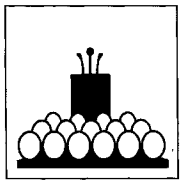
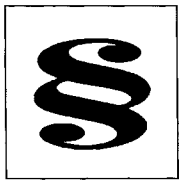




Empfehlungen des Ministerrats des Europarats zu Informatikanwendungen im Recht und Informationsrecht

7. Das Programm einer erneuerten Rechtsinformatik ist auch ein Programm für Lehre und Ausbildung.

Für die Juristenausbildung hat der Ministerrat des Europarats schon zum zweiten Mal eine Empfehlung verabschiedet, welche sowohl die Thematik der Informatikanwendungen im Recht wie auch die Thematik des Informationsrechts einbezieht. Auf diese Empfehlungen (1980 bzw. 1992) kann hier verwiesen werden, insbesondere auch hinsichtlich der Tendenz ihrer Fortentwicklung. Im Zeitalter der Informationsgesellschaft kann sich die Rechtsinformatik mit erneuertem Selbstvertrauen für die Einbeziehung ihrer Themen in die Lehre und Ausbildung für Juristen einsetzen. Auch in die Ausbildung der Informatiker sollten entsprechende Themen einbezogen werden. Es wäre in Deutschland insbesondere eine Aufgabe der GI (Gesellschaft für Informatik), dazu Empfehlungen zu erarbeiten.

Initiativen der GI

8. Das Programm einer erneuerten Rechtsinformatik bedarf der Umsetzung in Aktionen und in organisatorischen Zusammenhängen.

Dies setzt gemeinsame Anstrengungen voraus, sowohl mit den dogmatischen Fächern der Rechtswissenschaft, wie auch zur besseren Zusammenarbeit zwischen Juristen und Informatikern. Hierzu sind Initiativen von Seiten der GI in Vorbereitung. Es ist zu hoffen, daß gerade auch die Beiträge der Tagung „Die zweite Geburt der Rechtsinformatik" Anregungen für gemeinsame Aktionen bieten.

Wie sind PCs und Personal Computing datenschutzrechtlich zu behandeln?

Helmut Rüßmann

Die Überredungskunst Herbert Fiedlers

Nach meinem Schlußvortrag: „Richterliche Tätigkeit und Datenschutz" auf dem Ersten Deutschen EDV-Gerichtstag in Saarbrücken 1992 war ich fest entschlossen, mich nicht mehr zu Fragen des Datenschutzrechts zu äußern. Ich bin Zivilrechtler und Prozeßrechtler sowie PC-Nutzer. Datenschutzrechtlich kann ich mich nur als Laien bezeichnen. Die anscheinend weit verbreitete Annahme, der letzte Satz sei falsch, ist wohl dem Umstand zuzuschreiben, daß das Parlament eines Bundeslandes mich zum Datenschutzbeauftragten dieses Landes gewählt hatte. Ich trat indessen das Amt nie an. Hätte ich es angetreten, wäre ich wohl heute ein Experte des Datenschutzrechts. Aber ich tat es nicht, und deshalb war der Entschluß zur Enthaltsamkeit in öffentlichen Äußerungen zum Datenschutzrecht wohl begründet. Die Überredungskunst Herbert Fiedlers brachte den Entschluß, mich nicht mehr zu Fragen des Datenschutzrechts zu äußern, ins Wanken. Aufgegeben wurde er, nachdem ein Mitarbeiter eine einfache Großlösung für die datenschutzrechtliche Behandlung von PCs und Personal Computing in Aussicht gestellt hatte. Sie lief auf eine teleologische Reduktion des Anwendungsbereichs des Datenschutzrechts (der Datenschutzgesetze des Bundes und der Länder sowie der Verbote und Regelungsvorbehalte aus dem Recht auf informationelle Selbstbestimmung) auf Großrechenanlagen hinaus. Vor dem Hintergrund der auf solchen Anlagen erfaßbaren Datenmengen sei das Recht auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht entwickelt worden[2]. Die von den Verarbeitungskapazitäten solcher Anlagen ausgehenden Gefahren hätten bei der Entwicklung des Datenschutzrechts Pate gestanden. PCs verfügten nicht über entsprechende Speicher- und Verarbeitungsmöglichkeiten. Sie seien deshalb datenschutzrechtlich frei.

