NETZWERK
GROSSBEERENSTRASSE e.V.

Sicherheit im Mittelstand 2012

Datenschutzrecht

RA Christian Leege, UNITAS Rechtsanwaltsgesellschaft mbH

Datenschutz ist ein in der zweiten Hälfte des 20. Jahrhunderts entstandener Begriff, der nicht einheitlich definiert und interpretiert wird. Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Der Datenschutz will den so genannten gläsernen Menschen verhindern.

Je nach Betrachtungsweise:

- Schutz vor missbräuchlicher Datenverarbeitung,
- Schutz der Privatsphäre
- Schutz des Rechts auf informationelle Selbstbestimmung

Die Bedeutung des Datenschutzes ist seit der Entwicklung der Digitaltechnik stetig gestiegen, weil Datenverarbeitung, Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse immer einfacher werden.

Technische Entwicklungen wie Internet, E-Mail, Mobiltelefonie, Videoüberwachung und elektronische Zahlungsmethoden schaffen neue Möglichkeiten zur Datenerfassung. Interesse an personenbezogenen Informationen haben sowohl staatliche Stellen als auch private Unternehmen:

- Sicherheitsbehörden möchten beispielsweise durch Rasterfahndung und Telekommunikationsüberwachung die Verbrechensbekämpfung verbessern,
- Finanzbehörden sind an Banktransaktionen interessiert, um Steuerdelikte aufzudecken.
- Unternehmen versprechen sich von Mitarbeiterüberwachung höhere Effizienz, Kundenprofile sollen beim Marketing einschließlich Preisdifferenzierung helfen und Auskunfteien die Zahlungsfähigkeit der Kunden sicherstellen (Verbraucherdatenschutz, Schufa, Creditreform).

Dieser Entwicklung steht eine gewisse Gleichgültigkeit großer Teile der Bevölkerung gegenüber, in deren Augen der Datenschutz keine oder nur geringe praktische Bedeutung hat.

Ursprung im Recht auf informationelle Selbstbestimmung:

- ist im bundesdeutschen Recht das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.
- nach der Rechtsprechung des Bundesverfassungsgerichts ein Datenschutz-Grundrecht, das im Grundgesetz für die Bundesrepublik Deutschland nicht ausdrücklich erwähnt wird. Vorschlag, ein Datenschutz-Grundrecht in das Grundgesetz einzufügen, fand bisher nicht die erforderliche Mehrheit. Personenbezogene Daten sind jedoch nach Art. 8 der EU-Grundrechtecharta geschützt.

Das informationelle Selbstbestimmungsrecht ist eine Ausprägung des allgemeinen Persönlichkeitsrechts und wurde vom Bundesverfassungsgericht im so genannten Volkszählungsurteil 1983 als Grundrecht anerkannt. Ausgangspunkt für das Bundesverfassungsgericht ist das Allgemeine Persönlichkeitsrecht, aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG.

„(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“

Danach kann der Betroffene grundsätzlich selbst darüber entscheiden, wem er welche persönlichen Informationen bekannt gibt.

Dagegen wurde in den meisten Landesverfassungen eine Datenschutzregelung aufgenommen, so in Berlin (Art. 33).

Landesverfassung Berlin

Artikel 33

„Das Recht des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, wird gewährleistet. Einschränkungen dieses Rechts bedürfen eines Gesetzes. Sie sind nur im überwiegenden Allgemeininteresse zulässig.“

Schutzbereich:

Das Recht auf informationelle Selbstbestimmung ist weit gefasst. Es wird nicht unterschieden, ob sensible Daten des Einzelnen betroffen sind. Das Bundesverfassungsgericht stellte fest, dass unter den Möglichkeiten der Informationstechnologie auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen könne und es insoweit keine belanglosen Daten gebe.

Einschränkungen des Grundrechts seien zwar möglich, bedürften aber einer gesetzlichen Grundlage. Dabei habe der Gesetzgeber abzuwägen zwischen dem Geheimhaltungsinteresse des Betroffenen und dem öffentlichen Informationsinteresse der verarbeitenden Stelle.

Einschränkungen sind nur zulässig im überwiegenden Allgemeininteresse. Sie bedürfen einer klaren gesetzlichen Grundlage.

Dabei Unterscheidung zwischen Maßnahmen, die ohne oder gegen den Willen des Betroffenen vorgenommen werden, und solchen, die freiwillig erfolgen.

Für erstere muss die gesetzliche Ermächtigung auch „bereichsspezifisch, präzise und amtshilfefest“ sein (Volkszählungsurteil, BVerfGE 65, 1 [46]).

Weiterhin wird unterschieden zwischen anonymisierten Daten, die keinen Rückschluss auf den Betroffenen zulassen (z. B. für statistische Erhebungen), und zwischen Daten, die personalisierbar sind. Bei anonymisierten Daten ist die Zweckbindung gelockert, für Daten, die personalisierbar sind, gilt eine strenge Zweckbindung.

Das informationelle Selbstbestimmungsrecht wurde Grundlage für die bestehenden Bundesdatenschutzgesetze und Landesdatenschutzgesetze und beeinflusste auch die Entwicklung der Richtlinie 95/46/EG (Datenschutzrichtlinie).

In letzter Zeit hat das Recht auf informationelle Selbstbestimmung in der verfassungsgerichtlichen Rechtsprechung eine große Rolle gespielt. So wurde die Rasterfahndung in Nordrhein-Westfalen für verfassungswidrig erklärt, sofern sie nur auf Grundlage einer „allgemeinen Bedrohungslage“ geschieht, (Beispiel Mandant Speichelprobe)

die § 100c und § 100d StPO (der sogenannte Große Lauschangriff) mussten um einen Straftatenkatalog und um explizite Löschungsvorschriften ergänzt werden (BVerfGE 109, 279).

