9. Tätigkeitsbericht 2001/2002

9ème Rapport d'activités 2001/2002

Eidgenössischer
Datenschutzbeauftragter

Préposé fédéral à la protection
des données

Tätigkeitsbericht 2001/2002

des Eidgenössischen Datenschutz-beauftragten

Der Eidg. Datenschutzbeauftragte hat dem Bundesrat periodisch einen Bericht über seine Tätigkeit vorzulegen (Art. 30 DSG). Der vorliegende Bericht deckt den Zeitraum zwischen 1. April 2001 und 31. März 2002 ab.

Dieser Bericht ist auch über das Internet (www.edsb.ch) abrufbar

Inhaltsverzeichnis

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

Vorwort

Der 11. September veränderte die Diskussion zum Verhältnis zwischen der öffentlichen Sicherheit und dem Schutz der Persönlichkeit schlagartig. Seitdem zwei Flugzeuge die beiden Tower des World Trade Center in New York in Schutt und Asche legten, ist die Diskussion nicht mehr abgeflaut. Weltweit steht Terrorismusbekämpfung und die Frage nach der öffentlichen Sicherheit zuoberst auf der Traktandenliste. Im Zentrum der Auseinandersetzung steht damit auch die Frage, wie weit darf der Datenschutz angesichts dieser Bedrohung gehen. Das ist eine legitime Frage, denn Datenschutz bewegt sich nie im luftleeren Raum. Er beinhaltet ein ständiges Abwägen der unterschiedlichsten Interessen. Dieser Herausforderung hat man sich als Datenschützer zu stellen. Dabei liegt es an der Gesellschaft zu definieren, wie viel öffentliche Sicherheit sie wünscht und wie viel Schutz der Privatsphäre sie dafür opfern will.

Als Datenschützer haben wir diesen Prozess allerdings zu begleiten und dafür zu sorgen, dass die Grundsätze des Datenschutzgesetzes, welche mit grundlegenden Prinzipien eines freiheitlichen Rechtsstaates identisch sind, nicht aus den Augen verloren werden. Wir haben deshalb wiederholt darauf hingewiesen, dass vor irgendwelchen Reaktionen die Ursachen analysiert werden müssen und nur Massnahmen in Frage kommen, die zweckmässig und verhältnismässig sind. Das heisst, die vorgeschlagene Massnahme müssen tatsächlich mehr Sicherheit bringen und es muss gleichzeitig fest stehen, dass dieses Ziel auf einem andern, für den Einzelnen weniger einschneidenden Weg nicht erreicht werden kann.

Dabei sind zwei Punkte hervorzuheben: Mehr öffentliche Sicherheit muss nicht zum vornherein auf Kosten des Persönlichkeitsschutzes gehen: Wenn beispielsweise festgestellt wird, dass die mangelhaften Kontrollen auf den Flughäfen in den USA die Anschläge wesentlich begünstigt haben, steht aus datenschutzrechtlicher Sicht einer Verstärkung der Kontrolle nichts entgegen. Denn Datenschutz ist weder Täter- noch Terroristenschutz.

Gleichzeitig ist aber auch festzuhalten, dass ein rigoroses Sicherheitsdenken die Grundrechte eines freiheitlichen Rechtstaates zerstören kann. Wir müssen uns stets vor Augen halten, dass es eine absolute Sicherheit nicht gibt. Unsere westliche Zivilisation wird mit zunehmender technischer Entwicklung immer verwundbarer. Wissenschaftler und Intellektuelle analysieren dieses Phänomen nicht erst seit dem 11. September unter dem Stichwort «Risikogesellschaft». In den letzten Jahrzehnten standen in diesem Zusammenhang vor allem die Gefahren der Kernenergiegewinnung und der chemischen und biochemischem Produktionsprozesse im Zentrum. Als neuer Risikofaktor kommt hinzu, dass sich terroristische Strategien dieser vom Mensch geschaffenen technischen Risiken ebenfalls bedienen. Neu daran ist indessen nur, dass Terroris-

ten mittlerweile von dieser Möglichkeit tatsächlich auch Gebrauch machen. Risikotheoretiker haben dies längst vorausgesehen und erfolglos davor gewarnt.

Wie ist dieser Herausforderung in einem freiheitlich demokratischen Rechtsstaat zu begegnen? Könnte es sein, dass mit den zusammenbrechenden Türmen des World Trade Center auch die Hoffnung auf einen «zivilisierten» Umgang mit unseren modernen technischen Risiken zusammenbricht? Die Versuchung ist jedenfalls gross, dass man sich nicht mehr über den Sinn der durch die Technik verursachten Risiken und allfälliger Alternativen unterhält, sondern, darauf konzentriert, Sicherheit dadurch herzustellen, dass die heute zur Verfügung stehenden gewaltigen technischen Möglichkeiten zur Kontrolle und Ueberwachung der Bürgerinnen und Bürger eingesetzt werden. Totale Sicherheit hiesse dann Einführung von umfassenden DNA-Datenbanken, kombiniert mit Rasterfahndung, Erstellung von Täterprofilen, flächendeckende Video- und Satellitenüberwachung, Verknüpfung von sämtlichen bestehenden Datenbanken und Einsatz des GPS (Global Positioning System), mit dem der Standort jeder Person jederzeit ermittelt werden könnte. Das ist kein Hirngespinst aus einem Sciencefiction-Roman, sondern eine mit den heute bestehenden technischen Möglichkeiten realisierbare Horrorvision. Orwell ist durch die realen Möglichkeiten längst überholt! Damit dieser Horror nicht schrittweise Realität wird, brauchen wir eine offene Debatte mit mündigen Bürgerinnen und Bürger, die wissen, dass totale Sicherheit in den Totalitarismus führt.

Dieser Risikodiskurs muss deshalb radikal erweitert werden, wenn wir nicht einen schleichenden Abbau des freiheitlich demokratischen Rechtsstaates in Kauf nehmen wollen. Dieser Prozess ist deshalb stets schleichend, weil Demokratie, Datenschutz und Freiheitsrechte nicht einfach vorhanden sind oder fehlen. Diese Werte sind stets mehr oder weniger vorhanden und verschwinden, wenn sie nicht beansprucht und verteidigt werden. In dem Mass wie wir unsere technischen Möglichkeiten immer weiter treiben (AKW, Genmanipulation, Computertechnologie, Internet usw.), müssen wir uns auch bewusst sein, dass wir damit angreifbarer werden. Katastrophen – nicht nur terroristische! – werden im Rahmen des technisch Denkbaren mit einer gewissen Wahrscheinlichkeit auch geschehen. Das bedeutet, dass der Risikodialog bereits bei der Frage ansetzen muss, welcher technische Fortschritt unter dem Gesichtspunkt der Gefahrenzunahme gesellschaftlich noch akzeptiert werden kann. Nach dem Grundsatz: Nicht alles, was technisch möglich ist, darf auch realisiert werden. Wenn diese Risikodebatte nur auf das Spektrum der Terrorismusbekämpfung reduziert wird, blenden wir andere ebenso virulente Gefahren aus und wähnen uns am Ende in falscher Sicherheit. Wie delikat diese Diskussion ist, zeigt sich am Beispiel des Internet: Niemand möchte dieses genial einfache Kommunikationsmittel missen. Ganze Wirtschaftszweige leben davon und nicht nur Weltfirmen, sondern auch mittlere und klei-

nere Unternehmer benützen es täglich. Wenn nun der Verdacht besteht, dass Osama bin Laden die Angriffe über das Internet vorbereitet und koordiniert hat, könnte dieser Gefahr durch eine rigorose Kontrolle des Internetverkehrs, mit dem Verbot von Verschlüsselung (wie von den USA verlangt) begegnet werden. Das wäre aber auch gleichzeitig das Ende des Internets. Denn wer wäre bereit, dieses Kommunikationsmittel zu benützen, wenn er gleichzeitig damit rechnen muss, dass die Geheimdienste jederzeit in jede Meldung Einblick nehmen können? Das heisst, es gibt unserer komplexen Welt keine einfachen Antworten mehr. Am Schluss bleibt stets die Erkenntnis, dass wir in einer Risikogesellschaft leben (und dazu auch immer wieder ja sagen) und deshalb auch Risiken bewusst wahrnehmen müssen.

Mein Vorgänger Odilo Guntern, dem ich an dieser Stelle für seine hervorragende Aufbauarbeit als erster Eidgenössischer Datenschutzbeauftragter meine Anerkennung und meinen Dank aussprechen möchte, hat 1994 in seinem ersten Tätigkeitsbericht darauf hingewiesen, dass eine der Aufgaben des Datenschutzbeauftragten sei, zur Entwicklung des Datenschutzbewusstsein beizutragen. Das ist ihm in ausgezeichneter Weise gelungen. Es ist ihm und seinen Mitarbeiterinnen und Mitarbeiter zu verdanken, dass diese Institution in der Bevölkerung ein hohes Ansehen hat und täglich um Rat und Stellungnahmen gebeten wird. Ich werde in diesem Bemühen weiter fahren.

Dabei scheint im Augenblick die innere Sicherheit sämtliche andere Themen in den Hintergrund zu stellen. Nun sind aber auch in andern Bereichen bedeutsame Entwicklungen im Gange, welche den Datenschutz herausfordern. Im Gesundheitswesen hält das elektronische Patientendossier mehr und mehr Einzug und schafft Chancen und Risiken für den Datenschutz. Wir sind hautnah dabei, indem wir ein Projekt begleiten, bei dem wir beispielhaft zeigen wollen, wie die Chancen genutzt und die Risiken vermieden werden. Mit der Gesundheitskarte stehen weitere Neuerungen zur Diskussion, welche aus Sicht des Datenschutzes begleitet werden müssen.

Eine wichtige Diskussion findet derzeit im Zusammenhang mit der Benützung von DNA-Analysen in Strafverfahren statt. In welchen Fällen darf eine solche Untersuchung durchgeführt werden und wer darf schliesslich in einer DNA–Datenbank gespeichert werden und wie lange?

Nicht minder bedeutsam ist die derzeit stattfindende Revision des Datenschutzgesetzes: Sie bringt eine wichtige Verstärkung des Persönlichkeitsschutzes, indem Bürgerinnen und Bürger automatisch informiert werden müssen, wenn über sie besonders schützenswerte Daten gespeichert und bearbeitet werden. Ich wünschte mir im Rahmen dieser Revision zusätzlich eine Verstärkung der Eigenverantwortlichkeit der Datenbearbeiter. Datenschutz muss vermehrt auch als Verkaufsargument eingesetzt werden und Konsumentinnen und Konsumenten sollten Firmen und ihre Produkte bevor-

zugen, welche in datenschutzrechtlicher Hinsicht vorbildlich sind. Im Umweltbereich hat sich dieser marktwirtschaftliche Ansatz längst durchgesetzt: Ein Produkt kann sich als besonders umweltfreundlich auszeichnen lassen, Nahrungsmittel erhalten das Prädikat «biologisch» und brachten einem Grossverteiler im vergangen Jahr überdurchschnittliche Wachstumsraten. Das Gleiche sollte im Bereich Datenschutz angestrebt werden: Wer sich selber einem Datenschutzaudit unterzieht, soll dafür ein Gütesiegel erhalten und sich damit im Markt einen Vorteil verschaffen können. Das setzt zwei Dinge voraus: Der Gesetzgeber sollte dies in der laufenden Revision berücksichtigen und die Konsumenten sollten vermehrt jenen Produkten den Vorzug geben, welche den Datenschutz ernst nehmen.

