

DATENSCHUTZ

Ungeliebtes Thema

**Besser spät als nie – die aktuellen Datenskandale zeigen:
Es ist höchste Zeit, den Datenschutz im Unternehmen ernst
zu nehmen.**

Ob der Diebstahl von 17 Millionen Datensätzen von T-Mobile oder der Verlust von Kreditkundendaten der Landesbank Berlin – aktuell erschüttern Datenschutzskandale die Republik. Doch nicht nur diese Fälle sind Grund genug, um den Datenschutz ernst zu nehmen und eine gesetzeskonforme Datenschutzorganisation im Unternehmen zu etablieren.

Rechtliche Grundlagen

Gemäß Bundesdatenschutzgesetz (BDSG) § 1 haben Unternehmen den Einzelnen davor zu schützen, dass er mit dem Umgang der personenbezogenen Daten in seinem Persönlichkeitsrecht nicht beeinträchtigt wird. Unternehmen mit mindestens zehn Mitarbeitern sind gesetzlich verpflichtet, einen Datenschutzbeauftragten zu bestellen, und Unternehmen, die mit besonderen Daten umgehen, müssen unabhängig von der Mitarbeiterzahl einen Datenschutzbeauftragten haben. Diese Bestellung hat maximal vier Wochen nach der Geschäftsaufnahme schriftlich zu erfolgen.

Wichtig ist, dass der Datenschutzbeauftragte über die entsprechende Fachkunde verfügen muss. Der Beauftragte ist der Geschäftsführung unmittelbar unterstellt. Alternativ ist die Bestellung eines externen Datenschutzbeauftragten möglich,

was für viele mittelständische Unternehmen eine bedeutende Erleichterung ist. Das Unternehmen muss technisch/organisatorische Schutzmaßnahmen zur Sicherstellung des Datenschutzes umsetzen. Bei Nichtbeachtung stehen Verantwortliche wie Geschäftsführer, IT-Leiter und Administratoren in der persönlichen Haftung. Die Geschäftsleitung haftet in vollem Umfang bei Schadensersatzansprüchen.

Datenschutz und IT-Sicherheit

Der zentrale rechtliche Anknüpfungspunkt für IT-Sicherheit findet sich in § 9 BDSG: Er verpflichtet Unternehmer, die personenbezogene Daten verarbeiten, alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die datenschutzrechtlichen Anforderungen zu erfüllen. Im Einzelnen sind – je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien – Maßnahmen zu treffen, um die folgenden acht Anforderungen („acht Gebote“) zu erfüllen: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Zweckbindung/Trennungsgebot.

Verhaltensregeln

Kunden und Interessenten erwarten, dass ihre Daten geschützt werden und stets verfügbar sind. Die Missachtung von Datenschutz kann das Image des Unternehmens nachhaltig schädigen. Daher ist der sorgfältige Umgang mit anvertrauten Informationen die Pflicht eines Jeden. Das Verhalten am Arbeitsplatz entscheidet über die Wirksamkeit der Sicherheitsvorkehrungen. Klassifizierte Daten sind nach dem Prinzip „need to know“ zu behandeln: Informationen dürfen also nur an Personen weitergegeben werden, die diese Daten für ihre Arbeit auch wirklich benötigen. Um den Umgang mit Daten zu vereinfachen, sollten Daten in Klassen eingeteilt werden. Hier ein Beispiel:

- Öffentlich: Informationen für die Öffentlichkeit wie offizielle Medienmitteilungen oder der Internetauftritt.
- Intern: Geschäftsunterlagen und Daten,

die für den normalen Geschäftsablauf benötigt werden und allen Mitarbeitenden zugänglich sind.

- Vertraulich: Geschäftsunterlagen und Daten, die nur für einen beschränkten Personenkreis bestimmt sind. Kundendaten sind als vertraulich klassifiziert.
- Geheim: Geschäftsunterlagen und Daten, die nur einem engen Kreis namentlich bezeichneter Personen zugänglich sind.