Das Ausspähen privater Daten aus einem staatlichen Interesse heraus ist strengen Beschränkungen unterworfen. Es bedarf nach dem Legalitätsprinzip generell der gesetzlichen Regelung und nach den Grundsätzen der Gewaltenteilung der richterlichen Anordnung. Nach bestimmter Frist muss dem Ausgespähten zudem Kenntnis über den Vorgang gegeben werden.

Recht auf Nichtwissen gilt als „negative Variante des Rechts auf informationelle Selbstbestimmung“.

Aus der Rechtsprechung folgt, dass jede Verknüpfung personenbezogener Daten für Zwecke Dritter der Zustimmung bedarf. Dazu sind Vereinbarungen möglich, die zwischen den Beteiligten getroffen werden und damit die ausdrückliche Zustimmung der Beteiligten dokumentieren.
Keine Vereinbarung zu Lasten Dritter: Es kann nicht durch Vereinbarung zweier Parteien eine Gültigkeit für Dritte erreicht werden. Im Umkehrschluss kann ebenso eine Vereinbarung zwischen zwei Parteien nicht durch eine Vereinbarung mit Dritten aufgehoben oder unwirksam werden.

Verhältnis der Datenschutzgesetze

Auf Bundesebene regelt das Bundesdatenschutzgesetz (BDSG) den Datenschutz für die Bundesbehörden und den privaten Bereich (d. h. für alle Wirtschaftsunternehmen, Institutionen, Vereinen etc. gegenüber natürlichen Personen).

Daneben regeln die Datenschutzgesetze der Länder den Datenschutz in Landes- und Kommunalbehörden.

Datenschutzrechtliche Regelungen finden sich darüber hinaus in etlichen Spezialgesetzen, etwa dem Telekommunikationsgesetz und dem Telemediengesetz, die jeweils für ihren Anwendungsbereich speziellere Regelungen zum Datenschutz enthalten. Diese bereichsspezifischen Regelungen gehen dem Bundesdatenschutzgesetz jeweils vor, das BDSG gilt nur ergänzend.

Die öffentlichen Stellen des Bundes sowie die Unternehmen, die geschäftsmäßig Telekommunikations- oder Postdienstleistungen erbringen, unterliegen der Aufsicht durch den Bundesbeauftragten für den Datenschutz. Die Landesbehörden werden durch die Landesdatenschutzbeauftragten kontrolliert. Die privaten Unternehmen (bis auf Telekommunikation und Post) unterliegen der Aufsicht der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, die beim Landesdatenschutzbeauftragten oder bei den Landesbehörden (z. B. Innenministerium) angesiedelt sind.

Bundesdatenschutzgesetz

Das deutsche Bundesdatenschutzgesetz von 1977 (BDSG 1977) sah es als Aufgabe des Datenschutzes an „durch den Schutz personenbezogener Daten vor Missbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken“ (§ 1 Abs. 1 BDSG 1977).

Der Datenschutz bezieht sich danach auf die Erhebung, die Verarbeitung und die Nutzung personenbezogener Daten.

Definitionen:

- Erheben = Beschaffen, § 3 Abs. 3 BDSG.
- Verarbeiten = Speichern, Verändern, Übermitteln, Sperren, Löschen, § 3 Abs. 4 BDSG.
- Nutzen = Jedes Verwenden, soweit es sich nicht um Verarbeiten handelt, d.h. Verwenden ist der Oberbegriff für Verarbeiten und Nutzen, § 3 Abs. 5 BDSG.

1970 verabschiedete Hessen das weltweit erste Datenschutzgesetz, 1977 folgte das Bundesdatenschutzgesetz (BDSG), Landesdatenschutzgesetze waren 1981 für alle westlichen Bundesländer beschlossen.

Mit der Richtlinie 95/46/EG (Datenschutzrichtlinie) haben das Europäische Parlament und der Europäische Rat Mindeststandards für den Datenschutz der Mitgliedsstaaten festgeschrieben. Die Richtlinie gilt jedoch nicht für den Bereich der justiziellen und polizeilichen Zusammenarbeit.

Geregelt wird auch die Übermittlung von personenbezogenen Daten an Drittstaaten, die nicht Mitglied der EU sind, bzw. einem Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum angehören: Gemäß Artikel 25 ist die Übermittlung nur dann zulässig, wenn der Drittstaat ein „angemessenes Schutzniveau“ gewährleistet. Die Entscheidung, welche Länder dieses Schutzniveau gewährleisten, wird von der Kommission getroffen, die dabei von der so genannten Artikel-29-Datenschutzgruppe beraten wird. Aktuell (Stand 02/2011) wird gemäß Entscheidung der Kommission von folgenden Drittstaaten ein angemessenes Schutzniveau gewährleistet: Schweiz, Kanada, Argentinien, Guernsey, Isle of Man sowie bei der Anwendung der vom US-Handelsministerium vorgelegten Grundsätze des „Sicheren Hafens“ an die US-Zoll- und Grenzschutzbehörde (CBP).

Nicht sicher: Japan, Indien, Israel, und China.

Hauptprinzipien des Datenschutzes sind

- Datensparsamkeit und Datenvermeidung,
- Erforderlichkeit,
- Zweckbindung.