Man kann sich sicherlich denken, daß dem PC-Anwender in mir diese einfache Großlösung nur recht sein konnte. Bei einer näheren Beschäftigung mit dem Thema mußte der Begründungstheoretiker in mir allerdings bald einräumen, daß es für die sympathische einfache Großlösung keine methodische Grundlage gibt. Zum einen reicht heute schon die Verarbeitungskapazität vieler PCs an das heran, was vor einigen Jahren noch Großrechenanla-

Prof. Dr. Helmut Rüßmann ist Richter am OLG Saarbrücken und Inhaber des Lehrstuhls für Bürgerliches Recht, Zivilprozeßrecht und Rechtsphilosophie an der Universität des Saarlandes.

[2] BVerfGE 65, 1 (49 ff.) – Volkszählungsurteil. Zur Entwicklung des Rechts auf informationelle Selbstbestimmung eingehend *Matthias Schuster*, Die Übermittlung von Personaldaten unter besonderer Berücksichtigung des Datenschutzes, Diss. Köln 1988, S. 45 ff.

gen vorbehalten war. Es kommen die immer weiter um sich greifenden Vernetzungsmöglichkeiten und damit der Zugriff auf immer größere Datenmengen hinzu. Zum anderen aber – und das ist entscheidend – werden für die Rechtsanwendung relevante Ziele nicht nach Sympathie des Rechtsanwenders vergeben, sondern in erster Linie durch den Gesetzgeber festgelegt. Und der hat sich ausweislich der Materialien zur Novellierung des Bundesdatenschutzgesetzes eindeutig dahin entschieden, daß die Regeln des Bundesdatenschutzgesetzes auch für die Datenverarbeitung auf dem PC Anwendung finden[3].

Fallstudie „Übungsverwaltung"

Ich kann also nicht mit einer einfachen Großlösung aufwarten. Das Datenschutzrecht gilt prinzipiell auch für das Personal Computing. Gesellschaftlich erfaßt das Personal Computing angesichts der heutigen Verbreitung von PCs riesige Bereiche. Es ist ausgeschlossen, globale Lösungen für alle Bereiche des PC-Einsatzes im Rahmen eines Vortrags anzubieten. Aus der Not läßt sich eine Tugend machen, indem man einen möglichen Bereich des PC-Einsatzes herausgreift und die datenschutzrechtlichen Probleme exemplarisch diskutiert. Bei einer Versammlung von Lehrenden liegt es nicht allzu fern, die Verwaltung von Übungen im Rahmen der Juristenausbildung zum Gegenstand der nachfolgenden Betrachtungen zu machen. Der Bereich ist überschaubar, und ein jeder verfügt über nützliches Anschauungsmaterial aus seiner eigenen Erfahrung. Ich selber habe aus Anlaß des Vortrages entdeckt, daß an meinem Lehrstuhl vielleicht doch nicht alles mit rechten Dingen zugeht. Ich halte es nicht für ausgeschlossen, daß auch andere in den nächsten Minuten für ihren Bereich eine ähnliche Entdeckung machen.

Stadien der Übungsverwaltung: Anmeldung, Leistungserfassung, Scheinerteilung, Archivierung

Eine Übungsverwaltung durchläuft die Stationen der Anmeldung, der Leistungserfassung, der Scheinerteilung und der Archivierung. Das Festhalten der relevanten Daten kann in Karteikästen oder Listen geschehen. Wenn die Scheine mit einer Schreibmaschine ausgefüllt werden, braucht es nicht zum Einsatz eines Computers zu kommen. Es ist aber auch denkbar und vielleicht sogar schon überwiegend üblich, daß man zur Übungsverwaltung einen Computer einsetzt. Auf ihm mag ein speziell für die Übungsverwaltung entwickeltes Programm laufen. Es kann aber auch zum Einsatz von Standardsoftware von Datenbankprogrammen über Tabellenkalkulationen bis zur Textverarbeitung kommen.

