Datenschutz -

„Ein Blick zurück – ein Blick nach vorn“

Inhaltsverzeichnis

Was heißt eigentlich „Datenschutz“?

Der Begriff Datenschutz ist erst Ende der 60er Jahre entstanden. Datenschutz will - entgegen dem inzwischen eingebürgerten, aber durchaus missverständlichen Sprachgebrauch - nicht die Daten als solche schützen, sondern seit jeher die Persönlichkeit dessen, auf den sie sich beziehen. So gesehen gab es Datenschutz bereits weit vor der Erfindung des Computers bzw. vor Einsatz von EDV-Systemen und der Errichtung von Datenautobahnen. Denn auch in früheren Zeiten gab es zahlreiche Vorschriften, die die Erhebung und Verarbeitung personenbezogener Daten zum Gegenstand hatten.

Die frühen Formen des Datenschutzes

Schon im antiken Eid des Hippokrates ist die ärztliche Schweigepflicht angelegt, eine sehr frühe und dennoch bis heute bedeutsame Form des Datenschutzes! Viel später dann, aber immer noch weit vor Beginn des Informationszeitalters, garantierte Art. 117 der Weimarer Reichsverfassung das Brief- und Fernsprechgeheimnis, verbot also - nicht anders als heute Art. 10 des Grundgesetzes (GG) und Artikel 27 der Sächsischen Verfassung - das Eindringen in bestimmte fremde Kommunikationsbeziehungen.

Das Steuergeheimnis, wonach die Finanzämter ohne ausdrückliche gesetzliche Offenbarungsbefugnis nicht einmal die Staatsanwaltschaft informieren dürfen, findet sich bereits in § 10 der Abgabenordnung (AO) von 1919. Auch die Personalakte eines Beamten besaß bereits schon vor 1918 vertraulichen Charakter - damals allerdings auch gegenüber dem Betroffenen selbst, dem nicht einmal bei drohendem Disziplinarverfahren Einsicht gestattet wurde. Auch das Beicht- und das Bankgeheimnis wurden nicht in unserem Jahrhundert entwickelt. Die Strafprozessordnung (StPO) sah bereits 1879 vor, dass Informationen über den Beschuldigten nicht auf beliebige Weise gewonnen werden dürfen. Nach dem Zweiten Weltkrieg wurde dies in § 136 a StPO konkretisiert und insbesondere ausdrücklich verboten, Aussagen zu erpressen oder sie durch das Versprechen gesetzlich nicht vorgesehener Vorteile zu erschleichen.

Die frühen Formen des Datenschutzes bezogen sich freilich nur auf eng begrenzte Bereiche. Das Bedürfnis, der Verarbeitung personenbezogener Daten allgemeine Schranken aufzuerlegen, war erst die Folge technischer und damit verbundener sozialer Veränderungen.

Der Beginn der Datenschutzgesetzgebung

Die Geschichte der Datenschutzgesetzgebung beginnt mit dem 7. September 1970, dem Tag der Verkündung des 1. Hessischen Datenschutzgesetzes.

Am 1. Februar 1977 wurde das erste Bundesdatenschutzgesetz (BDSG) im Bundesgesetzblatt verkündet. Bundes- und Landesgesetzgeber reagierten mit der Entscheidung, verbindliche Regeln für den Umgang mit personenbezogenen Daten aufzustellen, auf die sich zunehmend entwickelnde Automatisierung der Datenverarbeitung. Seit Mitte der 60er Jahre bedienten sich vor allem Unternehmen in der Buchhaltung und beim Geschäftsverkehr mit Kunden der elektronischen Datenverarbeitung (EDV). Aus den Systemen der Lohn- und Gehaltsabrechnung entwickelten sich Personalinformationssysteme und zunehmend wurde die EDV für die Steuerung von Arbeitsvorgängen eingesetzt. Auch die öffentliche Verwaltung, die sich mehr und mehr zur Leistungsverwaltung entwickelte, setzte auf die neue Form der Informationsverwaltung. Renten- und Sozialhilfeansprüche lassen sich leichter berechnen, wenn die Daten in Sekundenschnelle verfügbar und auswertbar sind. Auch die staatliche Planung wird erleichtert, wenn sie sich auf einfachem Weg auf statistisch gewonnene Erkenntnisse stützen kann.