Sind (dennoch) Daten einmal angefallen, so sind technisch-organisatorische Maßnahmen zur Gewährleistung des Datenschutzes zu treffen (Datensicherheit). Hierzu gehört insbesondere die Beschränkung des Zugriffs auf die Daten durch die jeweils berechtigten Personen.

Aus den Prinzipien der Datensparsamkeit und der Erforderlichkeit folgt, dass Daten zu löschen (vgl. Datenvernichtung) sind, sobald sie nicht mehr benötigt werden. Nicht mehr erforderliche Daten, die wegen gesetzlicher Aufbewahrungs- und Dokumentationspflichten (insb. im Steuerrecht bis zu 10 Jahren) nicht gelöscht werden dürfen, sind zu sperren.

Zu den grundlegenden Datenschutzanforderungen gehören ferner die unabdingbaren Rechte der Betroffenen (insb. das Recht auf Auskunft über die zu der jeweiligen Person gespeicherten Daten) und eine unabhängige Datenschutzaufsicht.

Nutzt ein Unternehmen für den Betroffenen erkennbar persönliche Daten, hat der Betroffene generell einen Rechtsanspruch auf Auskunft über die Speicherung dieser Daten und den Verwendungszweck dieser Daten. (Facebook – 1400 Seiten) Geht die Speicherung über einfache Adressdaten hinaus, hat der Betroffene generell einen Rechtsanspruch auf Löschung der Speicherung dieser Daten, wenn er mit dem Unternehmen keine Vertragsbeziehungen hat.

Lästige Werbeaktionen -> Betroffener kann in jedem Einzelfall durch Formschreiben unter Angabe der Adresse Auskunft einholen. Erfolgt keine Auskunft durch das Unternehmen, per Abmahnung durch einen Rechtsanwalt oder Klage bei Gericht Auskunft und Löschung durchsetzen. Kosten trägt aber zunächst der Betroffene.

Auf der Internationalen Datenschutzkonferenz 2005 haben die Datenschutzbeauftragten in ihrer „Erklärung von Montreux“ darüber hinaus an die international anerkannten Datenschutzprinzipien erinnert. Diese sind:

- Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten
- Prinzip der Richtigkeit
- Prinzip der Zweckgebundenheit
- Prinzip der Verhältnismäßigkeit (vgl. Verhältnismäßigkeitsprinzip)
- Prinzip der Transparenz
- Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen
- Prinzip der Nicht-Diskriminierung
- Prinzip der Sicherheit
- Prinzip der Haftung
- Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen
- Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr

Kollisionen des Datenschutzrechts

Datenschutz kollidiert in verschiedenen Bereichen mit anderen Zielen. Dabei jeweils genaues Abwägen des Datenschutzes mit den anderen Zielen. Ein übertriebener Datenschutz oder Datenschutz am falschen Ort kann auch schädlich sein.

Datenschutz und Informationsfreiheit

Datenschutz steht grundsätzlich im Konflikt mit der Forderung nach Informationsfreiheit. Informationsfreiheit bedeutet, dass Informationen der öffentlichen Verwaltung (Verwaltungstransparenz) und Politik dem Bürger öffentlich gemacht werden (Öffentlichkeitsprinzip). Diese Informationen unterliegen jedoch auch dem Datenschutz und sollten daher vertraulich behandelt werden. Dieser Zielkonflikt wird traditionell sehr unterschiedlich gelöst.

In Schweden wird das Öffentlichkeitsprinzip weitaus höher bewertet als der Datenschutz. Selbst hochprivate Daten wie die Einkommensteuererklärung sind öffentlich.
In Deutschland bestand traditionell eine geringe Bereitschaft öffentlicher Verwaltungen zur Veröffentlichung von Informationen. Erst 2006 wurde diese Haltung durch das Informationsfreiheitsgesetz gelockert. Die Abwägung zwischen den Belangen von Informationsfreiheit und Datenschutz wurde in § 5 Informationsfreiheitsgesetz aber weitgehend zu Gunsten des Datenschutzes vorgenommen: –

§ 5 INFORMATIONSFREIHEITSGESETZ

„Zugang zu personenbezogenen Daten darf nur gewährt werden, soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat. Besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 des Bundesdatenschutzgesetzes dürfen nur übermittelt werden, wenn der Dritte ausdrücklich eingewilligt hat“

Auf Grundlage des Informationsfreiheitsgesetz wurden Informationsrechte seitdem in 9 Bundesländern in Landesgesetzen umgesetzt.

Das IFG gewährt jeder Person einen voraussetzungslosen Rechtsanspruch auf Zugang zu amtlichen Informationen von Bundesbehörden. Eine Begründung durch Interesse rechtlicher, wirtschaftlicher oder sonstiger Art ist nicht erforderlich.

„Amtliche Information“ ist jede amtlichen Zwecken dienende Aufzeichnung, unabhängig von der Art ihrer Speicherung, also beispielsweise Schriftstücke in herkömmlichen Akten, elektronisch gespeicherte Informationen, Zeichnungen, Grafiken, Pläne, Ton- und Videoaufzeichnungen.

Bedient sich eine Bundesbehörde zur Erfüllung ihrer Aufgaben einer juristischen oder natürlichen Person des Privatrechts, so ist sie auch dann auskunftspflichtig, wenn die begehrten Informationen bei der privatrechtlichen Person vorliegen (etwa Abschleppunternehmen).

