherheit und Haftungsrisiken
im Unternehmen

Datenschutz in verbundenen Unternehmen (kein Konzernprivileg!)

Zulässige Auftragsverarbeitung nach § 11 BDSG ?

Beispiel zentrale Personalverwaltung

- Funktionsübertragung kein § 11 BDSG
- Auslagerung des gesamten Aufgabenbereichs Personalverwaltung an eine konzerninterne zentrale Personalverwaltung = *Funktionsübertragung* (h.M.)
- Kein Ausnahmetatbestand des § 28 Abs. 1 Nr. 1 BDSG: (-) denn konzernweite Übermittlung dient nicht der Zweckbestimmung eines Vertragsverhältnisses (des ArbeitsV des AN mit dem einen Unternehmen). TIPP: ggf. (+) wenn AN zur Leistungserbringung in den anderen konzernangehörigen Unternehmen verpflichtet
- **=> kein Konzernprivileg**

Grenzüberschreitende Datenverarbeitung

Übermittlung personenbezogener Daten

- außerhalb EU und EWR zulässig:
  - anerkanntes Schutzniveau (EU-Konmmission): CH, Kanada, Argentinien, Guernsey, Isle of Man
  - konzernweite verbindliche Verhaltenskodizes: „Codes of Conduct“; in § 4c BDSG ausdrücklich vorgesehen - str., ob Genehmigung der zuständigen Aufsichtsbehörde erforderlich; TIPP: vorsorglich abklären
  - Safe Harbour Grundsätze des US-Handelsministeriums (akzeptiert von der EU-Kommission): Selbstverpflichtung von US-Unternehmen: Datenübermittlung zulässig

Grenzüberschreitende Datenverarbeitung

Beispiel Einwilligungserklärung

„Ich willige ein, dass meine personenbezogenen Daten, die ich (*zum Beispiel auf dem Antragsformular* ..) angegeben habe, für die Zwecke (*genaue Angabe des Übermittlungzwecks*) an die xy Inc. in Kalifornien, USA übermittelt werden. Es ist mir dabei bekannt, dass die xy Inc. dort einem Datenschutzrecht unterliegt, dass mir möglicherweise keinen dem Datenschutzrecht in der Europäischenunion vergleichbaren Schutz bietet.

Ich bin berechtigt, diese Einwilligungserklärung jederzeit mit Wirkung für die Zukunft zu widerrufen.“

IT-Sicherheit und Haftungsrisiken
im Unternehmen

Anforderungen an technische und organisatorische Maßnahmen nach § 9 BDSG

Anforderungen an technische und organisatorische Maßnahmen nach § 9 BDSG

Grundsatz § 9 S. 1 BDSG

> Öffentliche und nicht-öffentliche Stellen, die ... personenbezogene Daten erheben, verarbeiten oder nutzen, haben die **technischen und organisatorischen Maßnahmen** zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem **angemessenen Verhältnis zu dem angestrebten Schutzzweck** steht.

Konkrete Vorgaben der Anlage des § 9 BDSG

1. Zutrittskontrolle (Hochsicherheitstrakt, Key Card)
2. Zugangskontrolle (Passwörter)
3. Zugriffskontrolle (funktionsgebundener Zugriff)
4. Weitergabekontrolle (Verschlüsselungsverfahren)
5. Eingabekontrolle (Sicherheitssoftware)
6. Auftragskontrolle (Protokollierung von Anweisungen)
7. Verfügbarkeitskontrolle (Brandschutz)
8. Datentrennungskontrolle (Datenseparierung)

Konkrete Vorgaben der Anlage des § 9 BDSG

1. Zutrittskontrolle

Ziel, Unbefugten den körperlichen Zugang zu Datenverarbeitungsanlagen zu verwehren

- Sicherstellung durch Kontrolle des Zugangs und Absicherung der Zugangswege
- Maßnahmen (nicht abschließend):

  - Zutrittsberechtigung der Benutzer für die Räumlichkeiten
  - automatische Abmeldungen des Terminals nach längerer Untätigkeit
  - Berechtigungsausweise/Besucherausweise
  - Einrichtung von Sicherheitsbereichen
  - Bewachungsanlagen/-personal