Hanspeter Thür

Abkürzungsverzeichnis

AUPER	Automatisiertes Personenregister
BAP	Bundesamt für Polizei
BKP	Bundeskriminalpolizei
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
CIRCA	Communication & Information Resource Centre Administrator
CJPD	Projektgruppe für den Datenschutz
CJPD GTPJ	Arbeitsgruppe für den Datenschutz bei Polizeidaten und gerichtlichen Daten in Strafsachen
DAP	Dienst für Analyse und Prävention
EDI	Eidgenössisches Departement des Innern
EJPD	Eidg. Justiz- und Polizeidepartement
GEWA	Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei
IDA	Interexchange of Data between Administrations (Informationenaus tausch zwischen öffentlichen Verwaltungen)
IPAS	Informatisiertes Personennachweis-, Aktennachweis- und Verwaltungs system
ISIS	Staatsschutz-Informations-System
JANUS	Gemeinsames Informationssystem der kriminalpolizeilichen Zentral stellen des Bundes
KVG	Bundesgesetz über die Krankenversicherung
PESEUS	Projektgruppe – EJPD – Strategie - EU-Schweiz
PSBV	Verordnung über die Personensicherheitsprüfungen
RIPOL	Automatisiertes Fahndungssystem
SIRENE	Supplementary Information Request at the National Entry
SIS	Das Schengener Informationssystem
StGB	Strafgesetzbuch
VBS	Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport
VVG	Versicherungsvertragsgesetz
ZAR	Zentrales Ausländerregister
ZentG	Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes
ZStV	Zivilstandsverordnung

1. Grundrechte

1.1. E-Government

Trotz aller Unbestimmtheit der Bezeichnung E-Government können darunter die Transformationsprojekte in der Verwaltung zusammengefasst werden, deren Umsetzung einen signifikanten Informatikanteil beinhaltet. Auf Bundesebene sind aufgrund ihrer Sichtbarkeit insbesondere das Projekt des virtuellen Amtsschalters (Guichet virtuel) sowie die Bestrebungen in Richtung elektronischer Stimmabgabe (Vote électronique) zu nennen. Beide verfolgen hochgesteckte Ziele und sind aus der Optik des Datenschutzes von Bedeutung.

Guichet Virtuel

Gemäss E-Government-Strategie des Bundes ist Guichet virtuel eines der strategischen Leitprojekte. Sein Inhalt ist das «Schaffen eines nach Alltagsproblemen der Bürgerinnen und Bürger gegliederten Zugangs zu den Behörden». Schon aus dieser Beschreibung geht hervor, dass Zweck und Grenzen des Projekts zwar sehr umfassend, aber auch ausserordentlich unscharf definiert sind. Für eine echte Beurteilung aus Optik des Datenschutzes ist es jedoch zentral zu wissen, welches schliesslich die Geschäfte sind, die über den virtuellen Amtsschalter abgewickelt werden. Erst aufgrund dieser Angaben kann auch beurteilt werden, welche Informationen zu diesem Zwecke über den Amtsschalter fliessen sollen bzw. dürfen und erst dann können für die verschiedenen Geschäftsfälle die erforderlichen Sicherheitsmassnahmen zugeordnet und umgesetzt werden.

Soweit wir den Prototyp begleitet haben, wies er noch keine wirkliche Funktionalität auf, welche aus Datenschutzsicht hätte beurteilt werden können. Für die Jahre ab 2002 ist gemäss E-Government-Strategie des Bundes der «Aufbau eines Kommunikations- und Transaktionsportals» geplant. Für verschiedene Kategorien von Kommunikation und für jede Art von Transaktionen werden sich Sicherheitsfragen organisatorischer und technischer Natur stellen, welche in verschiedenen Bereichen der Datensicherheit angesiedelt sind. Zu erwähnen sind hier insbesondere die Wahl und Ausgestaltung der für Identifikation und Authentifikation einzusetzenden Verfahren sowie diejenigen zum Schutz der Vertraulichkeit, sei es der Teilnehmer oder bloss des Kommunikationsinhaltes. Weiter ist für die verschiedenen Geschäftsfälle jeweils zu fragen, welcher Grad an Verbindlichkeit und Nachvollziehbarkeit zu gewährleisten ist. Und schliesslich dürfte in vielen Fällen nicht trivial sein, Berechtigungen (Autorisierungen), die in der nicht-virtuellen Welt als selbstverständlich erscheinen, korrekt in den mit dem Guichet

virtuel zusammenwirkenden Systemen zu implementieren. Sobald mit der Einführung von virtuellen Transaktionen schliesslich Kompetenzen geändert werden, stellen sich Fragen, die weit über die Technik hinaus gehen.

Vote électronique

Der bundesrätliche «Bericht über den Vote électronique» vom 9. Januar 2002 definiert den Begriff Vote électronique als die Vereinigung von drei recht unterschiedlichen Teilgebieten. Das erste, die Möglichkeit für Behörden, Wahl- und Abstimmungsinformation elektronisch zur Verfügung zu stellen, ist vom Prinzip her schon heute mehr oder weniger gegeben. Die Möglichkeit, Referenden und Initiativen auf elektronischem Weg zu unterzeichnen, ist demgegenüber schon anspruchsvoller, weil hier die Authentizität der elektronischen Unterschriften und die Unterschriftsberechtigungen geprüft werden müssen.

Das dritte Teilgebiet – die Möglichkeit, elektronisch abzustimmen und zu wählen – ist mit Abstand das komplexeste und verdient etwas genauere Betrachtung. Hauptgrund für die Komplexität ist nicht die Anforderung, nebst dem elektronischen Weg auch weiterhin die traditionellen Wege Urne und Brief offenzuhalten. Der Kern der Komplexität ist angelegt im Spannungsverhältnis zwischen dem Anonymitätserfordernis betr. Stimmabgabe (Stimmgeheimnis) einerseits und dem Erfordernis nach einer gewissen Nachvollziehbarkeit andererseits. Beides sind Wesensmerkmale von Wahlen und Abstimmungen im traditionellen Sinn und wohl auch in der virtuellen Welt erforderliche Eigenschaften. Zur Illustration der Nachvollziehbarkeit folgender fiktive Fall im Jahre 2015: Im Anschluss an eine Abstimmung lässt eine politische Gruppierung verlauten, die Abstimmung sei elektronisch verfälscht worden oder sie habe diese gar selbst verfälscht. Was ist dann zu tun? Ohne Nachvollziehbarkeit kann nichts bewiesen oder widerlegt werden und die Abstimmung nochmals durchzuführen ist eine Lösung, die in den meisten Fällen von Anfang an ausser Betracht fällt. Man kann zwar behaupten, es werde der Tag kommen, an welchem eine Nachvollziehbarkeit nicht mehr erforderlich sein werde, weil allseits derart grosses Vertrauen in die Informatik gesetzt wird, dass niemand mehr die Möglichkeit von Fehlern oder Sicherheitslücken ernsthaft in Betracht zieht. Man mag dies auf die eine oder andere Weise sehen, wir weisen hier bloss darauf hin, dass auch renommierte Informatiksicherheitsexperten mittlerweile Projekte im Hinblick auf elektronische Abstimmungen als für die Demokratie zu gefährlich beurteilen. Es gibt zwar auf blinden Signaturen basierende Methoden, welche erlauben, den Gegensatz zwischen Anonymität und Nachvollziehbarkeit ein Stück weit zu überwinden. Die Komplexität lässt sich aber auch mit diesen nicht zum Verschwinden bringen und sie sind dementsprechend schwer zu implementieren. Aus diesem Grund ist zu bedauern, dass die Frage der Machbarkeit zwar im Titel des Berichts über den

Vote électronique erscheint, im Projekt selbst jedoch keine Checkpunkte betreffend diese Frage eingebaut sind.

Aus der Optik des Datenschutzes ist im Projekt in erster Linie von Bedeutung, was im Zusammenhang mit den Stimmrechtsregistern angestrebt wird. Schon aus Kostengründen sollte hier erst dann etwas im grossen Stile unternommen werden, wenn ein konkretes Modell vorliegt, für welches die Machbarkeitsfrage fürs effektive Abstimmen übers Netz schlüssig und positiv beantwortet wurde. Eine positive Antwort allein für den Anwendungsfall der Unterzeichnung von Referenden und Initiativen wäre kaum genügende Rechtfertigung für Investitionen in den Umbau von Stimmrechtsregistern, denn die elektronisch gesammelten Unterschriften lassen sich von ihrer Natur her nicht mit den auf herkömmliche Weise gesammelten vergleichen, weil sie sich schlicht leichter «eintreiben» lassen.

2. Datenschutzfragen allgemein

2.1. Bekanntgabe von Personendaten

2.1.1. Aufforderung zur Einreichung eines Softwareinventars

Um zu überprüfen, ob die nötigen Softwarelizenzen vorliegen, hat Microsoft Schweiz in einem Schreiben Firmen dazu aufgefordert, Angaben über die eingesetzten Softwareprodukte zu machen. Dass die Beantwortung einer solchen Befragung völlig freiwillig ist, war zuwenig klar ersichtlich. Microsoft hat sich aufgrund unserer Intervention bereit erklärt, die Adressaten in einem zweiten Schreiben deutlicher über die Freiwilligkeit der Beantwortung zu informieren.

Eine Anfragelawine hat ein Brief der Softwareherstellerin Microsoft bei uns ausgelöst. Im November 2001 schrieb Microsoft massenweise kleine und mittlere Unternehmen (KMUs) unter dem Titel «Illegale Software auch in Ihrem Unternehmen?» an. In diesem Schreiben bittet die Softwareproduzentin die KMUs um Mithilfe bei der Bekämpfung der illegalen Softwarenutzung. Dazu sollten detaillierte Angaben über die installierten Microsoftprodukte gemacht werden oder bestätigt werden, dass keine solche eingesetzt werden.

Viele Empfänger – darunter auch solche, die überhaupt keine Microsoft-Produkte einsetzen – waren verunsichert und fragten uns an, ob eine Verpflichtung bestehe, das Schreiben zu beantworten und insbesondere ein Softwareinventar zuhanden von Microsoft zu erstellen. Dies konnten wir verneinen.

Da aus der Formulierung des Schreibens zu wenig klar hervorgeht, dass die Beantwortung freiwillig ist, haben wir Microsoft gebeten, nochmals an die Empfänger des Briefes zu gelangen und ausdrücklich auf die Freiwilligkeit hinzuweisen. Dies hat uns Microsoft zugesichert.

Falls ein Softwarehersteller über Anhaltspunkte verfügt, dass eine Person gegen urheberrechtliche Bestimmungen im Zusammenhang mit Produkten, an denen er die Rechte hat, verstösst, kann er an die entsprechenden Behörden gelangen. Letztere werden sodann die nötigen Schritte unternehmen.

Im Übrigen haben wir die Personen, die sich in dieser Sache an uns wandten, darauf hingewiesen, dass sie das im Datenschutzgesetz verankerte Auskunftsrecht ausüben können, um herauszufinden, welche Daten bei Microsoft bearbeitet werden.

2.1.2. Herausgabe von Adressen von Aktionärinnen und Aktionären

Dem Verwaltungsrat einer Aktiengesellschaft werden die Personendaten von Aktionärinnen und Aktionären zur Erfüllung seiner Aufgaben zur Verfügung gestellt. Er trägt die Verantwortung für einen datenschutzkonformen Umgang mit diesen Daten.

Der Verwaltungsrat einer im Finanzbereich tätigen Aktiengesellschaft wandte sich an uns und wollte wissen, ob interessierten Aktieninhaberinnen oder -inhaber die im Aktienregister eingetragenen Adressen anderer Aktieninhaberinnen oder -inhaber herausgegeben werden dürfen. Die Statuten der Aktiengesellschaft sahen vor, dass der Verwaltungsrat diesen gestatten muss, das Aktienregister einzusehen und sich die Namen und Adressen eingetragener Personen zu kopieren, sofern nachgewiesen werden kann, dass die Daten benötigt werden, um die betroffenen Personen in einer Angelegenheit anzuschreiben, welche die Gesellschaft betrifft.

Ohne Bedeutung für die Beurteilung war dabei die Tatsache, dass diese Statutenbestimmung bereits vor dem Inkrafttreten des DSG formuliert worden ist; die Aktiengesellschaft als private Person muss die Bestimmungen des DSG anwenden.

Nach dem Datenschutzgesetz dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Mit dem Kauf von Namenaktien erklären sich die Erwerbenden auch bereit, den Inhalt der Statuten anzuerkennen (Ausnahme: Verstoss gegen zwingende Normen des Aktienrechts). Damit wird gleichzeitig auch die Einwilligung zur Datenbearbeitung im Sinne der erwähnten Statutenbestimmung abgegeben. Somit ist der Verwaltungsrat nicht nur berechtigt, sondern sogar verpflichtet, Aktienin-

haberinnen und -inhabern Einsicht ins Aktienregister zu gewähren, wenn diese den Nachweis erbringen können, dass sie die Daten benötigen, um diese in einer die Gesellschaft betreffenden Angelegenheit anzuschreiben.