<u>Beschränkungen und Ausnahmen</u>

Regelmäßig nicht erfasst vom Informationszugangsrecht werden Belange der inneren und äußeren Sicherheit, Ermittlungs- und Gerichtsverfahren, geistiges Eigentum, Betriebs- und Geschäftsgeheimnisse und personenbezogene Daten, bei

denen ganz allgemein der Grundsatz gilt, dass das Informationszugangsrecht nicht das Informationelle Selbstbestimmungsrecht bricht.

Die Informationsfreiheit bezieht sich ausschließlich auf abgeschlossene dokumentierte Vorgänge, öffnet also keinen Zugang zu laufenden Planungen (§ 3 Schutz von besonderen öffentlichen Belangen, § 4 Schutz des behördlichen Entscheidungsprozesses).

Bezüglich der Inhalte von Personalakten und Personalverwaltungssystemen besteht kein Informationszugangsanspruch. Informationen über Namen und dienstliche Anschriften von Beschäftigten sollen jedoch grundsätzlich zugänglich gemacht werden. Dasselbe gilt für Informationen zu Gutachtern und Sachverständigen.

Verfahren

Die Behörde gewährt den Informationszugang grundsätzlich nur auf Antrag, und zwar „unverzüglich“ durch Auskunftserteilung oder Gewährung von Akteneinsicht. Der Antrag hierfür kann mit einem formlosen Schreiben, aber auch mündlich oder telefonisch erfolgen. Die Behörde kann Gebühren und Auslagen in Höhe bis zu 500 € erheben. Die Ablehnung des Antrags ist ein Verwaltungsakt, der mit Widerspruch und Verpflichtungsklage angefochten werden kann.

Die Abkehr vom Amtsgeheimnis führt dazu, dass Informationsersuchen dritter Personen, die nicht an einem Verwaltungsverfahren beteiligt sind, künftig nicht einfach pauschal zurückgewiesen werden können. Stattdessen muss grundsätzlich Zugang zu den begehrten Informationen gewährt werden, es sei denn, im Einzelfall stehen schützenswerte und höherwertige Interessen Dritter dem Informationszugang entgegen. Die Behörde muss dies einzelfallbezogen prüfen und darlegen.

Verweigerung der Information, wenn schutzwürdige Belange des Betroffenen schwerer wiegen als das Informationsinteresse

In der Regel überwiegen schutzwürdige Belange nicht, wenn die Angaben lediglich Namen, Geburtsdatum, Beruf, Funktion, Anschrift und Telefonnummer enthalten und sich darauf beziehen, dass die Betroffenen:

– an einem Verwaltungs- oder sonstigen Verfahren beteiligt sind,
– vorgeschriebene Erklärungen, Anzeigen, Auskünfte etc. gegenüber einer Behörde abgegeben haben,

– von einer Behörde überwacht wurden,
– Eigentümer, Pächter, Mieter, Gutachter oder Sachverständige sind,
– als Amtsträger an Verwaltungsvorgängen mitwirken.

Die Stelle hat den Betroffenen Gelegenheit zu geben, sich dazu zu äußern, ob aus ihrer Sicht schutzwürdige Belange das Informationsinteresse des Antragstellers überwiegen. Erst danach darf die öffentliche Stelle abschließend über die Offenbarung der Daten entscheiden. Über den Inhalt der Entscheidung hat sie auch die Betroffenen zu informieren.

Kopien, auch von elektronischen Datenträgern, sind auf Verlangen des Antragstellers durch die öffentliche Stelle für ihn anzufertigen.

Ähnliche Konflikte wie bei behördlichen Auskunftsrecht, ergeben sich auch auf Unternehmensebene. Hier kollidiert ein eventueller Auskunftsanspruch von Kunden oder Dritten mit dem Datenschutz. So hatte etwa der Mobilfunkbetreiber T-Mobile den Wunsch eines Kunden, den Absender von Werbe-SMS zu erfahren, mit dem Hinweis auf Datenschutz abgewiesen – und wurde erst durch ein Urteil des Bundesgerichtshof (Az. I ZR 191/04) dazu gezwungen.

Weiterer wichtiger Konflikt: Datenschutz und Kriminalitätsbekämpfung. Ein weitgehender Zugriff der Strafverfolgungsbehörden auf personenbezogene Daten (auch von Unschuldigen/Unverdächtigen) erleichtert diesen die Arbeit. Ein Datenschutz ist hier jedoch besonders wichtig, da ein Überwachungsstaat mit dem Prinzip eines Rechtsstaates unvereinbar ist. Der Schutz der Grundrechte der Einwohner bedarf der gesetzlichen Regelung der Zugriffs- und Speichermöglichkeiten der Strafverfolgungsbehörden auf persönliche Daten. Der Umfang dieser Möglichkeiten und damit verbunden das Verhältnis zwischen Nutzen (Sicherheit) und Schaden (Eingriff in die Freiheits- und Bürgerrechte) ist politisch hoch umstritten. Während die einen auch bei kleineren Eingriffen das Bild eines Überwachungsstaates bemühen, lautet ein pauschales Schlagwort der Gegenseite „Datenschutz ist Täterschutz“.

Für die Abwägung der Interessen des Datenschutzes und der Kriminalitätsbekämpfung muss immer konkrete Maßnahme betrachtet werden. Ansatzpunkte für eine Bewertung sind:

- Schwere der Eingriffe in den Datenschutz
- Eignungsgrad der Maßnahme zur Verbesserung der Kriminalitätsbekämpfung

Die Themen, an denen sich die Diskussion um Datenschutzes und Kriminalitätsbekämpfung festmacht, wechselten im Laufe der Zeit. In den 1970ern wurde die Rasterfahndung, in den 1990er Jahren die Videoüberwachung intensiv diskutiert. Heute DNA-Reihenuntersuchungen, der Einführung von biometrischen Daten (Fingerabdruck, Gesichtsmaße, zukünftig eventuell Irisscan) und RFID-Chips in den Reisepass (Elektronischer Reisepass) fest.