Die mit dem EDV-Einsatz verbunden Gefahren liegen auf der Hand: Fehlerhafte Angaben oder atypische Umstände können zu Irrtümern und Fehlentscheidungen führen, die aufgrund der automatisierten Verarbeitung ganz anders gewichtet und schwieriger durchschaut werden. Außerdem gewinnt derjenige, der auf gespeicherte Information zurückgreifen kann, einen gewissen Machtvorsprung. Datenschutzgesetze begegnen ausschließlich diesen nicht gewollten Konsequenzen und Risiken der automatisierten Datenverarbeitung und stellen nicht die Automatisierung als solche in Frage. Die gelegentlich geäußerten Vorurteile, Datenschutz sei technikfeindlich und würde Ängste schüren, sind daher unbegründet.

Das Volkszählungsurteil des Bundesverfassungsgerichts

Mit dem sog. "Volkszählungsurteil" des Bundesverfassungsgerichts (BVerfG) vom 15. Dezember 1983 erfährt die Entwicklung der Datenschutzgesetzgebung eine Zäsur. War der Datenschutz bislang durch die Aktivitäten der Landes- und des Bundesgesetzgebers geprägt, stand nun erstmals eine richterliche Entscheidung im Mittelpunkt des weiteren Geschehens. Auf die Verfassungsbeschwerde zahlreicher Bürger hin entschied das BVerfG, dass das im selben Jahr einstimmig vom Bundestag beschlossene Volkszählungsgesetz zum Teil verfassungswidrig sei. Hierdurch wurde den Bedenken einer breiten Bewegung von Volkszählungsgegnern Rechnung getragen, die vor allem auf Misstrauen gegenüber einer kaum durchschaubaren Informationstechnologie und Furcht gegenüber einer unkontrollierten Persönlichkeitserfassung basierten. Mit dem Volkszählungsurteil fand der Datenschutz erstmals verfassungsrechtliche Anerkennung. Das Gericht stellte nicht nur klar, dass das Recht auf informationelle Selbstbestimmung des Einzelnen ein Grundrecht ist, in das nur unter ganz bestimmten Voraussetzungen eingegriffen werden darf, sondern steckte den Rahmen für alle weiteren Überlegungen zum Umgang mit personenbezogenen Daten ab. Die wichtigsten Aussagen und Vorgaben des Volkszählungsurteils im Überblick:

Das Recht auf informationelle Selbstbestimmung:

Das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht umfasst auch die *"Befugnis des einzelnen,* ***grundsätzlich frei zu entscheiden****, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden"* (BVerfGE 65, 1, 42).

Grundlagen der Datenverarbeitung:

Die Anerkennung des Rechts des Einzelnen auf informationelle Selbstbestimmung hat zur Folge, dass jede Erhebung und Verwendung eines Datums einer ***besonderen Grundlage*** bedarf, die entweder im Willen des Einzelnen (Vertrag, Einwilligung) oder in gesetzlicher Anordnung liegen kann. Fehlt es an diesen Voraussetzungen, liegt ein rechtswidriger Grundrechtseingriff vor.

Schranken des Rechts auf informationelle Selbstbestimmung

Das BVerfG distanziert sich ausdrücklich von der Vorstellung eines Rechts im Sinne einer absoluten, uneinschränkbaren Herrschaft des Einzelnen über seine Daten. Er sei *"eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit"* und müsse daher Einschränkungen seines Rechts auf informationelle Selbstbestimmung *"im* ***überwiegenden Allgemeininteresse"*** hinnehmen (a.a.O. S. 44).

Als weitere Voraussetzung nennt das BVerfG eine klare ***Rechtsgrundlage***, *"aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen* ***Gebot der Normenklarheit*** *entspricht"* (a.a.O. S. 44). Der Gesetzgeber muss vor allem den ***Verwendungszweck*** präzise bestimmen, die Angaben müssen für diesen Zweck ***geeignet*** und ***erforderlich*** sein und dürfen das ***erforderliche Minimum*** nicht überschreiten. Eine Sammlung von Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken ist daher ausgeschlossen. Weiter sei der Grundsatz der ***Verhältnismäßigkeit*** zu beachten.