Auch hinsichtlich der Form der Herausgabe von Adressen muss sich der Verwaltungsrat genau an die Statuten halten, die an besagter Stelle klar vorsehen, dass der «Verwaltungsrat [...] den Aktionärinnen und Aktionären zu gestatten [hat], das Aktienregister einzusehen und sich die Namen und Adressen eingetragener Personen zu kopieren [...]». Das schweizerische Aktienrecht hält zu diesem Punkt lediglich fest, dass die Gesellschaft verpflichtet ist, ein Aktienbuch zu führen. Es spricht sich aber nicht darüber aus, in welcher Form dies zu geschehen hat. Heute wird die Ansicht vertreten, dass diese Aktienbücher auch informatikgestützt geführt werden können. Wir haben dem Verwaltungsrat geraten, aufgrund des datenschutzrechtlichen Verhältnismässigkeitsprinzips den Interessierten nur ausgedruckte bzw. auf Papier kopierte Listen und keine elektronischen Datenträger auszuhändigen. Ausserdem haben wir dem Verwaltungsrat empfohlen, von Personen, die eine solche Adressliste ausgehändigt erhalten, eine Zusicherung zu verlangen, dass die Adressen nicht für andere Zwecke (beispielsweise für die Versendung von Werbung) verwendet werden. Mit der Vereinbarung einer Konventionalstrafe kann dies zusätzlich abgesichert werden.

2.1.3. Datenschutz in der Familienforschung

Das Betreiben von Familienforschung (Genealogie) erfordert die Einsichtnahme in zahlreiche private Papiere oder amtliche Dokumente bei den verschiedensten Behörden der Kantone und des Bundes. Für die Einsichtnahme und den Datenschutz gelten dabei unterschiedliche Regeln je nachdem, ob in öffentliche Register des Privatrechtsverkehrs (z.B. Zivilstandsregister) oder andere amtliche Dokumente Einblick gewünscht wird. Es muss dabei auch unterschieden werden, ob die Genealogin bei den direkt Betroffenen oder in amtlichen Dokumenten nachforscht.

Nachforschungen bei den direkt Betroffenen oder Dritten

Als Grundsatz gilt, dass Personendaten von noch lebenden Personen stets bei diesen in Erfahrung gebracht werden müssen. Erfolgt die Familienforschung bei den direkt Betroffenen oder Dritten (Verwandten oder Bekannten), so kommt das Datenschutzgesetz zur Anwendung. Es sieht vor, dass derjenige, der Personendaten bearbeitet, die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzen darf (Art. 12 Abs. 1 DSG). Es dürfen dabei insbesondere nicht ohne Rechtfertigungsgrund Daten einer Person gegen deren ausdrücklichen Willen bearbeitet werden (Art. 12 Abs. 2 lit. b DSG).

Als mögliche Rechtfertigungsgründe nennt Art. 13 Abs. 1 DSG die Einwilligung des Verletzten, ein überwiegendes privates oder öffentliches Interesse oder ein Gesetz.

Aus dem Gesagten ergibt sich, dass bei der Familienforschung für jede Form des Bearbeitens (z.B. Beschaffen, Aufbewahren, Publizieren) von Personendaten immer die ausdrückliche Einwilligung bei noch lebenden Personen eingeholt werden muss. Zudem gilt zu beachten, dass beispielweise bei der Publikation von Personendaten von Verstorbenen die Persönlichkeitsrechte der Nachkommen verletzt werden können; diese müssen somit grundsätzlich ihre Einwilligung zur Bekanntgabe geben.

Nachforschungen in Zivilstandsregistern oder anderen öffentlichen Registern des Privatrechtsverkehrs

Das Datenschutzgesetz findet keine Anwendung auf öffentliche Register des Privatrechtsverkehrs (Art. 2 Abs. 2 lit. d DSG). Dazu gehören auch die Zivilstandsregister, die bei genealogischen Nachforschungen vor allem Verwendung finden. Dies bedeutet aber nicht, dass bei Nachforschungen in den Zivilstandsregistern den Interessen des Datenschutzes keine Beachtung geschenkt werden muss. Die Einsichtnahme in diese Register ist in der Zivilstandsverordnung (ZStV) geregelt. Sie hält fest, dass für Privatpersonen grundsätzlich kein Anspruch auf Einsicht in die Zivilstandsregister besteht. Nur wenn die Beschaffung der Daten bei den direkt betroffenen Personen nicht möglich oder offensichtlich nicht zumutbar ist, kann die kantonale Aufsichtsbehörde die Bekanntgabe von Personendaten zum Zweck personenbezogener Forschung bewilligen (Art. 29a Abs. 2 ZStV). Diese Bewilligung wird stets mit Auflagen zur Sicherung des Datenschutzes verbunden. Es empfiehlt sich somit, ein schriftliches, begründetes Gesuch an die Aufsichtsbehörde des Kantons einzureichen, in dem die Nachforschungen angestellt werden.

Sollen die so erforschten Daten in der Folge in eine Familienchronik integriert und damit Dritten bekannt gemacht werden, so muss auch hier – nun wieder als Anwendungsfall des Datenschutzgesetzes – die Einwilligung bei den betroffenen Personen eingeholt werden. Wird die Einwilligung verweigert, so müssen die Daten umgehend vernichtet werden.

Zum Thema Nachforschungen in anderen amtlichen Dokumenten sowie Auskunftserteilung durch Bundesorgane verweisen wir Sie auf dem 2. Tätigkeitsbericht 1994/95, S.80.

2.2. Datenschutz und Datensicherheit

2.2.1. Alle Stufen zwischen Bekanntgabe der persönlichen Identität und Anonymität

Seit jeher konnte der Mensch entscheiden, ob er im Kontakt mit seinen Mitmenschen seine Identität offen legt, sie mehr oder weniger verbirgt oder gänzlich verschweigt. Je nach Art der Beziehung kann das Gegenüber diese Entscheidung akzeptieren, mehr Informationen über die Identität verlangen, oder falls die betroffene Person dies ablehnt, gänzlich auf Kontakt mit ihr verzichten. Im Zeitalter der interpersonellen Kommunikation, der Massenmedien, des elektronischen Geschäftsverkehrs und zahlreicher anderer im Internet angebotener Dienste gewinnt diese Praxis eine besonders grosse Bedeutung. Eine klare Definition der verschiedenen Typen und Einsatzmöglichkeiten von Anonymität und Pseudonymität, zwischen denen man als Individuum wählen kann, ist daher notwendig.

Die Identität wird definiert durch «die Gesamtheit der tatsächlichen und rechtlichen Daten (Geburtsdatum, Geburtsort, Name, Vorname, Namen der Eltern, usw.), die es erlauben, jemanden als Individuum zu erkennen». Die notwendigen Angaben hängen logischerweise mit dem Kontext zusammen, innerhalb dessen die Identifizierung stattfinden soll. Im engen Kreis (Klasse, Freunde, Arbeitskollegen) reicht in der Regel ein Identitätselement wie der Vorname, um jede Person zu identifizieren. Im breiteren Kreis (Schule, Unternehmen) müssen zuweilen mehrere Elemente wie Vorname, Name und manchmal Geburtsdatum zusammengenommen werden, um den einzelnen identifizieren zu können. So definiert, liefert die Identität aber keine Merkmale zur äusseren Erkennung eines Individuums, weshalb offizielle Ausweisdokumente darüber hinaus anthropometrische Angaben enthalten, wie Körpergrösse, Augenfarbe und ein Passbild.

Die *Anonymisierung* besteht darin, Personendaten so zu ändern, dass Informationen über die persönliche oder materielle Situation nicht mehr (oder nur noch mit ausserordentlichem Aufwand) mit einer bestimmten oder bestimmbaren natürlichen Person in Verbindung gebracht werden können. Gemäss dieser Definition müssen somit sämtliche Identitätsdaten einer Person entfernt werden, da in einem engeren Kontext ein einziges Merkmal zur Identifikation der Person ausreicht. Allerdings hängt dies auch von der Unterscheidungskraft des jeweiligen Merkmals ab, so ist die Angabe des Geschlechts relativ harmlos, während das Geburtsdatum hinsichtlich des Geburtsjahrs oder des Alters der Person anonymisiert werden muss. Grundsätzlich ist es riskant,

auch nur das geringste Identitätsmerkmal in der Annahme zu behalten, dass die Anonymisierung in einem ausreichend grossen Rahmen stattfindet, denn dieser kann sich im Laufe der Zeit verändern (z.B. verkleinern). Bleibt noch das «Scheinproblem» einer so spezifischen unpersönlichen Information, die es einem gut informierten Dritten erlauben würde, eine Person zu identifizieren, die er bereits sehr genau kennt.

Diese Form der *unverkettbaren Anonymität* lässt keinerlei Rückschlüsse oder Zusammenführung von Daten zu, die von derselben natürlichen Person stammen. Barzahlungen, selbst an einen einzigen Gläubiger, gehören zu dieser Form von Anonymität. Es gibt aber auch eine *«verkettbare» Anonymität*, die darin besteht, dass durch einen in jedem Eintrag enthaltenen anonymen Identifikator Ereignisse miteinander verbunden werden können, die aus derselben Quelle, also möglicherweise von derselben Person stammen. Prepaid-Karten für die Telefonie (und manche Chipkarten) sind ein ausgezeichnetes Beispiel für diese Form der Anonymität.

Keine der genannten Arten der Anonymität erfordern besondere Datenschutzmassnahmen, da es sich nicht um Personendaten oder personenbezogene Daten handelt. Auch ist der Begriff der «Deanonymisierung» ungenau, da eine Re-identifikation der betroffenen Person technisch nur im Falle einer ungenauen oder fehlerhaften Anonymisierung möglich ist.

Bei der *Pseudonymisierung* werden Personendaten durch eine sogenannte *Korrespondenzregel* verwandelt, so dass es nicht mehr möglich ist, den Bezug zwischen den Informationen über eine persönliche oder materielle Situation und der betroffenen natürlichen Person herzustellen, ohne die Regel zu kennen, bzw. anzuwenden. Die *Identitätsdaten werden durch eine Bezeichnung,* dem sogenannten *Pseudonym*, ersetzt, das durch die Korrespondenzregel erzeugt wurde. Ziel des Unterfangens ist es, den eindeutigen Bezug zur Identität einer Person nur falls unbedingt notwendig und unter Einhaltung der im Voraus festgelegten Bedingungen wiederherstellen zu können («Depseudonymisierung»). Das Pseudonym bietet somit eine *relative Anonymität* gegenüber all jenen, die es nicht «depseudonymisieren» können. Es kann aber auch – beispielsweise wenn es um die Haftung der betroffenen Person geht – aufgehoben werden. Von der Verwendung desselben Pseudonyms für mehrere Anwendungen ist abzuraten, da sich durch das Zusammenführen von pseudonymisierten Daten aus verschiedenen Quellen ein individuelles Persönlichkeitsprofil herstellen lassen kann, dessen Häufung von typischen Merkmalen allzu leicht zu einer missbräuchlichen Re-identifikation führen könnte.

Die *mathematische Pseudonymisierung* erfolgt durch eine *Einwegfunktion*, die von persönlichen Identitätsdaten ausgehend ein Pseudonym erzeugt. Die Funktion beruht auf einem asymmetrischen Verschlüsselungsverfahren, mit dem der Rückschluss auf

alle oder einen Teil der Identitätsdaten anhand des Pseudonyms vollkommen unmöglich ist. Eine weitere - mitnichten triviale - Eigenschaft der Funktion muss darin bestehen, dass die zufällige Erzeugung desselben Pseudonyms ausgehend von anderen Identitätsdaten praktisch ausgeschlossen werden kann. Möglich ist eine «Depseudonymisierung» theoretisch durch den Vergleich des fraglichen Pseudonyms mit allen Pseudonymen, die anhand der Identitätsdaten aller Personen in einer Gruppe erzeugt wurden, in der sich die gesuchte Person befindet (dictionary attack, Wörterbuchangriff). Da dies in der Praxis nicht unbedingt durchführbar ist, wird von einigen der gewagte Begriff des «anonymen Pseudonyms» verwendet, welcher der «verkettbaren» Anonymität scheinbar sehr nahe kommt. Einweg-Pseudonyme eignen sich somit gut für statistische Längsschnittuntersuchungen, bei denen im Nachhinein gesammelte Personendaten mit bestehenden Daten zusammengeführt werden, ohne dass ein Bezug zu den Personen notwendig ist.