Faustregel: Alle klassifizierten Daten der Stufen „intern“, „vertraulich“ und „geheim“ müssen so behandelt werden, dass Unberechtigte sie nicht einsehen können. Für den korrekten Umgang (Erstellen, Verarbeiten und Löschen) mit klassifizierten Daten trägt der Mitarbeiter die Verantwortung. Bei Weitergabe von Daten sollte überlegt werden, welche Klassifizierungsstufe vorliegt. Wenn zum Beispiel ein Verlust der Daten bzw. die unabsichtliche Weiterleitung an Unberechtigte einen Geld- oder Image-Schaden anrichten könnte, sollten die Daten immer gesichert bzw. verschlüsselt transportiert werden.

Informationsquellen für Datenschutz



www.bfdi.bund.de

(Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)

www.gdd.de

(Gesellschaft für Datenschutz und Datensicherung e.V. – GDD)

www.datenschutz-praxis.de

(WEKA MEDIA GmbH & Co. KG)

www.bitkom.de

(Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)

www.heise.de

(Heise Mediengruppe)

Diskutieren Sie mit
im **IHK-Blog** zum Thema
Datenschutz!
www.ihk-blog.de

Der Datenschutzbeauftragte kann die Fachkunde durch Seminare und Praxis erlangen. Schulungen und Zertifizierungen werden unter anderem durch die Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) und vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein angeboten.

Aufgaben des Datenschutzbeauftragten

Die Aufgaben eines Datenschutzbeauftragten lassen sich unterscheiden in eine Art Bestandsaufnahme zu Beginn seiner Tätigkeit und regelmäßigen Aufgaben. Bei Aufnahme der Arbeit stehen zunächst folgende Dinge an (Auswahl):

- Ermittlung des Datenschutzniveaus und Aufbau bzw. Ergänzung der Schutzorganisation
- Erstellung einer Datenschutzrichtlinie
- Aufbau eines externen und internen Verfahrensverzeichnis
- Verpflichtung aller Dienstleister
- Überprüfung des Internetauftritts, der

10 Tipps und vertrauensfördernde Maßnahmen

- Setzen Sie nur einen qualifizierten fachkundigen Datenschutzbeauftragten ein
- Schulen Sie Ihre Mitarbeiter
- Verpflichten Sie alle Mitarbeiter auf den Datenschutz und auf Verschwiegenheit
- Verpflichten Sie alle Dienstleister, die theoretischen und praktischen Zugriff auf Ihre personenbezogene Daten haben
- Dokumentieren Sie Ihre Schutzorganisation mit Standardtools (zum Beispiel BDSG-Basic)
- Führen Sie jährliche Prüfungen der IT-Berechtigungskonzepte durch
- Erstellen Sie ein internes und externes Verfahrensverzeichnis und pflegen Sie dieses regelmäßig
- Führen Sie eine jährliche Datenschutzsensibilisierung Ihrer Mitarbeiter(innen) durch
- Führen Sie grundsätzlich eine Vorabkontrolle bei der Einführung bzw. Änderung datenschutzrelevanter Geschäftsprozesse durch
- Regeln Sie die Nutzung von Schnittstellen (USB), Systemen (PDA, Notebook, PC) und der Dienste E-Mail und Internet.

Betriebsvereinbarungen und Anweisungen auf Datenschutzkonformität

- Erstellung einer DV-Rahmenvereinbarung und von IT-Richtlinien etwa für Arbeitsplatz-PC, Notebooks und andere mobile Computer, den Umgang mit Passwörtern sowie die Nutzung von E-Mail und Internet

Technisch-organisatorischer Datenschutz: (siehe die „acht Gebote“ links)