Schließlich wird darauf hingewiesen, dass der Gesetzgeber auch ***organisatorische und verfahrensrechtliche Vorkehrungen*** zu treffen hat, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. Insbesondere ist die öffentliche Verwaltung keine "Informationseinheit". Daher muss die Verwaltungsorganisation so beschaffen sein, dass eine Kenntnisnahme der Daten durch Personen, die sie für andere Zwecke verwenden könnten, ausgeschlossen ist. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungs-, Auskunfts- und Löschungspflichten und die Beteiligung unabhängiger Datenschutzbeauftragter zu nennen.

In der Volkszählungsentscheidung bestand kein Anlass zur Frage Stellung zu nehmen, inwieweit diese Grundsätze auch im ***Verhältnis zwischen Privaten*** Anwendung finden müssen. Aus der späteren Rechtsprechung - insbesondere der Fachgerichte - lassen sich jedoch einige Anhaltspunkte gewinnen: Das allgemeine Persönlichkeitsrecht des Einzelnen umfasst auch das Recht, Privaten gegenüber frei über die Preisgabe der ei-

genen Daten zu entscheiden. So hat etwa das Bundesarbeitsgericht (BAG) einem abgewiesenen Stellenbewerber das Recht eingeräumt, die Rückgabe oder die Vernichtung des von ihm ausgefüllten Personalfragebogens zu verlangen. Gleichzeitig ist aber zu beachten, dass der private Datenverarbeiter ebenfalls Grundrechtsträger ist, sich z.B. als Arbeitgeber auf die Berufsfreiheit des Art. 12 GG berufen kann. Dies führt nach der Rechtsprechung des BVerfG dazu, dass der Gesetzgeber bzw. der Richter verpflichtet ist, für einen angemessenen Ausgleich der widerstreitenden Interessen zu sorgen. Hierzu gehört insbesondere, Machtungleichgewichte zu korrigieren und ggf. Schutzvorschriften zugunsten der schwächeren Seite zu entwickeln. Neben den Begrenzungen, die sich aus kollidierenden Grundrechten ergeben, sind auch Eingriffe im überwiegenden Allgemeininteresse denkbar. Hierzu zählt z.B. die Verpflichtung des Arbeitgebers, Lohnsteuer und Beiträge zur Sozialversicherung abzuführen und dabei die nötigen Daten zu übermitteln.

Die Datenschutzrichtlinie der EG

Nach fünfjährigen intensiven Diskussionen ist am 24. Juli 1995 die EG-Richtlinie "zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (EG-DSRL) verabschiedet worden. Die Richtlinie konkretisiert und ergänzt die Grundsätze der Datenschutzkonvention des Europarates von 1981. Sie erweitert die Informationsrechte des Bürgers und verpflichtet die Mitgliedsstaaten zur Einrichtung staatlichen Kontrollstellen, die die Einhaltung der in Umsetzung der Richtlinie geschaffenen nationalen Vorschriften überwachen. Durch die Richtlinie wird ein einheitliches Datenschutzniveau für die Ausführung und Anwendung des Gemeinschaftsrechts durch die Mitgliederstaaten der EU geschaffen. Für den Austausch personenbezogener Daten mit Drittstaaten sieht die Richtlinie ebenfalls die grundsätzliche Geltung der gemeinschaftlichen Standards vor, ohne den Wirtschaftsverkehr unangemessen zu beeinträchtigen.

Die Richtlinie enthält detaillierte Vorgaben sowohl für öffentliche als auch für nichtöffentliche Stellen. Mit der Novellierung des Bundesdatenschutzgesetzes wurde die Europäische Datenschutzrichtlinie in deutsches Recht umgesetzt. Auch das Sächsische Datenschutzgesetz wurde novelliert, um es an die Richtlinie anzupassen. Ziel der Richtlinie, die Rechte der Bürger zu stärken, soll insbesondere durch Neuregelungen, wie

- die Einschränkung der Verarbeitung besonders sensibler Daten
- die Schaffung des Rechts, aus persönlichen Gründen auch gegen eine rechtsmäßige Datenverarbeitung zu widersprechen
- die Einführung einer Bestimmung über automatisierte Einzelentscheidungen
- die Ersetzung der Dateibeschreibung durch Verfahrensbeschreibung
- die Erweiterung des Schadensersatzanspruchs wegen unzulässiger oder unrichtiger Datenverarbeitung
- die Neuregelung der Übermittlung personenbezogener Daten ins Ausland u. a.

Darüber hinaus soll der Grundsatz der Datenvermeidung und Datensparsamkeit im Gesetz verankert werden.