Am 24. Februar 2012 entschied das Bundesverfassungsgericht, dass Polizei und Nachrichtendienste bei ihren Ermittlungen nicht auf Passwörter und PIN-Codes zugreifen dürfen.

Zur Zeit stehen auch die in Folge eines Abkommens zwischen der EU und den USA bei Flugreisen übermittelten Passenger Name Records in der Kritik, bei der vor Flugantritt personenbezogene Daten des Passagiers an die USA übermittelt und dort für mindestens 15 Jahre gespeichert werden. Ein ähnliches Abkommen wurde bereits 2006 vom EuGH gekippt, allerdings kurz darauf wenig verändert wieder auf den Weg gebracht. Im März 2012 stimmte das Europäische Parlament für das transatlantische Abkommen zum Transfer von Flugpassagierdaten. Gespeichert werden u.a. auch

- Kreditkarten- und Telefonnummern, IP-Adressen oder besondere Speisewünsche

Abrufe derzeit pro Tag: bis zu 82.000 Mal

Zur selben Zeit wurde bekannt, dass die EU zukünftig auch die Passagierdaten auf innereuropäischen Flügen sammeln und speichern will. Die Daten der Fluggäste sollen zwei Jahre lang komplett gespeichert werden. Danach werden sie für weitere drei Jahre "anonymisiert" aufbewahrt und nach insgesamt fünf Jahren vernichtet.

<u>Überwachung des Datenschutzes</u>

Obliegt den Datenschutzbeauftragten. Er überwacht und berät die öffentlichen Stellen des Bundes und des Landes in Fragen des Datenschutzes. Im Rahmen dieser Aufgabenerfüllung ist er unabhängig, weisungsfrei und nur dem Gesetz unterworfen.

Die Rechtsstellung und die Befugnisse sind im BDSG und in den jeweiligen Landesdatenschutzgesetzen geregelt.

Die Landesdatenschutzbeauftragten von Schleswig-Holstein, Nordrhein-Westfalen, Brandenburg, Berlin, Mecklenburg-Vorpommern, Bremen, Hamburg, Rheinland-Pfalz, des Saarlandes und Sachsen-Anhalt sind außer für den Datenschutz auch für die Informationsfreiheit und für das Akteneinsichtsrecht zuständig.

Außer in Bayern sind die Landesbeauftragten für den Datenschutz darüber hinaus auch für die Datenschutzaufsicht im nichtöffentlichen Bereich, d. h. bei Wirtschaftsunternehmen, Vereinen, Verbänden oder Parteien, zuständig. In Bayern besteht hierfür ein eigenständiges Landesamt für Datenschutzaufsicht mit Sitz in Ansbach. Im Zuge der Umsetzung eines Urteils des Europäischen Gerichtshofs vom 9. März 2010 unterliegen die Landesdatenschutzbeauftragten auch bei ihrer Aufsichtstätigkeit im nichtöffentlichen Bereich keiner Aufsicht durch andere staatliche Institutionen mehr. Die ursprünglich in vielen Ländern bestehende Rechtsaufsicht der jeweiligen Landesregierung gewährleistete nach Ansicht des Europäischen Gerichtshofs nicht die erforderliche Unabhängigkeit der Aufsichtsbehörden.

Berliner Beauftragte:

1. Hans-Joachim Kerkau (1. November 1979 bis 30. November 1989)
2. Hansjürgen Garstka (1. Dezember 1989 bis 1. Juni 2005)
3. Alexander Dix (seit 2. Juni 2005)

Dix erregte öffentliche Aufmerksamkeit mit der geäußerten Auffassung, die Kontrolle der von Schülern in die Schule mitgebrachten Handys nach Gewaltdarstellungen und Pornos durch Lehrkräfte widerspreche dem Fernmeldegeheimnis.

Berliner Datenschutzrecht

Das Berliner Datenschutzgesetz regelt die Voraussetzungen, unter denen Berliner Behörden personenbezogene Daten verarbeiten dürfen.

Nach dem BlnDSG ist die Verarbeitung der Daten von Bürgern in der Regel nur zulässig, wenn entweder

- eine besondere Rechtsvorschrift sie erlaubt oder
- wenn der betroffenen Bürger eingewilligt hat.

Für bestimmte Ausnahmefälle enthält das Berliner Datenschutzgesetz selbst Befugnisse zur Verarbeitung personenbezogener Daten, z.B.