- Erstellung Verpflichtungs- und Schulungskonzept
- Belehrung, Schulung und Verpflichtung der Mitarbeiter
- Identifizierung aller Applikationen/Datenbanken mit personenbezogenen Daten
- Zu den regelmäßig wiederkehrenden Aufgaben zählen (Auswahl):
- Beratung bei der Einführung neuer Verfahren, falls hierbei personenbezogene Daten verarbeitet werden (Vorabkontrolle)
- Prüfung von Zulässigkeitsvoraussetzungen bei der Verarbeitung personenbezogener Daten
- Beratung bei der Umsetzung der erweiterten Transparenzpflichten des BDSG zum Beispiel bei der Erhebung in Erhebungsformularen und in der Werbung
- Information der Geschäftsführung über datenschutzrelevante Vorgänge
- Anpassung der Schutzkonzeption an neue Gegebenheiten (Dokumenten-Management, Intranet, neue Software)
- Security-Check Datenhaltung/Sicherheit der Applikationen mit personenbezogenen Daten

Verpflichtungen

Nach § 5 BDSG haben Unternehmen die Pflicht, ihre Mitarbeiter – soweit diese bei der Verarbeitung personenbezogener Daten beschäftigt sind – bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Aus Beweisgründen wird empfohlen, diese Erklärung schriftlich

abzufassen. Durch § 11 BDSG ist geregelt, dass Unternehmen, die im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen auf die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verpflichtet werden müssen.

Auch muss dafür gesorgt werden, dass IT-Dienstleister, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, bestimmte Voraussetzungen erfüllen. Auch externe Personen, die theoretisch Zugriff auf personenbezogene Daten direkt oder über das beauftragte Unternehmen zur Geheimhaltung und/oder auf das Datengeheimnis haben, müssen verpflichtet werden. Verpflichtungsdokumente stehen auf den Internetseiten des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Aufsichtsbehörde und Sanktionierung

Verstöße gegen datenschutzrechtliche Vorschriften können erhebliche Auswirkungen auf das Image und die Vertrauenswürdigkeit Ihres Unternehmens haben. Der Gesetzgeber hat bei bestimmten Vergehen, insbesondere bei Datenmissbrauch, Sanktionen vorgesehen. Bei Nichtbeachtung des BDSG stehen Verantwortliche in der persönlichen Haftung. Sie haften in vollem Umfang bei Schadensersatzansprüchen. Es drohen Schadenersatz, Geld- oder Freiheitsstrafe bis zu zwei Jahren, Bußgeld bis zu 250 000 Euro oder arbeitsrechtliche Maßnahmen wie Abmahnung oder Kündigung.

Die Aufsichtsbehörde kann ohne Grund eine Überprüfung durchführen. Eine vorhandene, dokumentierte Schutzorganisation ist dann von großem Vorteil.

Michael J. Schöpf, zertifizierter Datenschutzbeauftragter – GDDCert, www.s-con.de

DATENSCHUTZ

Aufgepasst!

Nachlässigkeit, teils aber auch rechtliche Unkenntnis, können zu Datenschutz-Problemen führen. Die Fülle komplexer Einzelprobleme ist groß. Hier einige Beispiele.

Der fehlerhafte Umgang mit personenbezogenen Daten wird gemäß dem Bundesdatenschutzgesetz und dem Telemediengesetz mit einem umfangreichen Bußgeld- und Strafvorschriftenkatalog geahndet (§§ 43, 44 BDSG, § 16 TMG). Die folgenden Beispiele stellen eine kleine Auswahl der zahlreichen tatsächlichen und rechtlichen Fragestellungen des Datenschutzes im Bereich der neuen Medien dar.

IP-Adressen

Stellt ein Computer eine Verbindung mit dem Internet her, wird ihm vom Internet-Provider eine sogenannte IP-Adresse zugewiesen. Eine IP-Adresse ist eine Zahlenkolonne (zum Beispiel 123.456.24.1), die es dem Internet-Provider erlaubt, ein bestimmtes Endgerät für die Dauer der Verbindung eindeutig zu identifizieren und an dieses Daten zu versenden. Besucht nun ein Nutzer einen Internetauftritt, so wird die IP-Adresse des Endgeräts auch der Internetpräsenz bekannt gegeben. Häufig wird die IP-Adresse dort in sogenannten Logfiles gespeichert. Diese können dann für statistische Zwecke ausgewertet werden.