Bundesdatenschutzgesetz (BDSG)

Um die Bestimmungen der europäischen Datenschutzrichtlinie 95/46 EG vom Oktober 1995 in nationales Recht umzusetzen, wurde das BDSG im Jahre 2001 geändert. Es ist am 23. Mai 2001 in Kraft getreten.

Neben zahlreichen Detailfragen gehört zu den Kernelementen des neuen Gesetzes die Regelung zur Datenübermittlung in Drittstaaten. Daneben enthält das novellierte BDSG eine Reihe neuer gesetzlicher Bestimmungen, mit denen u. a. technikspezifische Risiken der Datenerhebung und -verarbeitung durch Videoüberwachung (§ 6 b) und Chipkarten (§ 6 c) begrenzt werden sollen. Neu eingeführt wurde auch die Regelung zum Datenschutzaudit (§ 9 a). Nach dieser Regelung können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitenden Stellen zur Verbesserung des Datenschutzes und der Datensicherheit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Das neue BDSG enthält aber auch eine Vielzahl von Änderungen/Neuerungen gerade für den privatwirtschaftlichen Bereich.

Das BDSG gliedert sich in 6 Abschnitte, die im folgenden kurz vorgestellt werden sollen:

- **Erster Abschnitt: Allgemeine und gemeinsame Bestimmungen (§§ 1 - 11)**

Hier finden sich zahlreiche Begriffsbestimmungen und der Grundsatz, dass eine Datenerhebung, -verarbeitung und -nutzung nur zulässig ist, wenn das BDSG selbst bzw. eine andere Rechtsnorm sie erlaubt oder anordnet oder der Betroffene seine Einwilligung gegeben hat (§ 4 Abs. 1 BDSG).

In diesem Abschnitt ist der Grundsatz der Datenvermeidung und Datensparsamkeit verankert (§ 3 a). Es wird damit ausdrücklich das Ziel festgeschrieben, **so wenig personenbezogene Daten wie möglich** zu erheben, zu verarbeiten oder zu nutzen.

- **Zweiter Abschnitt: Datenverarbeitung der öffentlichen Stellen (§§ 12 - 26)**

Inhaltlich regelt dieser Abschnitt die Voraussetzungen für ein rechtmäßiges Verhalten der Bundesbehörden, geht dann zu den Individualrechten des Betroffenen über (Auskunft, Berichtigung, Sperrung und Löschung, Widerspruchsrecht und Recht auf Anrufung des Bundesdatenschutzbeauftragten) und regelt die Rechtsstellung des Bundesbeauftragten für den Datenschutz.

- **Dritter Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen (§§ 27 - 38 a)**

Dieser Abschnitt bestimmt, wann und unter welchen Voraussetzungen personenbezogene Daten von nichtöffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen verarbeitet werden dürfen. Mit nicht-öffentlichen Stellen sind insbesondere Privatunternehmen, wie Banken, Versicherungen, Versandhäuser, Auskunfteien etc. gemeint. Zu den öffentlich-rechtlichen Wettbewerbsunternehmen zählen z. B. Sparkassen, AG, GmbH mit eigener Rechtspersönlichkeit.

Der § 27 dieses Abschnittes findet Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden. Dies gilt nicht, wenn vorgenanntes ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt; wer also als Privatperson eine Datei von Adressen seiner Bekannten anlegt und diese ausschließlich privat nutzt, unterfällt nicht den Regelungen des BDSG.

Im nicht öffentlichen Bereich sind die Beauftragten für den Datenschutz intern im Unternehmen für die Einhaltung der Datenschutzregelungen zuständig. Die externen (anlassfreien) Kontrollen führen die regional zuständigen Aufsichtsbehörden durch. Sie überwachen die Ausführung dieses Gesetzes sowie andere Vorschriften über den Datenschutz. Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften fest, so ist sie befugt, den Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zu unterrichten. Gravierende Verstöße durch das Unternehmen sind u. a. solche, wenn trotz mehrmaliger Aufforderung von Seiten der Aufsichtsbehörde Auskünfte nicht erteilt werden oder wenn im Datenverarbeitungsprozess Auswertungen bzw. Listen mit personenbezogenen Daten ohne Erlaubnistatbestand erstellt worden sind.

- **Vierter Abschnitt: Sondervorschriften (§§ 39 - 42)**

Die Sondervorschriften regeln die Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder Amtsgeheimnisse unterliegen, die Verarbeitung durch Forschungseinrichtungen und die Medien.