Prüfung an Hand des BDSG

Was ist nun datenschutzrechtlich zur Übungsverwaltung zu sagen? Ich möchte dieser Frage vor dem Hintergrund des Bundesdatenschutzgesetzes nachgehen, obwohl dieses Gesetz auf die Übungsverwaltung keine Anwendung findet. Zum einen ist die Universität keine öffentliche Stelle des Bundes (§ 1 Abs. 1 Satz 2 Nr. 1 BDSG); zum anderen gehört sie auch nicht zu den öffentlichen Stellen der Länder, die Bundesrecht ausführen (§ 1 Abs. 2 Nr. 2 lit. a BDSG). Das saarländische Landesrecht kennt keine bereichsspezifische Regelung der Übungsverwaltung[4]. Das saarländische Universitätsgesetz bestimmt in dem Kapitel über Studenten und Studentenschaft, daß in einer der Zustimmung des zuständigen Ministers bedürftigen Ordnung im einzelnen festzulegen sei,

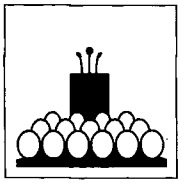
1. welche erforderlichen Daten zur Person sowie zur Hochschulzugangsberechtigung, zum Studienverlauf und zu Prüfungen erhoben werden,
2. an wen, zu welchen Zwecken und unter welchen Voraussetzungen diese Daten übermittelt werden können,
3. in welcher Form Auskunft an den Betroffenen über die zu seiner Person gespeicherten Daten erteilt wird und
4. wann die Daten zu löschen sind; für die Bestimmung des Zeitpunkts der Löschung sind die Belange des Auskunftspflichtigen und der Hochschulverwaltung zu berücksichtigen.

Eine solche Ordnung ist bislang nicht in Kraft gesetzt worden. Ich vermute, daß die Rechtslage sich in den anderen Bundesländern vergleichbar darstellt. Dem bin ich aber nicht weiter nachgegangen. Im Bundesdatenschutzgesetz finden wir jedenfalls in einer Art Modellgesetz die allgemeinen Grundsätze des Datenschutzrechts, anhand derer sich die datenschutzrechtlichen Probleme der Übungsverwaltung beispielhaft zeigen lassen. Es dürfte nicht schwer sein, die Überlegungen am jeweils einschlägigen Landesrecht nachzuvollziehen.

---

3 Vgl. *Auernhammer*, Bundesdatenschutzgesetz, 1991, Einführung Rdnr. 25 mit wörtlichen Belegen aus der Begründung zum Regierungsentwurf.

4 Es gilt das Saarländische Datenschutzgesetz vom 17. Mai 1978, das inhaltlich weitgehend mit den Regelungen des BDSG übereinstimmt.



Anmeldung

Die Übungsverwaltung beginnt mit der Anmeldung. Dort werden personenbezogene Daten erhoben[5]. Die Erhebung ist nach § 13 Abs. 1 BDSG nur zulässig, wenn die Daten zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich sind. Das gilt völlig unabhängig davon, in welchem Medium die Übungsverwaltung stattfindet. Bei der letzten von mir veranstalteten Übung im Bürgerlichen Recht für Fortgeschrittene im Sommersemester 1993 habe ich einen Anmeldungsbogen verwendet, in dem die Studierenden zur Preisgabe der folgenden Daten angehalten wurden: *Name, Vorname, Matrikelnummer, Anschrift, Geburtsdatum, Geschlecht, Anzahl der Fachsemester, Anzahl der Studiensemester, Teilnahme zum Erwerb des Übungsscheins oder Teilnahme nur zu Übungszwecken, Anzahl der Versuche zum Erwerb des Übungsscheins im Bürgerlichen Recht für Fortgeschrittene.* Weder das Geburtsdatum noch das Geschlecht noch die Anzahl der Fachsemester oder Studiensemester noch die Anzahl der Versuche, den Übungsschein im Bürgerlichen Recht für Fortgeschrittene zu erwerben, sind zur Durchführung einer ordnungsgemäßen Übung erforderlich. Sie ermöglichen mehr oder weniger interessante statistische Auswertungen. Für die Scheinerteilung benötigt man sie nicht. Nur wenn man auf dem Schein den glücklichen Erwerber mit „Herr" oder die glückliche Erwerberin mit „Frau" anreden möchte, bedarf es der Angaben zum Geschlecht, weil Vornamen häufig keine eindeutige Entscheidung ermöglichen[6]. Es steht die Höflichkeit gegen das Datenschutzrecht. Und da siegt allemal das Recht?! Bei strenger Betrachtung schuf also schon die Datenerhebung bei der Anmeldung einen datenschutzrechtswidrigen Zustand.