Es stellt sich dabei die Frage, ob bereits die IP-Adresse ein personenbezogenes Datum ist, denn theoretisch könnte mit ihrer Hilfe ermittelt werden, welche Website ein bestimmter Nutzer aufgerufen hat. Bejahendenfalls wäre eine Speicherung und Auswertung nur in den strengen Grenzen des Datenschutzrechts möglich. Diese Frage ist in juristischer Literatur und Rechtsprechung sehr umstritten. Als personenbezogene Daten werden Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person verstanden (§ 3 I BDSG). Es kommt also darauf an, ob eine Person bereits mittels ihrer IP-Adresse identifizierbar ist. Eine Zuordnung der Person zu der IP-Adresse ist nur dem Internet-Provider und anderen Internet-Dienstleistern möglich, denen weitere Daten des Nutzers bekannt sind, zum Beispiel Online-Banking-Dienste. Für sie ist eine IP-Adresse zweifelsohne ein personenbezogenes Datum. Schwieriger wird es bei einer x-beliebigen

Website. Deren Betreiber ist nur die IP-Adresse bekannt. Er kann ohne Mithilfe des Internet-Providers die Person hinter der IP-Adresse nicht ausmachen und der Internet-Provider wiederum darf die Identität des Nutzers nicht preisgeben. Daher ist es gut vertretbar, dass für einen normalen Website-Betreiber die IP-Adresse ohne verfügbare weitere Daten keinen Personenbezug aufweist (so auch AG München 30.09.2008, Az. 133 C 5677/08). Anders sieht es dagegen das AG Berlin-Mitte (27.03.2007, Az. 5 C 314/06, bestätigt durch das LG Berlin 06.09.2007, Az. 23 S 3/07), das darauf abstellt, dass es rein technisch möglich ist, mit Hilfe weiterer Daten von Dritten, eine bestimmte Person zu identifizieren. Dass diese Möglichkeit nach geltendem Recht grundsätzlich verboten und in der Praxis auch eher fernliegend ist, störte das Gericht nicht. Daher urteilte das AG-Berlin Mitte, dass jede IP-Adresse ein personenbezogenes Datum ist.

Zwar sprechen die besseren Argumente dafür, IP-Adressen nur dann dem Datenschutzrecht zu unterwerfen, wenn eine tatsächliche Identifizierbarkeit des Nutzers möglich ist. Das beträfe nur den Internet-Provider oder Internetdienste, die durch Dateneingabe des Nutzers diesen identifizierbar machen. Da die Frage bisher noch nicht höchstinstanzlich geklärt ist, sollte einstweilen davon ausgegangen werden, dass IP-Adressen personenbezogene Daten darstellen und daher nur im Rahmen des Datenschutzrechts verwertet werden dürfen. Das bedeutet unter anderem, dass Logfiles von Internetpräsenzen keine IP-Adressen speichern sollten. Bei vielen Hosting-Providern kann man diese Funktion deaktivieren. Andernfalls sollte der Provider schriftlich aufgefordert werden, Logfiles nicht mehr oder nur noch anonymisiert zu speichern.

Auskunftsanspruch gegenüber speichernden Stellen

Wer personenbezogene Daten speichert, ist dem Betroffenen gegenüber zur Auskunft verpflichtet. Dabei kann nicht nur Auskunft über die Daten, die zur Person des Betroffenen gespeichert sind, verlangt

werden; es besteht regelmäßig auch ein Auskunftsanspruch, der sich auf die Herkunft der Daten und den Zweck der Speicherung bezieht. Wurden die Daten weitergegeben, hat der Betroffene sogar ein Recht auf Kenntnis der Daten-Empfänger.