Die *exogene Pseudonymisierung* besteht in der Schaffung eines *Referenzpseudonyms*, das so unabhängig wie möglich von der dazugehörigen Identität gewählt wird und nur in einer *Referenzliste* zusammen auftritt. Da die Liste die einzige Möglichkeit der Reidentifikation darstellt, hängt die Solidität des Pseudonyms ausschliesslich von der Zugänglichkeit der Liste ab. Sie kann beispielsweise bei einer oder mehreren Vertrauensinstanzen hinterlegt werden, die darüber hinaus die Schlüssel zur Depseudonymisierung unter sich verteilen können. Beim heutigen Stand der Technik sollten für die Referenzliste einer als robust geltenden Pseudonymisierung folgende Mindestanforderungen gelten:

- nur akkreditierte und formell authentifizierte Personen sind für die Verwaltung zuständig,
- die Liste wird nur in elektronischer verschlüsselter Form gespeichert,
- die Reidentifikation kann nur selektiv für ein gegebenes Pseudonym stattfinden (statt das Pseudonym zu speichern, ist es ebenfalls denkbar, dass es lediglich in seiner Funktion als symmetrischer Schlüssel zur Ver- und Entschlüsselung Zugang zur entsprechenden Identität gibt),
- über die Reidentifikation und deren Zweck ist ausführlich Protokoll zu führen.

Wenn die Referenzliste *halb-öffentlich zugänglich* ist, also beispielsweise von einer die Vertraulichkeit der Daten garantierenden Instanz verwaltet wird (z.B. Kreditkarten-Nummern), hängt die Sicherheit ausschliesslich davon ab, wie gewissenhaft diese Daten von Angestellten, Gläubigern und der betroffenen Person behandelt werden. Es muss allerdings eingeräumt werden, dass organisatorische Massnahmen in der Regel weniger effizient sind als technische Massnahmen (siehe die weiter oben aufgeführten Anforderungen).

Bei *öffentlich zugänglichen* Referenzlisten hingegen (z.B. «Liste blanche», d.h. Standardeintrag, und «Liste verte», d.h. beschränkt auf das elektronische Telefonverzeichnis ETV, im Telefonbuch) ist das Pseudonym so schwach, dass eher von *indirekter Identifikation* der Personen gesprochen werden sollte.

Das *endogene Pseudonym* ist ein *Deckname («Nom de Plume»)*, der von der betroffenen Person erfunden und dessen Bezug zur tatsächlichen Identität von ihr kontrolliert wird. Die einzige sinnvolle Vorsichtsmassnahme besteht darin, sich zu vergewissern, dass das gewählte Pseudonym nicht bereits von jemand anderem verwendet wird (Einmaligkeitsüberprüfung). Diese Art von Pseudonym eignet sich unter anderem besonders für wissenschaftliche Untersuchungen, die generische Informationen über ganz bestimmte Personengruppen liefern und gleichzeitig den Betroffenen die Möglichkeit geben sollen, sich inkognito nach ihrem eigenen Ergebnis zu erkundigen.

Abschliessend ist festzustellen, dass es zwischen Anonymität und Identität zahlreiche subtile Abstufungen gibt. Davon ist jede für eine bestimmte Art von Beziehung besonders gut geeignet, so dass dieselbe Person durchaus alle verschiedenen Formen abwechslungsweise einsetzen kann. Für den Internet-Benutzer gestaltet sich die entsprechende Verwaltung der Identitäten zweifellos extrem aufwendig und schwierig, so dass er früher oder später die Hilfe eines Identitätsmanagers (*Identity Protector)* benötigen wird.

2.2.2. Der elektronische Arbeitsplatz

Zur Büroausstattung, die der Arbeitgeber bzw. die Arbeitgeberin den Angestellten zur Verfügung stellt, gehört immer öfter auch ein elektronischer Office-Manager, der unter anderem aus E-Mail-Programm und elektronischem Terminplaner besteht. Angesichts der zahlreichen datenschutzrechtlichen Fragen im Zusammenhang mit der elektronischen Post wird diese in einem getrennten Kapitel behandelt. Während der elektronische Terminplaner gewöhnlich Funktionen wie Kalender, Adressbuch, Aufgabenplaner und Notizblock umfasst, bietet der elektronische Arbeitsplatz darüber hinaus die Möglichkeit der Protokollführung über Aufgaben, der automatischen Archivierung von veralteten Daten, des Datenaustauschs mit Kollegen sowie der Synchronisierung der Daten mit mobilen Geräten oder gar mit Internet-Servern.

Der elektronische Arbeitsplatz wird im allgemeinen Sprachgebrauch auch Personal Information Manager (PIM) genannt, obwohl er in der Praxis fast zwangsläufig eine Mischung aus persönlichen und beruflichen Daten enthält. Die Bezeichnung zeigt, wie sehr sich im persönlichen Arbeitsumfeld von Angestellten der berufliche Bereich - der dem Arbeitgeber «gehört» – mit der Privatsphäre überschneidet, die auch nach dem

Betreten der Büroräume weiter besteht und geschützt bleiben muss. Wenn die berufliche Tätigkeit eine gewisse Mobilität verlangt, der Arbeitsplatz jedoch nicht transportierbar ist, stellt der Arbeitgeber seinen Angestellten zuweilen noch einen mit dem elektronischen Arbeitsplatz synchronisierbaren Pocket-PC und ein Mobiltelefon zur Verfügung. Die dadurch entstehende Streuung von Daten geschieht nicht, ohne dass sich sowohl für den Arbeitgeber als auch für die Angestellten gewisse Sicherheits- und Schutzprobleme stellen. In jedem Fall muss der Arbeitgeber festlegen, unter welchen Bedingungen die Systemadministration auf die Dateien im elektronischen Arbeitsplatz der Angestellten zugreifen darf, ganz gleich ob diese auf einem Unternehmensserver, dem Arbeitsplatz, dem Pocket-PC oder einem anderen Datenträger gespeichert sind.

Mit Hilfe des *Protokollführers* lassen sich automatisch *chronologische Platzhalter* erzeugen, die auf Nachrichten, Sitzungen und Aufgaben in Verbindung mit einzelnen Kontakten oder auf bestimmte Arten von Dokumenten verweisen (Texte, Tabellen, Präsentationen oder Datenbanken). Darüber hinaus lassen sich die Einträge manuell durch Eingaben ergänzen, über die ebenfalls Protokoll geführt werden soll (z.B. Telefonanrufe). Die Platzhalter zeugen somit selbst nach der Löschung der ursprünglichen Dokumente noch von Tätigkeiten, die zu einem bestimmten Zeitpunkt ausgeführt wurden! Ob der Protokollführer aktiviert wird oder nicht, sollte daher reiflich überlegt werden, insbesondere wenn dieser statische Platzhalter erzeugt, deren Verbindung zu den ursprünglichen Objekten nach ihrer Verschiebung zu Archivierungszwecken verloren geht. Die Liste der mit allen Kontakten im Adressbuch ausgetauschten E-Mails kann im Grunde auch unabhängig vom Protokollführer aufgestellt werden (Registerkarte «History/Verlauf» für den jeweiligen «Kontakt»). Eine solche Liste ist vergleichsweise harmlos, da sie nur die Nachrichten anzeigt, in noch in den Ordnern (einschliesslich dem Ordner für gelöschte Objekte!) des elektronischen Arbeitsplatzes vorhanden sind.

Die *automatische Archivierung* von veralteten Objekten kann selektiv für die verschiedenen Ordnertypen des elektronischen Arbeitsplatzes eingestellt werden und bietet die Wahl zwischen der Archivierung in einem persönlichen Ordner und der endgültigen Löschung. Die Archivierung hat den Vorteil, den elektronischen Arbeitsplatz von alten Objekten zu entlasten und zugleich, falls notwendig, auf die archivierten Objekte zugreifen zu können. Damit kann natürlich eine gewisse Gefahr hinsichtlich der Verfolgbarkeit von verschwundenen Informationen entstehen.

Muss ein Angestellter bestimmten Kollegen den Zugriff auf berufliche Objekte gewähren, so muss er auch die Möglichkeit haben, *seine privaten Objekte deutlich zu kennzeichnen*, damit wenigstens ihr Inhalt nicht angezeigt (verdeckte Anzeige), besser aber keine Spur ihrer Existenz zu finden ist. Ein regelmässiger Termin am selben Wochenabend kann zu unterschiedlichsten Interpretationen führen!

Aufgrund der in verschiedenen Berufen verlangten Mobilität, der Möglichkeit, mehrere Teilzeitbeschäftigungen zu kumulieren und der zunehmenden Verbreitung von Telearbeit muss der elektronische Arbeitsplatz den Angestellten in fast allen Situationen zur Verfügung stehen. Technisch gibt es dazu im Grunde nur drei Lösungsansätze:

- *Den Zugang zum elektronischen Arbeitsplatz im Unternehmen von einem externen Netz aus zu gewähren*, wobei die mit der Authentifizierung der Angestellten und dem Austausch vertraulicher Daten einhergehenden Gefahren nur durch eine Public Key Infrastructure zu bewältigen sind. Der Zugang erfolgt ent weder über eine WAP-Schnittstelle (Wireless Application Protocol) für Mobiltelefone oder über eine RAS-Schnittstelle (Remote Access Service) für tragbare Computer, die an das Festnetz (per Modem oder ISDN-Karte: Integrated Services Digital Network) oder direkt an das Mobilfunknetz (per HSCSD-Protokoll: High Speed Circuit Switched Data oder GPRS: General Purpose Radio Service) angeschlossen sind. Um die Kommunikationssicherheit zu verbessern, kann ausserdem die Technologie der privaten virtuellen Netze (VPN: Virtual Private Network) eingesetzt werden.

- *Den elektronischen Arbeitsplatz mit persönlichen mobilen Endgeräten zu synchronisieren,* wobei den Gefahren im Hinblick auf die Vertraulichkeit von Daten in der Regel durch Passwörter oder wirksamer noch durch Datenverschlüsselung entgegengewirkt werden kann. Unter persönlichen mobilen Endgeräten versteht man tragbare Computer (im autonomen Modus), Pocket-PCs/Organizer und Mobiltelefone. Gegenwärtig verfügen nur die tragbaren Computer über Betriebssysteme, die leistungsfähig genug sind, um Dateiensysteme mit hoher Verschlüsselungsrate zu unterstützen. Mehr oder weniger robuste Software-Erweiterungen zur Verschlüsselung gibt es auch für Pocket-PCs (Palmtops und HPC: Handheld Personal Computers), die in der Regel leistungsfähiger sind als Personal Digital Assistants (PDA), auch elektronische Terminplaner oder Organizer genannt. Auf dem Markt sind ausserdem bereits Geräte in Westentaschengrösse erhältlich, die persönliche Terminplanung und Mobiltelefonie integrieren.

- *Den elektronischen Arbeitsplatz mit einer auf Synchronisierungsdienste spezialisierten Website abgleichen,* wobei der gewählte Dienstanbieter für den Schutz der Vertraulichkeit und für die Verfügbarkeit der Daten verantwortlich ist. Manche Dienstanbieter stellen gratis die Synchronisierung der Daten von Terminplaner, Adressbuch und Aufgaben im elektronischen Arbeitsplatz zur Verfügung; und sie ergänzen dies durch die integrierte Verwaltung von E-Mail, SMS, Fax, Voice-Mail und freigegebenen Dateien, die zuweilen sogar durch ein WAP-fähiges Mobiltelefon abgerufen werden können.

2.2.3. Sinnvolle Benutzung des E-Mail-Programms

Zur Büroausstattung, die der Arbeitgeber bzw. die Arbeitgeberin den Angestellten zur Verfügung stellt, gehört in der Regel auch ein E-Mail-Programm, das manchmal in den Office-Manager integriert ist. E-Mails dienen zum Austausch von beruflichen oder manchmal auch privaten Informationen innerhalb des Unternehmens oder mit externen Kontakten. Dem Schutz der elektronischen Kommunikation ist daher besondere Aufmerksamkeit zu schenken, namentlich durch die Verwendung von Funktionen des E-Mail-Programms, die häufig nicht ausreichend bekannt sind und daher kaum eingesetzt werden.