- **Fünfter Abschnitt: Schlussvorschriften (§§ 43 - 44)**

Für bestimmte Gesetzesverstöße sehen die Schlussvorschriften strafrechtliche Sanktionen oder Bußgelder vor. Neu geregelt wurde auch, dass die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde die strafrechtliche Verfolgung von Datenschutzverstößen nunmehr selbst veranlassen können. Bisher war hierzu nur der Betroffene berechtigt (§ 44 Abs. 2 BDSG).

- **Sechster Abschnitt: Übergangsvorschriften (§§ 45 - 46)**

§ 45 des neuen BDSG beinhaltet eine Regelung hinsichtlich des Anpassungszeitraumes für solche Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die zum Zeitpunkt des In-Kraft-Tretens der Änderungen des BDSG bereits begonnen haben.

Die „Reform des Datenschutzrechts“ geht weiter

Nach derzeitiger Planung soll in einer zweiten Stufe der Novellierung eine **umfassende Neukonzeption** des BDSG vorbereitet werden, die das Gesetz modernisiert, vereinfacht und seine Lesbarkeit erhöht.

Das aktuelle Landesrecht im Freistaat Sachsen

Der Sächsische Landtag hat als verfassungsgebende Landesversammlung am 26. Mai 1992 die Sächsische Verfassung beschlossen und damit das Recht auf informationelle Selbstbestimmung ausdrücklich in den Katalog der Grundrechte aufgenommen: *"Jeder Mensch hat das Recht, über die Erhebung, Verwendung und Weitergabe seiner personenbezogenen Daten selbst zu bestimmen. Sie dürfen ohne freiwillige und ausdrückliche Zustimmung der berechtigten Person nicht erhoben, gespeichert, verwendet oder weitergegeben werden. In dieses Recht darf nur durch Gesetz oder auf Grund eines Gesetzes eingegriffen werden" (Artikel 33 der Sächsischen Verfassung - SächsVerf)*

Mit dem am 14. Dezember 1991 in Kraft getretenen Gesetzes zum Schutz der informationellen Selbstbestimmung (Sächsisches Datenschutzgesetz (SächsDSG)) hat der sächsische Landtag Sachsens erstes Datenschutzgesetz verabschiedet, das bereits einen hohen Standard des Datenschutzes garantierte. Im Jahre 2003 erfolgte eine umfangreiche Gesetzesnovellierung zur Umsetzung der Vorgaben der EG-Datenschutzrichtlinie von 1995.

Eine erneute Änderung erfolgte mit dem Gesetz zur Änderung des Sächsischen Datenschutzgesetzes vom 14. Dezember 2006. Im Rahmen der Novellierung wurde unter anderem die Zuständigkeit für die Kontrolle der Einhaltung des Datenschutzes bei den nicht-öffentlichen Stellen von den Regierungspräsidien auf den Sächsischen Daten-

schutzbeauftragten übertragen. Die neuen Regelungen sind am 01.01.2007 in Kraft getreten. Schließlich wurden durch das Zweite Gesetz zur Änderung des Sächsischen Datenschutzgesetzes vom 14. Juli 2011 die Vorgaben des Europäischen Gerichtshofes umgesetzt, womit der Sächsische Datenschutzbeauftragte nunmehr keiner Rechtsaufsicht mehr unterliegt, sondern als unabhängiges Kontrollorgan tätig ist.

Das Sächsische Datenschutzgesetz regelt verbindlich für die Behörden und alle sonstigen öffentlichen Stellen im Freistaat Sachsen die Voraussetzungen der Verarbeitung personenbezogener Daten. Es legt insbesondere fest, unter welchen Voraussetzungen eine Behörde welche Daten von welchen Personen zu welchen Zwecken erheben, speichern, verändern, übermitteln oder nutzen darf (§§ 12 bis 17 SächsDSG). Es regelt auch die Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung, Sperrung, Schadensersatz sowie auf Anrufung des Sächsischen Datenschutzbeauftragten (§§ 18 bis 24 SächsDSG).

Neben den allgemeinen Vorschriften des SächsDSG gibt es auch zahlreiche andere, spezielle gesetzliche Regelungen zum Datenschutz, wie z.B. im Sächsischen Meldegesetz, Sächsischen Polizeigesetz, Sächsischen Krankenhausgesetz.