Diese Rechte können nicht nur gegenüber Unternehmen, deren Geschäftszweck das Sammeln von Daten ist (zum Beispiel SCHUFA oder Adresshändler) geltend gemacht werden; auch kleine Betriebe, bei denen personenbezogene Daten eher nebenbei anfallen, sind verpflichtet, Auskunft zu erteilen. Dies gilt auch für Online-Dienstleister. Prinzipiell sind daher nebenberufliche Betreiber von kleinen Online-Shops und große Internet-Versandhäuser unterschiedslos betroffen. Die Auskunft ist grundsätzlich schriftlich und kostenfrei zu erteilen. Nur ausnahmsweise kann davon abgewichen werden.

Unternehmen verweigern oft die Auskunft aus Unkenntnis ihrer Verpflichtung wegen technischer Schwierigkeiten oder wegen unzumutbarer Zeitbelastung. Dies ist aber schlicht rechtswidrig. Es ist Sache der speichernden Stelle, die Voraussetzungen für eine umfassende Auskunftserteilung gegenüber dem Betroffenen zu schaffen. Ist ein Unternehmen dem nicht gewachsen, darf es keine Daten erheben.



Fallstricke der EDV-Wartung

Ein praxisrelevantes Sonderproblem des Datenschutzes betrifft vorrangig Ärzte, Anwälte, Amtsträger, Wirtschaftsprüfer sowie bestimmte Versicherungen und Abrechnungsstellen. Denn bei ihnen kann das Offenbaren eines fremden Geheimnisses mit einem Freiheitsentzug von bis zu einem Jahr bestraft werden (§ 203 StGB). Geheimnisse werden definiert als Tatsachen, die sich auf den Betroffenen beziehen, nur einem begrenzten Personenkreis bekannt sind und an denen ein sachlich begründetes Geheimhaltungsinteresse besteht. Schon das Bestehen eines Vertragsverhältnisses kann unter Umständen als Geheimnis angesehen werden und muss dann auch vertraulich behandelt werden. Was an sich eine Selbstverständlichkeit darstellt, kann im EDV-Bereich zu schwer lösbaren Konflikten führen. Der Bundesgerichtshof (BGH) hat entschieden, ein Offenbaren eines Geheimnisses könne bereits darin zu sehen sein, dass ein externer EDV-Dienstleister bei seinen Wartungsaufgaben Zugriff auf relevante Datensätze eingeräumt bekommt und dadurch ohne Weiteres eine Kenntnisnahme des Geheimnisses möglich ist (BGH NJW 1995, 2915, 2916). An dieser Beurteilung ändert sich selbst dann nichts, wenn der

Dienstleister seinerseits vertraglich zur Geheimhaltung verpflichtet wird. Das mag insofern verwundern, als dies bei fest angestellten Arbeitnehmern anders beurteilt wird, da dann zwischen Arbeitgeber und Arbeitnehmer eine Funktionseinheit vorliegt und daher EDV-Wartungen auch bei Zugriff auf geheimnisrelevante Daten möglich ist. Im Einzelnen sind im Bereich der EDV-Wartung durch externe Dienstleister aber noch viele Fragen ungeklärt. Um eine Kenntnisnahme Dritter auszuschließen und den Straftatbestand zu umgehen, ist es daher betroffenen Auftraggebern in jedem Fall anzuraten, die maßgeblichen Daten unkenntlich zu machen oder einen zuverlässigen Verschlüsselungsmechanismus einzusetzen.