- wenn wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung schutzwürdiger Belange der betroffenen Bürger nicht beeinträchtigt werden (§ 6 Absatz 1 Satz 2 BlnDSG)
- wenn zulässig für einen bestimmten Zweck erhobene Daten innerhalb derselben Behörde zu demselben Zweck weiterverarbeitet oder im erforderlichen Umfang an andere Behörden übermittelt werden (§ 11 Absatz 1 Satz 1; § 12 Absatz 1 Satz 2 BlnDSG)

Grundsatz der Erforderlichkeit

In jedem Fall ist eine Verarbeitung personenbezogener Daten durch Berliner Behörden nur zulässig, wenn und soweit diese Daten zur rechtmäßigen Erfüllung einer gesetzlichen Aufgabe im konkreten Einzelfall erforderlich sind (§ 9 Absatz 1 Satz 1 BlnDSG)

Auch wenn ein Gesetz die Verarbeitung einer Information über den Bürger erlaubt, muss sie dennoch unterbleiben , wenn die Verwaltung diese Information im konkreten Fall nicht benötigt wird (Verbot der Datenverarbeitung auf Vorrat). Rechte des Einzelnen

Nach dem Berliner Datenschutzgesetz hat jeder ein Recht auf

1. Auskunft und Benachrichtigung über die zu seiner Person gespeicherten Daten (§ 16 BlnDSG)
2. Berichtigung, Sperrung oder Löschung der zu seiner Person gespeicherten Daten (§ 17 BlnDSG)
3. Schadenersatz und Unterlassung (§ 18 BlnDSG)
4. Anrufung des Berliner Datenschutzbeauftragten (§ 27 BlnDSG)
5. Einsicht in das beim Berliner Datenschutzbeauftragten geführte Register (§ 25 BlnDSG)

<u>Auskunftsrecht</u>

Werden personenbezogene Daten in einer (manuellen oder automatisierten) Datei gespeichert, so hat der betroffene Bürger gegenüber der Behörde, die seine Daten verarbeitet, einen Anspruch auf gebührenfreie Auskunft über

1. die zu seiner Person gespeicherten Daten,

2. den Zweck und die Rechtsgrundlage der Verarbeitung und
3. die Herkunft der Daten und die Empfänger von Übermittlungen innerhalb der letzten zwei Jahre (§ 16 Absatz 1 BlnDSG)

Besonderes Datenschutzrecht

Zunehmend ist das Datenschutzrecht in Spezialgesetzen geregelt, die von den Behörden bei ihrer Tätigkeit in erster Linie zu berücksichtigen sind. Die allgemeinen Datenschutzgesetze treten dahinter zurück.

Derartige Spezialgesetze gelten in Berlin für eine Vielzahl von Behörden, z.B.:

- Meldebehörden
- Polizei – und Ordnungsbehörden
- Verfassungsschutz
- Gesundheitsämter
- Sozialleistungsträger
- Wohnungsämter
- Vermessungsämter
- Grundbuchämter
- Friedhofsverwaltungen
- Schulen
- Hochschulen
- Ärzte-, Zahnärzte-, Tierärzte- und Apothekerkammern
- Umweltämter
- Berliner Verkehrsbetriebe
- Berliner Stadtreinigung
- Berliner Wasserbetriebe
- Landesarchiv
- Opernhäuser, Theater, Orchester, Bibliotheken (soweit in öffentlicher Trägerschaft)

Fazit: Datenschutz derzeit durch Auskunfts- und Informationsrechte beeinträchtigt, zudem viele Spezialgesetze, die eigene meist weniger strenge Regeln vorsehen.

NETZWERK

GROSSBEERENSTRASSE e.V.

So sichern Sie Ihre Daten richtig

Datensicherheit & Co.

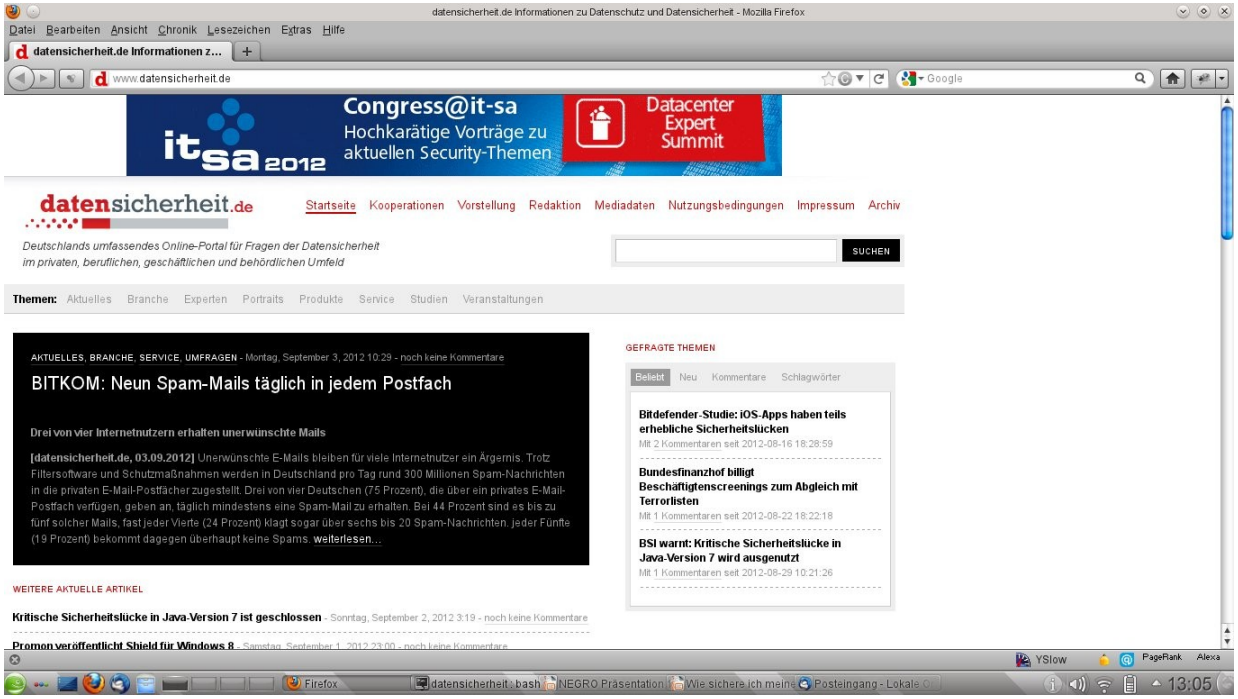
PRÄSENTATION

NG NETZWERK GROßBEERENSTRAßE

Vorstellung des Redners

Dipl.-Ing. Carsten J. Pinnow

- Studium der Elektrotechnik in Berlin
- beschäftigt mit dem Thema Datensicherheit seit 1991
- Herausgeber des Nachrichtenportals: www.datensicherheit.de