Das Werkzeug: ACCESS

Die Verarbeitung der erhobenen Daten an meinem Lehrstuhl rief einen weiteren datenschutzrechtswidrigen Zustand ins Leben. Die Daten wurden nämlich unter Verwendung eines Standarddatenbankprogramms[7] in einen Computer eingegeben. Damit war der Tatbestand der automatisierten Verarbeitung erfüllt. Wir sind auch als datenschutzrechtliche Laien daran gewöhnt, datenschutzrechtliche Fragen gerade im Zusammenhang mit der Automation der Datenverarbeitung zu sehen. Und das ist auch der Standpunkt des Gesetzgebers, der durch § 1 Abs. 3 Nr. 2 BDSG automatisierte Dateien strengeren Vorschriften unterwirft als nichtautomatisierte Dateien. Das legt folgende Argumentation nahe:

Die Einwilligungsproblematik

Nach § 4 Abs. 1 BDSG ist eine Verarbeitung darunter versteht der Gesetzgeber *„das Speichern, Verändern, Übermitteln, Sperren und Löschen"* (§ 3 BDSG) personenbezogener Daten nur zulässig, wenn sie durch Rechtsvorschrift angeordnet oder erlaubt ist oder soweit der Betroffene eingewilligt hat. Eine Rechtsvorschrift, die die automatisierte Verarbeitung erlaubte, gibt es nicht. § 14 Abs. 1 BDSG knüpft das Speichern – darunter versteht der Gesetzgeber *„das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke der weiteren Verarbeitung oder Nutzung"* (§ 3 Abs. 5 Nr. 1 BDSG) –, Verändern oder Nutzen personenbezogener Daten an das Merkmal der Erforderlichkeit zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben. Erforderlich ist die Verwendung von PCs sicherlich nicht, wie die Praxis vor der Einführung von PCs zeigt. Die Verwendung von PCs macht das Arbeiten angenehmer. Zum Teil befriedigt sie auch nur den Spieltrieb des Verwenders: *„Wie bekomme ich am Ende die Scheine etwa unter Verwendung der Serienbrieffunktion des Textverarbeitungsprogramms auf Knopfdruck aus dem Drucker?"* Die Arbeiten könnten aber auch ohne PC erledigt werden. Es bleibt die Einwilligung, um der Eingabe in den Computer das Odium der Rechtswidrigkeit zu nehmen[8]. Doch fehlte es insoweit jedenfalls in meiner Übung an den besonderen Voraussetzungen, die § 4 Abs. 2 BDSG[9] für die Wirksamkeit der Einwilligung aufstellt. Die Anmeldung zur Übung geschah zwar schriftlich. Doch fehlte auf dem Erfas-

---

5 Zum Begriff der personenbezogenen Daten vgl. *Tinnefeld/Ehmann*, Einführung in das Datenschutzrecht, 1992, S. 83 ff.

6 Dies zeigt sehr schön die Frage: „Is she a man?", die ein amerikanischer Kollege zur Person von Heike Jung stellte, als er zu einem Forschungsaufenthalt in Saarbrücken verfrüht ein- und Heike Jung deshalb nicht antraf. Für ihn war Heike Jung eine Frau, und das ist Heike Jung, wie wir in Saarbrücken wissen, nicht.

7 Microsoft-ACCESS, Version 1.0.

8 Vgl. *Tinnefeld/Ehmann*, S. 103 ff.

9 Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

sungsbogen jeglicher Hinweis darauf, daß die Daten in einem automatisierten Verfahren verarbeitet würden.

Einwilligung gerade für die automatisierte Verarbeitung erforderlich

Dieser Argumentation läßt sich nicht mit dem Hinweis begegnen, daß der Text der §§ 4 und 14 BDSG nicht zwischen automatisierter Verarbeitung und nichtautomatisierter Verarbeitung unterscheide und es deshalb nur darauf ankommen könne, ob die Verarbeitung überhaupt (in welcher Form auch immer) zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich sei. Die durch § 1 Abs. 3 BDSG begründete Systematik des Datenschutzgesetzes belehrt uns eines Besseren. Auf die nichtautomatisierten Dateien finden die §§ 4 und 14 BDSG keine Anwendung. Deshalb kann die Erforderlichkeit zur Erfüllung der Aufgaben der speichernden Stelle nur auf die besondere Form der automatisierten Verarbeitung bezogen sein. Und auch die Einwilligung muß sich gerade auf die Form der automatisierten Verarbeitung der Daten beziehen.