Arbeitgeber auf Spurensuche

Ein seit wenigen Jahren zu beobachtendes Phänomen stellen Online-Plattformen wie studivz.de und facebook.com dar. Diese laden – meist jüngere – Nutzer dazu ein, sich mit ihrem Privatleben öffentlich zur Schau zu stellen. Neben Hobbies, Bildungsabschlüssen und dem Beziehungsstatus kann man hier auch eigene Freunde „verlinken“, private Fotos hochladen und öffentlich zur Diskussion freigeben. Längst haben Arbeitgeber diese Communities als ergiebige Informationsquelle über Bewerber entdeckt. Zwar hat beispielsweise studivz.de folgenden Passus in die AGB aufgenommen „Nicht gestattet ist (...) die Verwendung der Daten eines Nutzers zum Zwecke der Personaldatenerhebung durch Arbeitgeber (...)“ Wirklich zu Ende gedacht ist das aber nicht, da dies nichts an der rein faktischen Möglichkeit, sich im Web über Bewerber zu informieren, ändert. Dazu kommt: Der potenzielle Chef-in-spe ist zu diesem Zeitpunkt noch gar kein „Arbeitgeber“. Da Auslegungsschwierigkeiten in Allgemeinen Geschäftsbedingungen zu Lasten des Verwenders gehen, lässt es sich gut vertreten, dass sich Noch-nicht-Arbeitgeber sehr wohl über studivz.de informieren dürfen.

Auch außerhalb von Online-Communities lauern Gefahren für Bewerber, denn: Was einmal im Internet steht, ist meist sehr lange Zeit abrufbar. Tippt man in Suchmaschinen den Namen eines Bewerbers ein, wird offenbar, wo diese oder eine gleichnamige Person seine Spuren hinterlassen hat – beispielsweise in Vereinspräsenzen, Diskussionsforen oder Zeitungsartikeln. Diese „Detektivarbeit“ ist rechtlich unbedenklich, denn die Informationen sind ja öffentlich für Jedermann zugänglich. Die Frage, ob die Informationen von anderen Personen überhaupt ins Netz gestellt werden durften, ist davon unabhängig zu beurteilen. Für Betroffene dürfte es sehr

SEMINAR

Anforderungen beim Datenschutz

Personaldaten, Kundendaten, Internet-Einsatz – die Datenschutz-Anforderungen an Unternehmen bergen Stolperfallen. Im IHK-Seminar am 29. Mai wird der Aufbau der Datenschutzorganisation erläutert, auf die Aufgaben des Datenschutzbeauftragten eingegangen, praktische Tools zum Aufbau und der Kontrolle der Datenschutzorganisation gezeigt sowie dargestellt, wie mit polizeilichen Auskunftersuchen umzugehen ist. Daneben wird aufgezeigt, inwieweit IP-Adressen personenbezogene Daten sind und welche rechtlichen Konsequenzen daraus entstehen.

Die Teilnahme am Seminar „Datenschutz – Mindestanforderungen an die Datenschutzorganisation“ kostet 75 Euro zzgl. 19% USt. (brutto 89,25 Euro). Anmeldung: www.begin.de/seminar

WORKSHOP

Software-Wartung

Die richtige Formulierung von Software-Wartungsverträgen ist wichtig. Was Anbieter einer solchen Dienstleistung beachten müssen, erfahren die Teilnehmer in einem Workshop am 19. Februar in Hannover. Dabei soll unter anderem für jeden Teilnehmer ein Software-Wartungsvertrag aus Anbieter-Sicht erstellt werden. *hg*

Info: Der Workshop „Individuelle Software-Wartungsverträge – Die Anbieter-Perspektive“ findet am 19. Februar in der IHK Hannover statt. Kosten: 350 Euro zzgl. 19% USt. (brutto 416,50 Euro), Frühbucher (bis 5. Februar) 300 Euro zzgl. 19% USt. (brutto 357 Euro). Anmeldung: www.begin.de/seminar

schwer sein, die Informationen aus dem Web zu löschen, denn oft sind die Inhaber der Websites (trotz Impressumspflicht und Nutzung von Registrierungsdatenbanken wie denic) schwer ermittelbar oder nur bedingt kooperativ.

Rechtsanwalt Thomas Feil, Fachanwalt für IT-Recht, und Alexander Fiedler, Wissenschaftlicher Mitarbeiter am Institut für Rechtsinformatik der Universität Hannover