Es genügt beispielsweise, statt des Feldes «An» das *Feld «BCC»* (Blind Carbon Copy) zu verwenden, damit die zahlreichen Empfänger derselben Nachricht den Eindruck haben, einzeln angeschrieben worden zu sein, d.h. die Adresse der übrigen Angeschriebenen nicht angezeigt wird. Diese Funktion eignet sich besonders für unpersönliche Nachrichten (Werbung, Ankündigungen,…) an eine Gruppe von nicht miteinander bekannten Personen, widerspricht aber dem Grundsatz der Transparenz, wenn sie dazu verwendet wird, eine «blinde» Kopie an andere Adressaten («BCC») als die primären oder sekundären Empfänger («An» bzw. «CC») zu senden.

Das Anfordern einer *Empfangsbestätigung* und vor allem einer *Lesebestätigung* garantiert dem Absender, dass der Empfänger den Erhalt einer übermittelten und geöffneten (also wahrscheinlich gelesenen) Nachricht nicht abstreiten kann.

Mit der Option «*Später senden*» kann eine Sperrfrist über eine Nachricht verhängt werden, während mit der Option «*Verfallsdatum*» eine veraltete, d.h. nicht mehr aktuelle und daher nicht mehr lesenswerte Nachricht automatisch vernichtet wird.

Mit der Funktion «*Rückgängig*» kann die versehentliche Versendung einer Nachricht rückgängig gemacht werden, vorausgesetzt sie wird ausgeführt, bevor der Empfänger die Nachricht erhält.

Die *Einstellungen für das Senden* erlauben es ausserdem, für jede gesendete Nachricht die Vertraulichkeitsstufe zu bestimmen (Standard, Persönlich, Privat, Vertraulich). Nachrichten mit dem Vermerk «Privat» bleiben somit für eventuel le Delegierte (siehe weiter unten) mit Zugriffsberechtigung auf Ihren Posteingang unsichtbar. Nachrichten mit dem Vermerk «Vertraulich» sollten nur verschickt werden können, wenn die Absicht, die Information an andere Empfänger weiterzuleiten, ausdrücklich bestätigt wird!

Für Vertraulichkeit ist die *Verschlüsselung des Inhalts und der Anlagen* (asymmetrische Verschlüsselung in einer Public Key Infrastructure) die unumstritten sicherste Lösung. Die Verschlüsselung gewährleistet ausserdem die Integrität der empfangenen Daten, da die geringste (absichtliche oder versehentliche) Veränderung der verschlüsselten Nachricht ihre Entschlüsselung unmöglich macht. Wird die *ausgehende Nachricht ausserdem mit einer digitalen Signatur* versehen, kann der Empfänger die Authentizität des Absenders überprüfen.

Darüber hinaus kann über benutzerdefinierte *Einstellungen* festgelegt werden, dass Nachrichten auf der Grundlage bestimmter Kriterien bezüglich ihres Inhalts und/oder ihrer Randdaten beispielsweise automatisch geprüft, bestimmten Kategorien (z.B. Privat) zugewiesen werden, verschoben, gelöscht, kopiert oder weitergeleitet werden. Auch kann eine Liste blockierter Absender aufgestellt werden, von denen *Nachrichten unerwünscht* (*Junk-Mail, Spam, usw.*) sind.

Für den Fall der *Abwesenheit vom Büro* gibt es die Möglichkeit, eine *automatische Abwesenheitsnachricht* zu erstellen, um den Absender über die Dauer der Abwesenheit (den Grund anzugeben, ist in der Regel überflüssig!) und die Adresse der im Notfall zu kontaktierenden Person zu informieren. Für denselben Fall kann auch die *automatische Weiterleitung der eingehenden Nachrichten* an eine bestimmte externe Adresse gewählt werden. Dabei ist jedoch grösste Vorsicht geboten, insbesondere wenn vertrauliche, für Arbeitgeber wie Angestellte potenziell sensible Nachrichten an eine per Internet zugängliche und daher weniger sicherere Mailbox weitergeleitet werden.

Zu erwähnen bleibt noch die wichtige Frage des *Speicherns der ausgetauschten Nachrichten*. Zwar werden in der Praxis meist zu viele Nachrichten aufbewahrt und demzufolge der Speicherplatz überfüllt, doch kommt es auch vor, dass wichtige Nachrichten überstürzt gelöscht werden oder kaum wieder auf zufinden sind. Die Lösung liegt in der Verwendung einer *nicht nominalen Dienst-Mailbox* (z.B.: info@firma.ch) und strenger Vorschriften für die *Speicherung von Nachrichten im Geschäftsführungssystem* des Unternehmens.

Im Rahmen der *E-Mail-Programme* sind die Nachrichten Gegenstand einer automatischen Vorbearbeitung auf der Grundlage der vom Arbeitgeber für Validierung, Kategorisierung, Priorisierung, Weiterleitung, Speicherung und Archivierung festgelegten Unternehmensregeln (Business Rules). Dabei erhalten die Mitarbeiter häufig nur eine Berechtigungsmarke für den Zugriff auf die in einer Datenbank gespeicherte Nachricht. Der Schutz der Privatsphäre setzt daher voraus, dass Verfolgungsaktionen und deren Zweck vollkommen transparent sind, ferner den Benutzern eine Funktion zur physischen Löschung privater Nachrichten zur Verfügung gestellt wird und sie vor der

endgültigen Löschung privater Objekte benachrichtigt werden, um sie gegebenenfalls sichern zu können.

Beim *Löschen von Nachrichten* rührt die grösste Gefahr daher, dass Nachrichten standardmässig *logisch gelöscht*, d.h. lediglich in einen Ordner mit gelöschten Dateien verschoben werden, wo sie aber lesbar bleiben, solange keine physische und endgültige Löschung (manuell oder durch automatisches Leeren beim Verlassen) stattgefunden hat. Ein gut informierter Benutzer sollte die Funktion zur endgültigen Löschung bestimmter Nachrichten kennen. Es bleibt allerdings ein weiteres Risiko, da sich aufgrund der automatischen Speicherung von E-Mail-Daten *eine gelöschte Nachricht nach wie vor auf einem Datenträger befinden kann*, der in der Zeit zwischen dem Abrufen der Nachricht und ihrer physischen Löschung beschrieben wurde.

Schliesslich kann ein Arbeitnehmer *Delegierte* bestimmen, die auf bestimmte Ordner seines elektronischen Arbeitsplatzes zugreifen dürfen (Lesen, Erstellen, Ändern und/oder Löschen). Im Posteingang kann festgelegt werden, ob ein Delegierter falls notwendig im Namen des Inhabers eine Nachricht senden oder beantworten soll, ob er eine Kopie der Nachrichten über Sitzungstermine erhalten soll und ob er die privaten Objekte (neue Nachrichten sowie Termine, Kontakte und gegebenenfalls Aufgaben) sehen darf. Am besten sind private Nachrichten natürlich geschützt, wenn sie in einem *persönlichen Ordner* auf bewahrt werden, der durch ein Passwort geschützt ist und sich in verschlüsselter Form in einer nicht freigegebenen aber dennoch regelmässig gesicherten Einheit befindet.

Abschliessend ist zu diesem Thema noch zu erwähnen, dass Internet-Mail (externe Mailboxes, die über POP3- oder IMAP4-Protokolle zugänglich sind) vom Arbeitgeber meistens aus offenkundigen Sicherheitsgründen deaktiviert ist. Die ausschliesslich internetbasierten Mail-Systeme, von denen einige die Verschlüsselung und digitale Signatur von E-Mail unterstützen, können jedoch für Angestellte beruflich oder privat durchaus von Interesse sein.

2.2.4. Sicherheitsprobleme in drahtlosen lokalen und persönlichen Netzwerken

Wie bei jeder neuen Technologie bringt auch der Einzug der drahtlosen (wireless) lokalen und persönlichen Netzwerke eine ganze Reihe von datenschutzrechtlichen Problemen mit sich. Die «drahtlose» Kommunikation bietet diverse Vorteile, wie geringere Kabelinfrastruktur und grössere Mobilität der Benutzer, denen jedoch eine verstärkte Abhörgefahr der Kommunikation (über Funkfrequenzen) gegenüber steht. In den Normen für drahtlose Netze muss das Übertragungsprotokoll daher immer die Datenchiffrierung vorsehen, die jedoch nur durch eine Public Key Infrastructure mit dem dazugehörenden technischen und organisatorischen Aufwand verwirklicht werden kann.

Für lokale Netzwerke (LAN: Local Area Networks) kam zu dem marktüblichen Ethernet-Standard IEEE 802.3 (drahtgebunden) der Standard 802.11 (drahtlos) und dessen Verschlüsselungsprotokoll WEP (Wired Equivalent Privacy) hinzu. Die Erfahrung hat aber gezeigt, dass das WEP nicht immer implementiert wird und selbst dann gewisse Lücken oder Schwierigkeiten bestehen bleiben, wenn er aktiviert ist (statische Chiffrier-Schlüssel müssen für jedes Endgerät definiert werden). Darüber hinaus teilen die drahtlosen Access Points (Zugangspunkte) beim Standard 802.11 im Umkreis von mehreren hundert Metern für alle mobilen Endgeräte dieselbe verfügbare Bandbreite (mit einer Datenrate von bis zu 11 MBit/s bei 802.11b und 54 MBit/s bei 802.11a). Bei 802.3-Switches hingegen wird die Bandbreite (10 oder 100 MBit/s) für jedes festverkabelte Gerät individualisiert und somit die Gefahr eines gross angelegten «Lauschangriffs» deutlich verringert. Der Verbindungsaufbau mit einem aktiven Access Point kann nur geschehen, wenn das drahtlose mobile Endgerät bei der Anmeldung den Netzwerknamen (SSID: Service Set IDentifier) kennt und überträgt und vor allem das Authentifizierungsverfahren der geteilten Schlüssel verwendet (WEP-Protokoll mit einem 104-Bit-Schlüssel ergänzt durch einen Initialisierungsvektor von 24 Bit). Eine Schwäche des von diesem Protokoll verwendeten RC4-Algorithmus besteht in der hohen Wahrscheinlichkeit, denselben Vektor wieder zu erzeugen. Daran zeigt sich, wie komplex die Umsetzung von kryptographischen Lösungen nach wie vor bleibt.

Für persönliche Netzwerke (PAN: Personal Area Networks), welche die drahtlose Verbindung zwischen tragbarem Computer, Personal Digital Assistant, Mobiltelefon und anderen persönlichen Geräten herstellen, gilt der auf der Bluetooth-Spezifikation beruhende IEEE-Standard 802.15 mit einem Datendurchsatz von 732 KBit/s im Umkreis von ca. 10 Metern. Glücklicherweise sind in dieser Norm auch Authentifizierungs- und Datenverschlüsselungsverfahren vorgesehen, für die wiederum Schlüssel verwaltet wer-

den müssen. Ausrüstungen ohne Eingabetastatur scheinen somit dazu verurteilt, einen Standardschlüssel verwenden zu müssen, was sie für Lauschangriffe oder gar unkontrollierte Datenweiterleitung anfällig macht. In jedem Falle hat die Erfahrung gezeigt, dass während der Einführungsphase einer solchen Technologie Vorsicht geboten ist.

Im einem noch lokaleren Umfeld werden Tastatur und Maus immer häufiger drahtlos mit dem Arbeitsplatz verbunden. Ergonomisch und praktisch bietet diese Entwicklung unbestreitbare Vorteile, doch darf nicht vergessen werden, dass die Eingabe von Passwörtern für den Zugriff auf besonders schützenswerte Informationen häufig über die Tastatur erfolgt und die drahtlose Übertragung dieser Daten offensichtlich nicht allzu schwer abzufangen und zu entziffern ist.