Pflichten aus § 9 BDSG

Nun läßt sich sicherlich denken, daß man für die nächste Übung ein Anmeldeformular entwirft, in dem dem Datenschutz Rechnung getragen wird. In diesem Formular müßte der Übungsveranstalter einerseits seine Neugierde zügeln und andererseits einen deutlichen Hinweis darauf geben, daß die Daten in ein Computersystem eingegeben und automatisch verarbeitet werden. Die Probleme sind damit aber noch nicht zu Ende. Eigentlich fangen sie jetzt erst an. § 9 BDSG verpflichtet den Übungsverwalter nun, *„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"*. Die nur für die automatisierte Verarbeitung personenbezogener Daten bestimmte Anlage hat es in sich. Ich gebe sie zunächst in ihrem Wortlaut wieder:

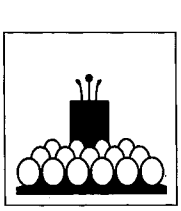
„Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

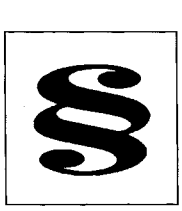
1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),
7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle)."

Die Pflichten nach der Anlage gelten auch für PC's.

Für die in dieser Anlage gestellten Anforderungen gilt ebenfalls kein Großrechnervorbehalt. Der Gesetzgeber hat die Anlage auch für das Personal Computing in Geltung gesetzt[10]. Es könnte allerdings sein, daß die in Satz 2 des § 9 BDSG zum Ausdruck gebrachte

[10] Aus der allgemeinen Begründung des Regierungsentwurfs: *„Die Anlage zu § 9 Satz 1 stellt keine Anforderungen auf, die nicht auch für Arbeitsplatzrechner und vernetzte Systeme erfüllt werden können."*





Einschränkung der Erforderlichkeit durch den Grundsatz der Verhältnismäßigkeit im engeren Sinne im PC-Bereich verstärkt zur Anwendung kommt. Diese Einschränkung ist von rechtstheoretischer Delikatesse. Sie erklärt etwas für nicht erforderlich, was zum Schutze des Rechtsguts an sich erforderlich ist. So etwas gelingt nur Juristen. In Wahrheit wird das zu schützende Rechtsgut relativiert. Es muß sich in der Konkurrenz zu widerstreitenden Rechtsgütern und haushaltspolitischen Zwängen durchsetzen.

Schutzzweck des Datenschutzrechts: § 1 BDSG

Den Schutzzweck des Datenschutzrechts legt § 1 BDSG fest. Der Einzelne ist danach davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Wiewohl absolut formuliert, kann es doch nicht um den Schutz auch der kleinsten Beeinträchtigung um jeden Preis gehen. Das macht § 9 Satz 2 BDSG deutlich, der nur solche Maßnahmen für erforderlich erklärt, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Damit eröffnet § 9 Satz 2 BDSG ein flexibles Reaktionspotential, in dem auf die Schwere der Beeinträchtigung, die Sensitivität der gespeicherten personenbezogenen Daten und die Wahrscheinlichkeit des Eintritts einer Beeinträchtigung Bedacht genommen und mit dem Schutzaufwand zur Verhinderung der Beeinträchtigung ins Verhältnis gesetzt werden kann[11].

Sensitivität von Noten

Wie sensitiv sind Noten, die für Leistungen in Übungen vergeben werden? Das möge jeder für sich selbst beantworten. Die einen werden einen kaum ins Gewicht fallenden Sensitivitätsgrad annehmen, weil auf dem Universitätscampus ohnehin jeder über jeden alles wisse. Die anderen mögen für höchste Sensitivität votieren, wenn sie daran denken, daß die Übungsdaten bei freier und unkontrollierter Verbreitung ohne Wissen des Betroffenen auf dem Rechner des Personalchefs liegen, mit dem der Betroffene gerade ein Einstellungsgespräch führt. Ich entscheide mich für mittlere Sensitivität, was immer das heißen mag.