Konkrete Vorgaben der Anlage des § 9 BDSG

2. Zugangskontrolle

Ziel, die Benutzung von Datenverarbeitungssystemen durch Unbefugte zu verhindern

- Sicherstellung durch Festlegung von Benutzerrechten
- Maßnahmen (nicht abschließend):
  - sicheres Passwortverfahren und Benutzerkennung
  - Verschlüsselung
  - Protokollierung unerlaubter Aktivitäten der Benutzer
  - Verzicht auf Zugriff über Wählleitung

Konkrete Vorgaben der Anlage des § 9 BDSG

3. Zugriffskontrolle

Ziel, den Zugriff der Benutzer eines Datenverarbeitungssystems ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zu beschränken

- Sicherstellung durch Beschränkung des Zugriffs auf Daten, die zur konkreten Aufgabenerfüllung erforderlich sind
- Maßnahmen (nicht abschließend):

  - sicheres Passwortverfahren und Benutzerkennung

  - Zuordnung der Benutzer zu bestimmten Terminals, Festlegung der Befugnisse

  - Protokollierung unerlaubter Aktivitäten der Benutzer

  - zeitliche Begrenzung der Zugriffsmöglichkeit

Konkrete Vorgaben der Anlage des § 9 BDSG

4. Weitergabekontrolle

Ziel, die unbefugte Bearbeitung (Lesen Kopieren, Löschen) von Daten zu verhindern

- Sicherstellung sicherer Übertragung von personenbezogenen Daten und sicherem Transport von Datenträgern
- Maßnahmen (nicht abschließend):

  - Kontrolle der Datenübertragungsprogramme, Protokollierung von Datenübertragungen

  - Verschlüsselung der Daten und verschlüsselter Transportweg (Virtual Private Network-VPN)

  - schriftliche Regelungen über Umgang mit Datenträgern

  - Protokollierung des Verbleibs von Datenträgern

  - Verbot der Verwendung privater Datenträger

  - Verbot der Mitnahme dienstlicher Datenträger nach Hause

Konkrete Vorgaben der Anlage des § 9 BDSG

5. Eingabekontrolle

Ziel, nachträglich feststellen zu können, welche Daten zu welchem Zeitpunkt von wem eingegeben worden sind

- Sicherstellung durch maschinelle Aufzeichnungen und sonstige Unterlagen (keine ständige Protokollierung angemessen und somit erforderlich)
- Maßnahmen (nicht abschließend):

  - Programmgesteuerte Festlegung der Befugnisse zur Kenntnisnahme, Eingabe etc.
  - Passwortverfahren, Benutzerkennung
  - Protokollierung von Eingaben, Zugriffen und Zugriffsversuchen
  - Einsatz von Sicherheitssoftware
  - Vermerk der Eingabe in den Erfassungsunterlagen (z.B. durch Handzeichen)

Konkrete Vorgaben der Anlage des § 9 BDSG

6. Auftragskontrolle

Ziel, dass im Auftrag verarbeitete Daten nur entsprechend den jeweiligen Weisungen verarbeitet werden

- Sicherstellung durch entsprechende Kontrolle
- Maßnahmen (nicht abschließend):

  - Protokollierung der jeweiligen Anweisungen

  - Abgleich der jeweiligen Verarbeitung mit den darauf bezogenen Anweisungen

Konkrete Vorgaben der Anlage des § 9 BDSG

7. Verfügbarkeitskontrolle

Ziel, Schutz der Daten vor zufälliger Zerstörung (Wasserschäden, Brand)

- Sicherstellung durch entsprechende Sicherheitsvorkehrungen
- Maßnahmen (nicht abschließend):

  - Auslagerung von Sicherheitskopien

  - Erstellung von Katastrophenplänen

Konkrete Vorgaben der Anlage des § 9 BDSG

8. Trennungskontrolle

Ziel ist die technische Sicherstellung der zweckbestimmten Verarbeitung

- Sicherstellung durch Trennung (keine zwingende räumliche Trennung, logische Trennung genügt)
- Maßnahmen (nicht abschließend):

  - Softwaremäßige Mandanten-/Kundentrennung

  - Trennung über Zugriffsregelungen

IT-Sicherheit und Haftungsrisiken
im Unternehmen

Vielen Dank für Ihre Aufmerksamkeit!

Rechtsanwältin

Natalie Wall

Karlsplatz 7
80335 München

FON 089 30 90 589-0
FAX 089 30 90 589-11

MOB 0173-3582228

wall@wall-legal.de
www.wall-legal.de