2.2.5. Biometrische Identifizierung und die damit verbundenen Risiken

Biometrische Methoden erlauben es, eine Person anhand bestimmter Körpermerkmale eindeutig zu identifizieren. Viele Körperteile sind einzigartig und verändern sich im Verlauf des Lebens nicht. Der Vorteil liegt darin, dass man Körpermerkmale (im Gegensatz zu Passwörtern) weder verlieren noch an andere weitergeben kann. Aus diesem Grund gilt die biometrische Identifizierung als besonders sicher. Allerdings sind neben den Vorteilen für Sicherheit und Datenschutz auch erhebliche Risiken damit verbunden.

Seit den Ereignissen vom 11. September 2001 ist die Technik der biometrischen Identifizierung im Aufwind. Hersteller preisen sie als das effizienteste Mittel für die Bekämpfung von Terrorismus an, da biometrische Merkmale extrem schwierig zu fälschen sind. Dies wird aber wenig nutzen, wenn das Betriebssystem unsicher ist, und Unberechtigte biometrische Daten entwenden können. Forschungsstudien haben gezeigt, dass einige kommerzielle Biometriesysteme verwundbar sind. Deshalb können solche Systeme nur dann sinnvoll eingesetzt werden, wenn die biometrischen Merkmale in einem absolut sicheren Umfeld aufbewahrt werden. Dabei ist ausschlaggebend, dass das Überprüfungssystem nicht nur die Daten mit den abgespeicherten Mustern vergleichen, sondern auch kontrollieren kann, ob die Daten von derselben Person zum Zeitpunkt der Überprüfung stammen. Wenn ein System diese zwei Kontrollen nicht bewältigen kann, so besteht ein Sicherheitsrisiko. Ein Grund für die noch bestehenden Risiken im Bereich der biometrischen Systeme liegt darin, dass die Biometrie eine noch junge Technik ist und in der Praxis bislang noch keine grossen Bewährungsproben zu bestehen hatte.

Allerdings ist die Lösung der Sicherheitsfrage von entscheidender Bedeutung, da sich die grosse Stärke biometrischer Methoden – die Unveränderbarkeit der Merkmale – als gravierende Schwäche erweisen kann. Denn wenn biometrische Daten gestohlen oder verloren gehen, können sie nicht wie ein Passwort oder ein Zertifikat ersetzt werden. Bei Verlust ist die biometrische Identifikation für immer kompromittiert und lässt sich nicht mehr gebrauchen. Deshalb besteht eines der zentralen Probleme biometrischer Systeme darin, ein Merkmal zu widerrufen, damit es nicht missbraucht wird. Das Ausweichen auf ein nicht kompromittiertes Merkmal ist nur eine scheinbare Lösung, denn wenn beispielsweise die Identifikation mit einem Finger erfolgt, stehen die übrigen Finger als Alternative zur Verfügung. Deren Anzahl ist aber begrenzt.

Damit Biometriedaten für hohe Sicherheit und effizienten Datenschutz eingesetzt werden können, müssen die bestehenden Sicherheitsrisiken biometrischer Betriebssysteme ausgeschaltet werden. Denn gestohlene Biometriedaten sind unersetzbar.

2.2.6. Grundsätzliche Anforderungen für den Schutz der Privatsphäre bei Chipkarten

Chipkarten nehmen bereits einen festen Platz im Alltag ein. Damit bei ihrem Einsatz die Privatsphäre geschützt bleibt, gilt es einigen grundsätzlichen Anforderungen zu genügen.

Obwohl die Chipkarten an Benutzerinnen und Benutzer abgegeben werden, bleiben sie Teil eines Datenbearbeitungssystems der herausgebenden Stellen. Deshalb müssen diese auch dafür sorgen, dass die technischen und organisatorischen Massnahmen getroffen werden, um beispielsweise den Zugriff von Unberechtigten zu verhindern. Besonders wichtig ist dieser Zugriffsschutz bei multifunktionalen Karten, die von mehreren Unternehmen gemeinsam genutzt werden. In diesen Fällen muss sichergestellt sein, dass jede dieser Stellen nur auf die für sie bestimmten Daten zugreifen kann.

Da der Einsatz von Chipkarten bestimmte Risiken für die Privatsphäre mit sich bringt, müssen Karteninhabende klar und transparent über deren Verwendung, über die damit verbundenen Risiken sowie über ihre Rechte informiert werden. Sie müssen wissen, an welcher Stelle sie Auskunft über die gespeicherten Daten bekommen und deren Berichtigung oder Löschung veranlassen können. Es muss sichergestellt werden, dass die gespeicherten Daten nur gelesen, an Dritte weitergegeben oder geändert werden können, wenn die Betroffenen darüber informiert sind. Sie müssen auch wissen, welche Folgen der Verlust der Karte haben kann und was in einem solchen Fall zu tun ist.

Festzuhalten ist auch die Pflicht der herausgebenden Stelle, die gespeicherten Daten

zu löschen, sobald sie nicht mehr benötigt werden (mehr zu Chipkarten im Gesundheitswesen auf S. 58)

2.2.7. Umsetzung der Datensicherheit in der Bundesverwaltung

Mit der Umsetzung der technischen und organisatorischen Massnahmen des Datenschutzes bzw. der Datensicherungsmassnahmen geht es nur langsam voran. Obwohl der Bundesrat aufgrund des jährlichen Berichtes des Informatikstrategieorgans Bund noch einmal darauf hingewiesen hat, dass die Datensicherheitsvorgaben in der Bundesverwaltung vollumfänglich einzuhalten sind, stellen wir immer wieder fest, dass diesen Vorgaben nicht die notwendige Aufmerksamkeit geschenkt wird. Es werden beispielsweise den Datenschutz- und Sicherheitsverantwortlichen nicht die notwendige Position in den Organisationseinheiten und insbesondere in den Informatikprojekten eingeräumt. Eine Optimierungsmöglichkeit für die Umsetzung der Datenschutzvorgaben sehen wir darin, dass unsere nicht befolgten oder abgelehnten Empfehlungen der Eidg. Datenschutzkommission zum Entscheid vorgelegt werden können.

Nur ein kleiner Teil der EDV-Projekte in der Bundesverwaltung wird beim Informatikstrategieorgan des Bundes (ISB) angemeldet und uns zugestellt. Die Anmeldung erfolgt gemäss dem Standard für die Abwicklung von Informatikprojekten in der Bundesverwaltung (HERMES) mit dem Projektantrag. Bereits in diesem sind erste Angaben zu Datenschutz- und Sicherheitsaspekten aufzuführen. In rund 50% der angemeldeten Projekte fehlen Angaben zu diesen Punkten. Dieses Problem kann man lösen, indem der Projektauftrag nur mit der Unterschrift des Datenschutz- bzw. Sicherheitsbeauftragten verabschiedet werden kann. Dieses Steuerungsinstrument wird aber nur selten eingesetzt.

Auch aufgrund der Position des Datenschutzverantwortlichen in der Organisation ist sehr schnell festzustellen, ob man Datenschutzanliegen die notwendige Bedeutung zukommen lässt. Selbstverständlich ist es auch wichtig, dass diese Aufgabenträger an den richtigen Ausschüssen oder Konferenzen teilnehmen, damit allfällige Soll-Ist-Abweichungen raschmöglichst erkannt werden. Wir stellen immer wieder fest, dass in den meisten Fällen die Verfügbarkeit der Systeme in angemessener Weise gewährleistet ist. Eine Nichtverfügbarkeit von Systemen wird sofort von allen Benutzern inklusive der Geschäftsleitung erkannt, womit auch der Druck steigt, das System zu verbessern. In Bereichen, in denen die Verfügbarkeit ein absolutes Muss ist, kann man mögliche Ausfallkosten recht genau quantifizieren, so dass klar ersichtlich ist, welcher Aufwand für die Verbesserung des Systems gerechtfertigt ist.

Anders sieht es bei den beiden anderen Komponenten der Datensicherheit aus. Vertraulichkeit und Integrität sind in den meisten Fällen weniger genau quantifizierbar. Bei mangelhafter Umsetzung können aber erhebliche Schäden entstehen. Nicht zu unterschätzen sind Imageschäden, wenn Datenschutz- oder Sicherheitsverletzungen an die Öffentlichkeit gelangen. Gemäss Medienangaben werden aber nur rund 3% Prozent dieser Verletzungen bekannt. Aus diesem Grunde wird es für die Leitungsinstanzen auch schwierig sein, weitergehende Massnahmen durchzusetzen.

Der Bundesrat hat in den rechtlichen Normen zum Datenschutz festgehalten, dass bei der Bearbeitung von sensitiven Personendaten die Datensicherheitsanforderungen gemäss dem Stand der Technik umzusetzen sind. In einem sich schnell ändernden Umfeld wie der Informatik hat man aber kaum Zeit, sich eingehend mit der Datenschutz- und Datensicherheitsproblematik auseinander zu setzen. Weil sich diese Aufgaben nur schlecht verkaufen lassen und durchaus auch einige «kreative» Konflikte entstehen könnten, weicht man diesen leider in vielen Fällen aus.

Wir haben heute im Bereich der Bundesverwaltung bei Nichteinhaltung von Datenschutzvorschriften die Möglichkeit, eine Empfehlung zuhanden des verantwortlichen Organs zu erlassen. Wird die Empfehlung nicht befolgt oder abgelehnt, so kann die Angelegenheit dem Departement zum Entscheid vorgelegt werden. Bleibt es bei der Ablehnung, so bleiben uns keine weiteren Möglichkeiten, der Umsetzung der Datenschutz- und Datensicherheitsanliegen Nachdruck zu verleihen. Wir erachten es deshalb als wichtig, dass die Regelung, die im Privatrechtsbereich gilt, auch in der Bundesverwaltung zur Anwendung kommt, so dass wir unsere Empfehlungen, welche von den Departementen oder der Bundeskanzlei nicht befolgt oder abgelehnt werden, der Eidg. Datenschutzkommission zum Entscheid vorgelegen können. Mit einer solchen Norm könnten sich auch die Leitungsinstanzen in der Bundesverwaltung auf Vorgaben abstützen, welche eine vorschriftkonformes Arbeiten ermöglichen würde.

2.2.8. Datenschutzaspekte bei der Fernwartung (Remote Access Tools)

Bei der Fernwartung von PCs ist darauf zu achten, dass die Freigabe dieser Arbeiten nur von der Stelle bzw. dem Organ ausgehen darf, deren Computer gewartet wird. Die Kommunikation zwischen den beiden Rechnern soll in chiffrierter Form erfolgen, damit keine interpretierbaren Daten an Dritte gelangen können. Der Zugriff auf die Systeme ist so zu gestalten, dass auf die gespeicherten Personendaten (Datensammlungen) nicht oder nur im Einzelfall zugegriffen werden kann, ausser die sensitiven Daten seien in chiffrierter Form gespeichert. Wartungsarbeiten sind revisionssicher zu protokollieren und die Protokolle sind regelmässig auszuwerten.

Eine Fernwartung kann entweder von eigenen System- oder Anwendungsverantwortlichen oder von Spezialisten externer Organisationseinheiten (Computer-, Softwarefirmen) durchgeführt werden. In beiden Situationen besteht die Gefahr, dass Informationen unkontrolliert abfliesen können. Jeder Firma sollte der Wert ihrer Kundendaten bekannt sein. Um so erstaunlicher ist es, dass man diese Daten oft in vollem Umfang Fernwartungsexperten «zur Verfügung stellt», ohne dass die notwendigen Sicherheitsmassnahmen getroffen wurden.

Bei Wartungsarbeiten existieren viele Angriffsmöglichkeiten auf Systeme bzw. Daten. Grundsätzlich muss die Person bzw. die Organisationseinheit, bei der Fehler behoben oder Wartungsarbeiten durchgeführt werden sollen, das Einverständnis dazu geben, indem sie z.B. auf dem PC ein Programm aktiviert. Bei einem solchen Vorgehen hat man die Gewähr, dass nicht unkontrolliert Wartungsarbeiten vorgenommen werden können.

Im Weiteren muss dafür gesorgt werden, dass die übertragenen Daten nicht von anderen Personen im Klartext eingesehen oder kopiert werden können. Es ist ein absolutes Muss, die Daten in chiffrierter Form zu übertragen. Ein weiterer wichtiger Punkt bei der Bearbeitung von sensitiven Daten ist die chiffrierte Form der Datenspeicherung, so dass man bei Wartungs- oder Unterstützungsarbeiten allenfalls auf die Daten gelangen kann, diese aber nicht interpretierbar sind. Ist es im Einzelfall für die Fehlerbehebung notwendig, die Daten zu entschlüsseln, so soll dies kontrolliert werden, z.B. durch das 4-Augen-Prinzip.