Persönlichkeitsrechte der Betroffenen

Wodurch könnte im Umgang mit personenbezogenen Daten das Persönlichkeitsrecht des Betroffenen verletzt werden? Welches sind mit anderen Worten die Schutzaspekte, um deren Wahrung es dem § 9 Satz 1 BDSG und dem Maßnahmekatalog der Anlage zu § 9 Satz 1 BDSG zu tun ist? Drei Aspekte kommen in Betracht: die Datenintegrität, die Datenvertraulichkeit und die Zweckbindung im Umgang mit den Daten[12]. Zur Datensicherheit im allgemeinen gehört auch die Verfügbarkeit der Daten für den berechtigten Nutzer. Die Datenverfügbarkeit ist allerdings kein Aspekt, um dessentwillen § 9 BDSG einschließlich seiner Anlage geschaffen worden wäre.

Datenintegrität

Die Datenintegrität spricht den Schutz vor der Verfälschung personenbezogener Daten an. Die Datenintegrität kann sowohl durch nicht berechtigte Nutzer, die in das System einbrechen, wie durch berechtigte Nutzer bedroht werden. Die Wahrscheinlichkeit, daß der berechtigte Nutzer eines Übungsverwaltungsprogramms falsche Noten einträgt, erscheint indessen so gering, daß Maßnahmen zum Schutz der Datenintegrität nur mit Blick auf unberechtigte Nutzer ins Auge zu fassen sind.

Datenvertraulichkeit

Die Datenvertraulichkeit gebietet die Geheimhaltung der zulässigerweise erhobenen und verarbeiteten personenbezogenen Daten und damit den Schutz vor der Kenntnisnahme und Nutzung durch Unbefugte.

Zweckbindung

Die Zweckbindung schützt vor der Verarbeitung und Nutzung zu anderen Zwecken als denen, zu denen die personenbezogenen Daten erhoben und ihre Verarbeitung erlaubt worden sind. Für diesen Bereich sind nicht nur die ursprünglich Unbefugten, sondern auch die ursprünglich Befugten ins Auge zu fassen: Der Professor greift für die Erstellung von Gutachten oder für die Entscheidung über eine Einstellung auf die Übungsdateien zurück.

Welche Maßnahmen nun beim Einsatz von PC's für die automatisierte Verwaltung von Übungsdaten zur Wahrung von Datenintegrität, Datenvertraulichkeit und Zweckbindung vorzusehen sind, läßt sich nicht generell beantworten. Zu verschiedenartig sind die Arbeitsumgebungen gestaltet, in denen die automatisierte Verwaltung Platz greifen kann. Beispielhaft möchte ich drei Szenarios ansprechen: den professoralen Einzelkämpfer am Stand-alone-PC, die Teamarbeit am Lehrstuhl-stand-alone-PC und die Teamarbeit im lokalen Netzwerk (LAN) des Lehrstuhls.

---

[11] *Dammann* in: *Simitis/Dammann/Mallmann/Reh*, Kommentar zum Bundesdatenschutzgesetz, 3. Aufl. 1981, § 6 Rdnr. 32; AOrdemann/Schomerus, BDSG, 5. Aufl. 1992, § 9 Anm. 2.3.

[12] Vgl. *Tinnefeld/Ehmann*, S. 253 ff.

Szenario 1: Der professorale Einzelkämpfer

Der professorale Einzelkämpfer am Stand-alone-PC (Hochschullehrer in Bremen) genügt den Anliegen der Datenintegrität und Datenvertraulichkeit dadurch, daß er den Raum verschließt, in dem der Computer steht. Schutzvorkehrungen vor datensüchtigen Putzfrauen und Hausmeistern braucht er nicht zu treffen. Ganz sicher ginge er allerdings auch insoweit noch, wenn er die sensiblen Daten auf einer Wechselplatte hätte, die er im Tresor verschlösse oder mit nach Hause nähme. Datenintegrität und Datenvertraulichkeit könnten allerdings auch bei ihm bedroht sein, wenn er den Computer zur Reparatur geben müßte. Vor den neugierigen Augen des technisch versierten Wartungspersonals wären die personenbezogenen Daten nur dann geschützt, wenn unser Einzelkämpfer sich eines Verschlüsselungsverfahrens bedient hätte. Manche Datenbank- und Tabellenkalkulationsprogramme bieten das standardmäßig an. Für mit anderen Programmen erstellte Datensammlungen müßte man ein zusätzliches Programm erwerben. Verlangen Datenintegrität und Datenvertraulichkeit den Einsatz von Verschlüsselungsverfahren und damit den Erwerb solcher Programme vom professoralen Einzelkämpfer? Ich meine nein.