NG NETZWERK GROßBEERENSTRAßE

Sicherheit ist Chefsache

- Wie lange ist Ihr Unternehmen ohne Daten überlebens- bzw. arbeitsfähig
- Verschiedene Gesetze und Regelungen belegen die persönliche Haftung von Geschäftsführern bzw. Vorständen im Falle von Versäumnissen.

Fehleinschätzungen

- „Bei uns ist noch nie etwas passiert.“
- „Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht.“
- „Unser Netz ist sicher“
- „Unsere Mitarbeiter sind vertrauenswürdig“

Grundwerte der Datensicherheit

Gefordert sind

- Verfügbarkeit
- Vertraulichkeit
- Integrität

von

- Hardware
- Software
- Orgware

Datensicherheit

- **… ist kein Produkt**
  - Datensicherheit kann man nicht kaufen, man muß sie schaffen
  - Zum Erreichen kann man selbstverständlich auf geeignete Produkte zurückgreifen

- **… ist kein Projekt**
  - „Einmal ist keinmal...“
  - Datensicherheit muß ständig aufrecht erhalten werden

- **Datensicherheit ist somit ein Prozeß**

Mögliche Bedrohungsszenarien

- Verlust eines Tablet-PC
- Kein Backup
- Ausfall des Administrators
- Hackerangriff aus dem Internet
- Innentäter
- Befall durch Schadprogramme (Viren, Trojaner, Würmer...)
- Verlust von Speichermedien
- Arbeiten in der Cloud
- Mitarbeiter scheidet aus / wechselt die Abteilung

Häufige Versäumnisse (1)

- Sicherheit hat einen zu geringen Stellenwert
- Dauerhafte Prozesse zur Beibehaltung des Sicherheitsniveaus fehlen
- Sicherheitsvorgaben sind nicht dokumentiert
- Kontrollmechanismen und Aufklärung im Fall von Verstößen fehlen
- Die Rechtevergabe wird nicht restriktiv genug gehandhabt
- IT-Systeme sind schlecht konfiguriert
- Sensitive Systeme sind gegen offene Netze unzureichend abgeschottet
- Sicherheitsmaßnahmen werden aus Bequemlichkeit vernachlässigt
- Anwender und Administratoren sind mangelhaft geschult
- Verfügbare Sicherheits-Updates werden nicht eingespielt
- Mit Paßwörtern wird zu sorglos umgegangen

Häufige Versäumnisse (2)

- Vorhandene Sicherheitsmechanismen werden nicht genutzt
- Räume und IT-Systeme werden nur ungenügend gegen Diebstahl oder Elementarschäden geschützt
- Einbrecher und Diebe haben oft allzu leichtes Spiel (gekippte Fenster, unverschlossene Türen ...)

Sicherheitsanforderungen ändern sich

- Cloud-Computing
- mehr mobile Geräte (Stichwort: BYOD)
- intensivere Nutzung von elektronische Medien
- Kriminelle professionalisieren sich
- geänderte gesetzliche Rahmenbedingungen

NETZWERK GROSSBEERENSTRASSE e.V.