Selbstverständlich ist darauf zu achten, dass Passphrasen oder Schlüssel, deren Kenntnis oder Besitz für die Dechiffrierung notwendig sind, Unberechtigten nicht zugänglich sind. Der Zugriff sollte nicht nur durch Passphrasen, sondern im sensitiven Bereich innerhalb der Organisationseinheit zusätzlich durch den Einsatz von Chipkarten oder biometrischen Systemen geschützt sein. Es soll nur auf die für die Aufgabenerfüllung notwendigen Daten zugegriffen werden können. Das Herunterladen von Dateien bei Fernwartungs- oder Reparaturarbeiten zur Fehlerbehebung ist insbesondere bei sensitiven Systemen zu untersagen, da sonst keine Kontrolle mehr möglich ist.

Sensitive Eingriffe, wie die Fernwartung oder die Fehlerbehebung in produktiven Systemen sind revisionssicher zu protokollieren. Dies bedeutet insbesondere, dass nachträgliche Änderungen oder das Löschen von Protokolldaten nicht unkontrolliert möglich sein darf. Die Protokolle sind während eines Jahres aufzubewahren und regelmässig auszuwerten, wofür die notwendigen Ressourcen vorhanden sein müssen.

Für (Fern-)Wartungsarbeiten empfiehlt es sich, einen schriftlichen Vertrag auszuarbeiten, in dem die notwendigen technischen und organisatorischen Massnahmen geregelt werden.

2.2.9. Die Umsetzung von Datenschutzmassnahmen bei der Strafurteilsdatenbank

Bei Statistiksystemen müssen Bundesorgane darauf achten, dass die Personendaten anonymisiert bzw. pseudonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt. Der erste Schritt der Anonymisierung erfolgt bei der Strafurteilsstatistik über das Kreieren von Identifikatoren, ein weiterer Schritt über die Erstellung von Identifikationsnummern für die Produktionsdatenbank. Eine vollständige Anonymisierung ist für den Identifikator beim vorliegenden System nicht möglich, weil sich die Identität der Personen, z.B. bei Heirat (Namens-, Heimatorts-, Nationalitätsänderung) zeitlich verändern kann. Es wurde deshalb ein «sprechender» pseudonymisierter Identifikator geschaffen, der es erlaubt neu eingehende Identitäten bereits bestehenden Identitäten zuzuordnen, soweit diese bereits in der Strafurteilsdatenbank registriert sind. Das Beispiel zeigt u.a. auch auf, dass eine Anonymisierung oder Pseudonymisierung von Daten in vielen Fällen weniger Kosten für die Datensicherheit verursacht.

Die Daten für die Strafurteilsstatistik stammen aus dem Strafregister (VOSTRA), aus rund 170 Anstalten des Straf- und Massnahmenvollzugs, 26 Vollzugsämtern oder Bewährungshilfsstellen sowie von 26 Jugendanwaltschaften. Diese Strafurteile werden wöchentlich dem dem Bundesamt für Statistik (BFS) durch elektronische Datenübermittlungen zur Verfügung gestellt, allerdings nicht in «sprechender» pseudonymisierter Form. Wir haben das BFS darauf aufmerksam gemacht, dass es diese Daten nur in entsprechender pseudonymisierter Form einholen darf. Die Ein- und Austritte aus den Anstalten, als auch Jugendurteile sowie Angaben zu Bewährungshilfen werden dem BFS mit Hilfe von Formularen, Disketten oder durch Datenübermittlung in «sprechender» pseudonymisierter Form zugestellt. Daten, die aus dem Strafregister stammen und nicht pseudonymisiert sind, werden durch einen proprietären Algorithmus mit einer Schlüssellänge von 72 Bit verschlüsselt. Gemäss Datenschutzgesetz muss bei der Bearbeitung von sensitiven Daten der Stand der Technik bei den Sicherheitsmassnahmen umgesetzt werden. Dies ist im vorliegenden Fall im Datennetz des EJPD bis heute noch nicht der Fall. Symmetrische Algorithmen, die dem Stand der Technik entsprechen, sind nicht proprietär, sondern der Öffentlichkeit zugänglich und haben eine Mindestschlüssellänge von 128 Bit. Beispiele dafür sind 3DES, IDEA oder AES.

Die «sprechende» Pseudonymisierung erfolgt aufgrund von Abkürzungen des Inhalts folgender Datenfelder, die dann den Identifikator bilden: Name, Aliasname, Vorname, Geschlecht, Geburtstag, Geburtsort bzw. -land, Heimatort bzw. Nationalität, Wohnsitz und Zivilstand. Aufgrund der Pseudonymisierung kann von der Identität der Person auf

die pseudonymisierten Daten dieser Person in der Strafurteilsdatenbank, soweit sie bereits registriert ist, geschlossen werden. Eine eindeutige Umkehrung aufgrund der Identifikator-Daten in der Datenbank auf die Identität der Personen ist aber nur schwer möglich. Insbesondere bei kurzen Namen besteht allerdings die Gefahr, dass Personen identifiziert werden könnten. Auch diesen Umstand muss man noch besser in den Griff bekommen.

Mit der Bearbeitung von «sprechenden» pseudonymisierten Daten im Bereich der Strafurteile beschäftigen sich beim BFS rund 3 Personen, womit der Zugriff auf die Daten eingeschränkt ist. Für die Produktionsdatenbank, auf die eine grössere Menge von Personen Zugriff haben, werden Identifikationsnummern kreiert, die einen Bezug zu den «sprechenden» pseudonymisierten Personendaten (Identifikator) haben. In der Produktionsdatenbank ist somit die Identifikation von Personen nicht möglich. Das Beispiel zeigt auch auf, dass die Anforderungen des Datenschutzes an die Datensicherheit sinken, wenn mit pseudonymisierten Daten gearbeitet wird. Nur derjenige Teil des Systems, der die Depseudonymisierung ermöglicht, ist noch sensitiv (Schutzstufe 3/höchste Sicherheitsstufe). Die anderen Systemteile müssen aus der Sicht des Datenschutzes nicht mehr mit Massnahmen dieser Stufe geschützt werden.

2.2.10. Datenleck beim World Economic Forum

Globalisierungsgegner nutzten eine Schwachstelle im Informatiksystem des World Economic Forum (WEF) und gelangten so in Besitz von Personendaten von Persönlichkeiten aus Wirtschaft und Politik. Diese Daten wurden verschiedenen Medien zugespielt und in der Folge publiziert.

Am 4. Februar 2001 und in mehreren späteren Ausgaben publizierte die Sonntagszeitung (und in der Folge auch andere Medien) Berichte über einen Hacker-Angriff von Globalisierungsgegnern auf den Web-Server des WEF. Dabei sollen die Hacker in den Besitz von Namen, Reisepassnummern, Handy- und privaten Telefonnummern, Kreditkartennummern, E-Mail-Adressen, Benutzernamen und Passwörtern von Tausenden von WEF-Teilnehmenden gelangt sein. Das Datenmaterial soll zudem subjektive Bemerkungen zu Persönlichkeiten aus Politik und Wirtschaft enthalten haben.

Der Sonntagszeitung wurde eine CD-ROM mit den erlangten Daten zugespielt. Wir erhielten von ihr eine Liste mit Beispielen von subjektiven Bemerkungen und Kommentaren zu einzelnen WEF-Teilnehmenden.

Aufgrund dieser Informationen sowie der Tatsache, dass die vom WEF angewandten Bearbeitungsmethoden geeignet waren, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler), entschlossen wir uns, am Hauptsitz des WEF

eine Kontrolle vorzunehmen. Dabei legten wir Wert darauf, der Direktion des WEF die allgemeinen Datenschutzgrundsätze wie das Transparenz-, Verhältnismässigkeits- sowie Zweckmässigkeitsprinzip darzulegen. Wir wiesen insbesondere darauf hin, dass das DSG vom Inhaber einer Datensammlung verlangt, Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen. Zudem haben wir der Direktion des WEF auch geraten, die Ablaufprozesse im Informatikbereich regelmässig analysieren sowie periodische Sicherheitsprüfungen vornehmen zu lassen. Die Direktion hat unsere Anregungen zur Kenntnis genommen und umgesetzt.

2.3. Weitere Themen

2.3.1. Outsourcing von Datenbearbeitungen im privaten Sektor

Bearbeitungen von Personendaten gehören immer weniger zur alleinigen Zuständigkeit des Bearbeitungsverantwortlichen. Aus wirtschaftlichen oder technischen Gründen oder wegen der beschränkten Kompetenzen und Mittel werden Bearbeitungen häufig an Dritte vergeben. Damit sind bestimmte Risiken für die Achtung der Persönlichkeitsrechte der Personen, deren Daten im Auftrag bearbeitet werden, verbunden. In solchen Fällen empfehlen wir, einen Datenschutzvertrag abzuschliessen.

Die Datenbearbeitung im Auftrag (Outsourcing) umfasst alle Bearbeitungen, für welche der Verantwortliche zuständig ist, die jedoch von einer ihm nicht unterstellten Drittperson ausgeführt werden. Dabei kann es sich um manuelle oder automatisierte Verfahren handeln. Die Bearbeitungen im Auftrag können ganze Bearbeitungsvorgänge oder nur bestimmte abgegrenzte Phasen umfassen. Sie unterstehen dem Bundesgesetz über den Datenschutz (DSG). Falls bestimmte gesetzliche Voraussetzungen erfüllt sind, gilt die Datenbearbeitung durch Dritte als Rechtfertigungsgrund, um Personendaten ohne Persönlichkeitsverletzung der Betroffenen zu bearbeiten und bearbeiten zu lassen. Der Auftraggeber muss jedoch weiterhin über die Daten bestimmen, deren Bearbeitung er einer Drittperson anvertraut.

Der Auftrag muss sich auf spezifische, auf ein bestimmtes Projekt bzw. eine Angelegenheit begrenzte Leistungen beziehen. Der beauftragte Dritte ist eine «Hilfskraft» des Auftraggebers: Er besitzt keine Entscheidungsbefugnis in Bezug auf die zu bearbeitenden Daten und kann nicht bestimmen, welche Daten beschafft und bearbeitet werden dürfen. Ebenso wenig kann er sie für seine eigenen Zwecke bearbeiten. Der Auftragnehmer bearbeitet im Rahmen des Mandats lediglich Daten, die ihm der Bearbeitungs-

verantwortliche verfügbar gemacht bzw. die er in dessen Namen beschafft hat. Zwischen dem Auftragnehmer und der betroffenen Person existiert kein Vertragsverhältnis. Für die Garantie der Rechte der betroffenen Person ist grundsätzlich der Auftraggeber verantwortlich. Die Bearbeitung im Auftrag im Sinne des DSG schliesst Mandate aus, die eine Aufgabenverlagerung herbeiführen und den Auftragnehmern die autonome Datenbearbeitung übertragen. In letzterem Fall kann der Auftraggeber nicht mehr über die Daten bestimmen. Der beauftragte Dritte wird zum Bearbeitungsverantwortlichen und führt den Vertrag mangels Weisungen des Auftraggebers weitgehend frei aus. Er kann die Daten für seine eigenen Zwecke verwenden und haftet für die Rechtmässigkeit der durchgeführten Bearbeitungen.

Um sich auf den Rechtfertigungsgrund für das «Bearbeiten von Personendaten durch Dritte» zu berufen, muss der Bearbeitungsverantwortliche dafür sorgen, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte. Mit anderen Worten hat er darauf zu achten, dass der beauftragte Dritte sich in gleichem Masse an die Datenschutzvorschriften hält, wie er selbst dazu verpflichtet ist. Ausserdem hat er sicherzustellen, dass keine gesetzliche oder vertragliche Geheimhaltungspflicht der Auftragsvergabe entgegensteht. Der Bearbeitungsverantwortliche muss also für die Achtung der Datenschutzvorschriften durch den beauftragten Dritten sorgen. Gegenüber der betroffenen Person bleibt er der Hauptverantwortliche für die Bearbeitung. Neben der Berücksichtigung der Kosten und der Rationalisierung muss er vor allem dem Know-how und der Qualität grosse Bedeutung beimessen.