Die Wahrscheinlichkeit, daß der PC mit den personenbezogenen Daten zur Reparatur gegeben werden muß und dort in die Hände eines datensüchtigen Reparateurs fällt, ist so gering, daß um dieser Gefahr willen, keine zusätzlichen Ausgaben (einschließlich des Lernaufwands für die Beherrschung neuer Programme) verlangt werden können. Zweckdienlich wäre allenfalls eine schriftliche Verpflichtung des Wartungspersonals auf die Wahrung des Datengeheimnisses[13].

Eine Eingabekontrolle (Nr. 10 der Anlage) ist für den professoralen Einzelkämpfer nicht erforderlich. Sie ließe sich unter DOS und auf DOS aufsetzenden Windows-Betriebssystemen nur mit zusätzlichen Programmen (wie etwa Safeguard) verwirklichen.

Noch offen ist, wie dem Schutzziel der zweckgebundenen Verwendung der personenbezogenen Daten Rechnung getragen, wie beispielsweise der Professor daran gehindert werden kann, die zu Zwecken der Übungsverwaltung aufgenommenen Daten zur Erstellung von Gutachten und Persönlichkeitprofilen (womöglich unter Mischung mit Daten aus anderen Übungen) zu nutzen. Die Frage kann für unsere Betrachtung offen bleiben. Denn mit ihr treten wir aus dem Maßnahmekatalog der Anlage zu § 9 BDSG heraus. Letztlich geht es um das Löschen nicht mehr benötigter personenbezogener Daten und damit um die Kontrollrechte des Betroffenen.

Szenario 2: Teamarbeit am Lehrstuhl-stand-alone-PC

Die Teamarbeit am Lehrstuhl-stand-alone-PC wirft erheblich größere Probleme zur Wahrung von Datenintegrität und Datenvertraulichkeit auf. Professor, Sekretärin und Mitarbeiter dürfen den PC nutzen. Sie sind aber nicht alle auch berechtigte Nutzer der zur Übungsverwaltung festgehaltenen Daten. Wie will man verhindern, daß die zur Übungsverwaltung nicht berechtigten Nutzer die Daten einsehen, sie kopieren und u. U. gar verändern?

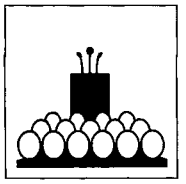
Sicherungsmöglichkeiten

Eine sichere, wenn auch umständliche Methode wäre die, die Übungsverwaltung exklusiv auf einem Wechselplattenlaufwerk und die Platte (Diskette) vom berechtigten Nutzer unter Verschluß zu halten. Wir bewegten uns dann im Szenario 1, wenn es nicht mehrere berechtigte Nutzer gäbe: etwa die Sekretärin, die die Daten eingibt, und den Professor, der die Daten auswertet. Dabei hätte sowohl die Sekretärin die Möglichkeit, Kopien zu fertigen, und der Professor die Gelegenheit, Daten zu ändern. Mit der Mehrfachszugriffsmöglichkeit müßten zum Schutze der Datenintegrität und der Datenvertraulichkeit die Zugriffe protokolliert werden. Das sehen die im PC-Bereich gängigen Betriebssysteme nicht vor. Schon deshalb könnte das Datenschutzrecht Softwarelösungen erzwingen, die die sprichwörtliche Unsicherheit der im PC-Bereich gängigen Betriebssysteme ausräumt. Datenschutzbeauftragte halten Safeguard für ausreichend.

Mißbrauchsmöglichkeiten

Die vom Datenschutzrecht verlangten Vorkehrungen werden dringlicher, wenn die Übungsverwaltung auf der nicht zum Austausch und Verschluß vorgesehenen Festplatte liegt. Ohne besondere Vorkehrungen scheint sie dann dem Zugriff eines jeden Lehrstuhlmitarbeiters anheim gegeben. Und jeder Mitarbeiter könnte nach harter wissenschaftlicher Arbeit seine Entspannung darin suchen, einmal nicht Solitair oder Minesweeper zu spielen, sondern nachzuschauen, was denn des verhaßten Lehrers Kinder in der BGB-Übung leisten. Im Interessefall ist auch schnell eine Kopie gezogen. Bestimmte Datenbank- und Tabellenkalkulationsprogramme bieten hier allerdings schon von sich aus Vorkehrungen, um