Sicherheit im Mittelstand

Datenschutz und Datensicherheit

Praktische Erfahrungen aus Unternehmen

Stefan Ebelt, EDV & Unternehmensberatung Ebelt

- Datenschutz fängt bei baulichen Maßnahmen an
  - separierte Gebäude oder Gebäudeteile (Serverraum)
  - Zugangsberechtigungen zum Serverraum und zu Konsolenräumen (Chipkarten, etc.)
  - Lagerung von Datenbackupgeräten und -medien in unterschiedlichen Räumen / Gebäuden
  - auch Brandschutzmaßnahmen und Gerätediebstahl gehören dazu
- Wie haben Sie Ihre IT-Landschaft organisiert ?
  - Server und Backup im eigenen Hause
  - Server bei einem Provider
    - Risiko: fremdes Personal
    - keine Verfügungsmacht über Geräte / Medien
    - kein Wissen, wo die Daten gespeichert sind (lokal, national, international -USA-)
    - Abhängig von Datenleitungen (es kann Störungen geben)
  - ‚schlimmer' noch: Datenspeicherung in der Cloud (verteilte Datenhaltung, Spionage)
- Welche Hardware ist zu betrachten
  - Welche Geräte speichern Daten: Server, PC, Notebook, Mobiltelefon, Smartphone
  - Aber auch: USB-Stick (Disketten sterben aus…)
  - BYOD (Bring Your Own Device) grundsätzlich zu vermeiden oder hoher interner Absicherungsaufwand – anderes ‚IT-Server-Datenkonzept'
- Datenschutz mit Software herstellen / bewahren
  - Die eingebauten Möglichkeiten des Betriebssystems nutzen
    - Der Bildschirmschoner kann ein Kennwort abfragen, wenn die Arbeit fortgeführt wird; Keine langen Wartezeiten für den Bildschirmschoner einstellen (max. 20 Min. ohne Aktivität)
    - Benutzer auf dem Arbeitsplatzrechner: 1 Admin, weitere Standardbenutzer (eingeschränkte Rechte)
    - Installation und Einstellungen sind NUR vom Administrator vorzunehmen
  - Nachrüsten / Ablösen mit den üblichen, aber notwendigen Tools
    - Virenscanner (nicht nur auf dem Server, sondern auch auf dem Arbeitsplatzrechner)
    - Firewall (auf jedem Rechner, der Zugang zur Außenwelt hat)
    - ZIP-Programme installieren (ZIP-Dateien sind nicht lesbar, können zusätzlich mit einem Passwort = Schlüssel codiert werden)
  - Verwenden Sie NUR lizenzierte Software (MS-Office, Tools, andere Anbieter; echte Freeware wie LibreOffice, etc.). Manche Dokumente sind nach Testablauf nicht mehr bearbeitbar
  - De-Installieren Sie nicht vorgesehene Software (die Mitarbeiter eingespielt haben / konnten) → Der Unternehmer haftet zuerst !! Weitergabe des Schadens an Mitarbeiter muss einwandfrei dokumentiert bewiesen werden.
- Zugriffsrechte für jeden Benutzer einrichten (bei Servern immer, sonst: Vertrauenssache)
  - Rechte auf Geräte, Verzeichnisse, Dokumente
  - Anmeldezeiträume festlegen (z.B. von 7:00 bis 22:00 Uhr)
  - Anmeldung und Zugriff nur mit Sicherheitskarte (Chipkarte)

- Verwenden Sie Passworte (JA: trotzdem !)
  - Passworte ermöglichen den Zugang zu Daten oder verschlüsseln Daten sogar
  - Bei der Anmeldung (am Rechner)
  - Bei bestimmten Programmen (z.B. Finanzsoftware)
  - Für Passworte sind alle Zeichen erlaubt !! Verwenden Sie auch die Sonderzeichen über den Zifferntasten oder ,;,.:--#'+*~<>|@€'
  - Wechseln Sie Passworte bitte wirklich mindestens 1x im Jahr
  - Verwenden Sie nicht bekannt Haustiernamen, Kosenamen der Frau / Mann, andere Vokabeln
  - In vielen Passwortsystemen MÜSSEN Sie eine Kombination mit Sonderzeichen eingeben
  - Es sollte nicht zu kurz gewählt werden (die Bank-PIN ist natürlich KEIN gutes Vorbild)
- Bei häufigerem Gebrauch oder zur Kommunikation mit Kunden oder Behörden brauchen Sie Signaturen (Diese gibt es als Datei oder auf einer Chipkarte); Signaturen kosten was.
  - Signieren Sie die Kommunikation in entsprechenden Programmen / Internetsites
  - Signieren Sie Ihre eMails
- Sie MÜSSEN eine betriebliche Datenschutzrichtlinie erstellen, die ALLE Ihre Mitarbeiter zu unterzeichnen haben
  - Sie müssen / sollten einen Datenschutzbeauftragten haben (oder einen Mitarbeiter, der bei kleineren Betrieben diese Aufgabe im Blick hat)
  - Das sichert das Unternehmen ab: bei Regressansprüchen an Sie verursacht durch Mitarbeiter
  - Das sichert den Mitarbeiter ab, der Unternehmer hat eine Kontroll- / Aufsichts- und Fürsorgepflicht und hat sonst bei Verstoß oder eingetretenem Schaden die Folgen zu tragen
  - Zu regeln ist, was verwendet werden darf und was ausdrücklich nicht verwendet werden darf (wenn es geht, namentlich nennen)
- Zu beachten ist, was für Daten ein Mitarbeiter oder Unternehmen ‚nach außen trägt'
  - verschiedenste Foren oder facebook, youTube, ähnliche ‚vergessen' immer noch schwer, was einmal gespeichert war
  - Geben Sie acht, welche Daten Sie eingeben / eingeben lassen (persönliche oder eher unternehmensinterne Daten (Alter der Mitarbeiter, Umsatzzahlen) haben dort nichts zu suchen)
  - Jeder (Unternehmer, interessierte Surfer) kann in sozialen Netzen nach Informationen suchen
- Machen Sie regelmäßige Updates (Server machen das auf Anordnung automatisch, kleine Netze ohne Server meistens nicht)
  - Sie müssen betriebliche Daten (Finanzamt) nicht nur lange Aufbewahren, sondern auch Zugriffsbereit halten (Hard- und Software) !!
- Daten müssen auch vernichtet werden
  - Wenn die Zeit abgelaufen ist, vernichten Sie Daten gründlich (ein Löschen reicht u.U. nicht aus -> Überschreiben)
  - Wenn Sie Festplatten ausmustern, kann eine Löschsoftware gute Dienste leisten; Man muss nicht schreddern ! Lassen Sie sich die Löschung durch Zertifikate bestätigen.
  - Papierakten: Die Dokumente sollten in kleinstem Partikelschnitt zerstört werden. Geheime Akten sollten anschließend in die Verbrennung gelangen.
  - Sichten Sie auch alte Aktenlager ! Hier liegen meist viele Informationen über das eigene Unternehmen (Finanzbuchhaltung, Bankbelege, etc.), Lieferanten, Kunden, Produkte und Personal offen in den Ordnern, die immer noch fremdes Interesse wecken können.