[13] Vgl. Nr. 8 der Bremer Richtlinien für den Datenschutz am Arbeitsplatz vom 7. August 1990 (Amtsblatt S. 221).



die Daten vor neugierigen Augen Unbefugter zu schützen (allerdings nicht vor der Zerstörung durch Frust). Sie können so eingerichtet werden, daß nur berechtigte Nutzer das Programm aufrufen dürfen. Zudem besteht die Möglichkeit, Dateien zu verschlüsseln und durch Passwörter zu schützen. Dadurch wird auch das Aufrufen der Datei durch denselben Programmtyp auf einem anderen Rechner verhindert.

Szenario 3: Mehrfachnutzung und Vernetzung

Auf dem ersten Blick sieht es so aus, als müßten die datenschutzrechtlichen Probleme, die die Übungsverwaltung auf dem PC aufwirft, im dritten Szenario noch drückender sein. Zur Mehrfachnutzung kommt jetzt auch noch die Vernetzung hinzu. Das Gesamtsystem wird komplizierter. Die Schutzvorkehrungen scheinen schwieriger zu werden. Dem ist aber nicht unbedingt so. Die Vernetzung bietet nämlich auch die Möglichkeit, ein wenig von der datenschutzrechtlich heilen Welt des professoralen Einzelkämpfers wieder zu gewinnen.

Fallstudie: Peer-to-peer-Netz unter Windows für Workgroups

Zur Zeit der letzten Übung im Sommersemester 1993 war an meinem Lehrstuhl ein Peer-to-peer-Netz unter Windows für Workgroups im Einsatz. Die Übungsverwaltungsdatei lag auf meinem Rechner (dort liegt sie noch). Sie hätte dreifachen Schutz vor neugierigen Einblicken genießen können, mußte sich tatsächlich mit einem zweifachen begnügen. Erstens konnte das Verzeichnis, in dem die Datei lag, nur von meinem Rechner allerdings von allen Nutzern meines Rechners oder von einem anderem im Netz befindlichen Rechner angesprochen werden, wenn das Verzeichnis von mir freigegeben war und der Nutzer des anderen Rechners das zur Freischaltung erforderliche Passwort kannte. Zweitens konnte das Datenbankprogramm nur durch die berechtigten Nutzer aufgerufen werden. Drittens hätte die Möglichkeit bestanden, die Datei als solche durch ein Kennwort zu schützen und zu verschlüsseln. Wäre nun mein Raum während meiner Abwesenheit verschlossen gewesen, hätten wir eine Situation ähnlich dem Szenario 1 vorgefunden. Tatsächlich war das nicht der Fall, und es gab auch kein Verbot für die Mitarbeiter, meinen Rechner zu nutzen. Vor diesem Hintergrund wäre es geboten gewesen, die kryptographischen Möglichkeiten von ACCESS einzusetzen.

Datenschutzmöglichkeiten unter Windows NT

Heute sieht die Situation an meinem Lehrstuhl datenschutzrechtlich günstiger aus. Jedenfalls mein Rechner hat Abschied von DOS und den auf DOS aufbauenden Betriebssystemen genommen. Windows NT bietet als Betriebssystem auch bei der Nutzung des Computers durch verschiedene Personen an Sicherungsmaßnahmen all das, was § 9 BDSG für die automatisierte Übungsverwaltung verlangt: paßwortgeschütztes Logon nur für legitimierte Nutzer, Protokollfunktionen, differenzierte Berechtigungszuweisungen für Verzeichnisse, Programme und Dateien, Dateiverschlüsselungen. Nutzt man sie, darf man die Übungen in Zukunft mit datenschutzrechtlich reinem Gewissen automatisch verwalten.

Ein Argument für die bessere Ausstattung der Lehrstühle

Daraus ließe sich unter Umständen auch ein Argument für die bessere Ausstattung unserer Lehrstühle gewinnen. Welche Universitätsverwaltung kann sich dem Wunsch nach leistungsfähigeren Rechnern und Programmen verschließen, wenn nur die Erfüllung dieses Wunsches den Übergang von der Rechtswidrigkeit in die Rechtmäßigkeit der Übungsverwaltung ermöglicht?