So hat der Bearbeitungsverantwortliche insbesondere die Datensicherheit zu gewährleisten. Daher evaluiert er die Risiken der Datenbearbeitung im Auftrag und erkundigt sich insbesondere nach den technischen und organisatorischen Massnahmen des potentiellen Partners; gegebenenfalls fordert er ergänzende Massnahmen. Ausserdem hat er die erwarteten Leistungen in quantitativer und qualitativer Hinsicht zu definieren, das Mandat einer strengen Leistungskontrolle zu unterstellen und Massnahmen vorzusehen, falls die erwarteten Leistungen nicht erbracht werden. Der Qualitätsaspekt beschränkt sich nicht auf die Frage der möglichst raschen Durchführung der Bearbeitung mit den leistungsstärksten Informatikinstrumenten, sondern betrifft im Wesentlichen die Garantie, dass der Auftragnehmer die Datenschutzauflagen befolgt. Der Auftragnehmer hat insbesondere der Kontrolle der Bearbeitungstätigkeiten durch den Auftraggeber, durch den Eidgenössischen Datenschutzbeauftragten oder durch ein unabhängiges Revisionsorgan zuzustimmen.

Je nach Bedeutung des Auftrags, insbesondere wenn es sich um besonders schützenswerte Daten handelt und eine grosse Anzahl von Personen betrifft, muss die Bearbeitung dokumentiert werden und Gegenstand einer Informatikrevision bilden. Im Übrigen sollte diese Revisionspflicht nicht nur für die Bearbeitung im Auftrag, sondern für

alle automatischen Bearbeitungen von bestimmten Umfang bzw. von besonders schützenswerten Daten oder Persönlichkeitsprofilen in das DSG aufgenommen werden.

Falls der Bearbeitungsverantwortliche im Rahmen der Mandatsausführung Daten an den beauftragten Dritten übermitteln muss, handelt es sich nicht um eine Bekanntgabe an einen «unabhängigen» Dritten, sofern der Verantwortliche weiterhin über die übermittelten Daten bestimmt. Das hat insbesondere zur Folge, dass der Bearbeitungsverantwortliche neben dem eigentlichen Auftrag keine weiteren Rechtfertigungsgründe für den Datentransfer nennen und dass er die Datensammlung nicht melden muss, falls die Anmeldungsvoraussetzungen erfüllt sind (siehe 3. Tätigkeitsbericht 1995/96, S. 78). Dagegen hat er für die Bekanntgabe ins Ausland die Bestimmungen des DSG zu befolgen.

Das DSG gestattet das Outsourcing zur Bearbeitung von Personendaten durch private Personen. Allerdings darf diese Bearbeitungsart den Datenschutz nicht schwächen. Im Interesse des Auftraggebers empfehlen wir, mit dem beauftragten Dritten einen Vertrag über die Auftragsvergabe abzuschliessen, in dem die zu befolgenden Datenschutzvorschriften niedergelegt werden. Je nach Art des Auftrags sollten insbesondere folgende Punkte behandelt werden:

- Achtung der Datenschutzbestimmungen, vor allem die Regelung der Rahmen bedingungen für die Datenbearbeitung (Umfang der Bearbeitung);
- Zweckbindung der Bearbeitung;
- Festlegung der angemessenen technischen und organisatorischen Massnahmen, um ein hohes Datenschutzniveau und Vertraulichkeit zu gewährleisten (Berücksichtigung des jüngsten Stands der Technik, Protokollierung, Zugangskontrolle, Chiffrierung);
- Trennung der Datenbearbeitung – vor allem bei besonders schützenswerten Daten oder Persönlichkeitsprofilen – von sonstigen, vom beauftragten Dritten durchgeführten Bearbeitungen, um Interessenskonflikte zwischen Auftraggeber und Auftragnehmer zu vermeiden (insbesondere in Bezug auf eigene bzw. für andere Auftraggeber ausgeführte Bearbeitungen);
- Verschlüsselung der besonders schützenswerten Daten und der Persönlichkeitsprofile, sofern die Mitarbeiter des beauftragten Unternehmens die Daten zur Erfüllung ihrer Aufgaben nicht zu lesen bzw. zu bearbeiten brauchen;
- Anforderungen an die Einstellung von Personal;
- Allfällige Vergabe von Unterverträgen durch den beauftragten Dritten: Es ist vor

allem zu regeln, was unter welchen Voraussetzungen als Unterauftrag vergeben werden darf. Der beauftragte Dritte muss den Auftraggeber in jedem Fall über etwaige Untervertragsnehmer benachrichtigen;

- gegebenenfalls Zugriffsvoraussetzungen zu Personendaten, wenn der Auftragnehmer für Wartungsarbeiten Fernzugriff auf die Computer des Auftraggebers hat;
- Zugangsvoraussetzungen zu den Anlagen des Auftraggebers;
- Unterstellung des Auftragnehmers und seiner Beschäftigten unter die Geheimhaltungspflicht;
- Kontrolle der Achtung der Vertragsbestimmungen, insbesondere eine Informatikrevision durch eine externe Stelle;
- Haftungsregelung im Schadensfall bzw. bei Vertragsverletzung;
- Konventionalstrafe, deren Höhe einen Abschreckungseffekt zeigen sollte, d.h. den Auftragnehmer von einer vertrags- oder datenschutzwidrigen Datenverwendung abhalten sollte;
- Informationspflicht des Auftragnehmers gegenüber dem Auftraggeber zur konkreten Durchführung der Bearbeitung;
- Ende des Vertrags, Bestimmung, was mit den Daten nach der Durchführung des Auftrags geschieht.

2.3.2. Das informatisierte Standesregister

Für die Beurkundung des Personenstandes will der Bund eine zentrale elektronische Datenbank schaffen. Gemäss einer dem Parlament unterbreiteten Gesetzesvorlage soll der Bundesrat für die Einhaltung des Datenschutzes besorgt sein. Wir haben mehrmals unsere datenschutzrechtlichen Bedenken gegen diesen Gesetzesentwurf angemeldet. Unsere Vorschläge wurden jedoch vom federführenden EJPD nicht berücksichtigt.

Der Bund beabsichtigt, die Beurkundung des Personenstandes zu informatisieren. Dafür sollen die rund 1750 Zivilstandsämter miteinander elektronisch vernetzt werden. Vorgesehen ist die Schaffung einer zentralen Datenbank namens Infostar, die durch den Bund im Auftrag der Kantone betrieben und durch die landesweit vernetzten Zivilstandsbehörden bearbeitet wird. Dieses Informatikprojekt bedarf einer gesetzlichen Grundlage im Zivilgesetzbuch. Vorgesehen ist, dass der Bundesrat die Oberaufsicht über die Beurkundung des Personenstandes innehat und auch für den Schutz der Persönlichkeit und der Grundrechte von Personen sorgen soll, über die in Infostar Daten

bearbeitet werden. Die geplante Datensammlung wird sämtliche Zivilstandsdaten von allen in der Schweiz wohnhaften Personen enthalten. Es handelt sich dabei um eine der grössten elektronischen Datensammlungen mit aktuellen und sensiblen Personendaten der Schweiz. Die Gesetzesrevision sieht vor, dass Infostar zugleich auch Funktionen erfüllen soll, die über die den Zivilstandsämtern ursprünglich übertragenen Aufgaben hinausgehen. So erhalten nicht nur die Zivilstandsbehörden der Kantone und des Bundes Zugriff auf Infostar, sondern gemäss Botschaft können auch zahlreiche andere Behörden die Datensammlung für ihre eigenen Zwecke nutzen, obwohl deren primäre Aufgabenerfüllung überhaupt nicht im Bereich der Personenbeurkundung und des Zivilstandswesens liegt.

Das DSG findet auf öffentliche Register des Privatrechtsverkehrs keine Anwendung (Art. 2 Abs. 2 lit. d DSG). Davon ist das Zivilstandsregister bzw. -wesen und damit auch Infostar betroffen. Dem Datenschutz muss daher direkt in der entsprechenden Gesetzgebung Rechnung getragen werden (ZGB, Zivilstandsverordnung). Wir plädierten deshalb dafür, dass bei der Schaffung der gesetzlichen Grundlagen für ein Informatikprojekt wie Infostar, das stark in die Persönlichkeit jeder einzelnen Bürgerin und jedes einzelnen Bürgers eingreift, die wichtigsten Grundsätze des DSG berücksichtigt werden.

Ebenso wiesen wir mehrmals daraufhin, dass das Auskunftsrecht, das wohl bedeutenste Institut des Datenschutzes, und dessen Ausgestaltung explizit in einer formellen gesetzlichen Grundlage geregelt werden müsse. Wir unterbreiteten einen ausformulierten Vorschlag, der das Auskunftsrecht und dessen Umfang, die Einschränkungen, die Form und den Inhalt der Auskunftserteilung umfassend regelt. Aus Gründen der Transparenz schlugen wir auch vor, dass im ZGB aufgeführt werden sollte, wer die Datenbank betreibt und welche Behörden Daten bearbeiten.

Da sowohl Bundes- wie auch kantonale Behörden Bearbeitungen in der Datenbank vornehmen können, sollte zwecks Sicherstellung einer klaren Kompetenzaufteilung zwischen Bund und Kantonen ausdrücklich im ZGB festgehalten werden, wer im Bereich der Aufsicht zuständig ist. Mit Infostar wird nun erstmals eine Datenbank geschaffen, deren Aufsicht nicht mehr den gleichen Regelungen wie die anderen elektronischen Datensammlungen des Bundes unterliegt. Datenbanken wie das Staatsschutz-Informations-System ISIS oder das Zentrales Ausländerregister ZAR unterstehen der gleichen und damit auch einheitlichen Aufsicht des EDSB. Gerade weil auf Infostar aber eine ungemein grosse Anzahl von Behörden (Zivilstandsbehörden sowie weitere Bundes- und kantonale Behörden) Zugriff haben wird, ist eine einheitliche Aufsicht durch eine unabhängige Fachstelle von eminenter Bedeutung. Wir sind der Ansicht, dass der Bundesrat als Oberaufsichtsbehörde diese Funktion nicht effizient ausüben kann. Die wirkliche Aufsichtstätigkeit kann nur durch eine sachkompetente Fachstelle

wie dem EDSB wahrgenommen werden. Damit wird auch sichergestellt, dass private Personen sich mit ihren datenschutzrechtlichen Fragen an eine neutrale und unabhängige Stelle wenden können.

Die Botschaft zur Teilrevision des ZGB wurde vom Bundesrat ans Parlament überwiesen. Die oben erwähnten Anliegen des Datenschutzes wurden vom federführenden EJPD nicht berücksichtigt.

2.3.3. Die Veröffentlichung von Bundesgerichtsentscheiden im Internet

Seit dem 23. April 2001 publiziert das Bundesgericht fast alle Entscheide auf dem Internet vollständig. Die Namen der Parteivertreter werden dabei veröffentlicht, in einigen wenigen Fällen auch diejenigen der Parteien. Das Bundesgericht überprüft jeden Fall einzeln und nimmt eine Abwägung der verschiedenen Interessen vor.

Seit dem 23. April 2001 publiziert das Bundesgericht fast alle seine Entscheide vollständig auf dem Internet. Dabei werden auch die Namen der Parteivertreter sowie in einigen Fällen ebenfalls diejenigen der Parteien veröffentlicht. In diesem Zusammenhang gelangten verschiedene Personen mit der Frage an uns, ob dies datenschutzrechtlich zulässig sei. Diesbezüglich ist zunächst zu beachten, dass das Bundesgericht jeden Fall einzeln überprüft und die verschiedenen Interessen, darunter auch die Interessen der betroffenen Parteien, gegeneinander abwägt. Je nach Fall erfolgt keine, oder nur eine teilweise Publikation. Zudem werden auch die Namen der Parteien in der Regel vor der Publikation entfernt. In wenigen Fällen, in denen keine überwiegenden privaten Interessen der Betroffenen entgegenstehen, werden die Namen der Parteien veröffentlicht.

Bei der Publikation von Urteilen sind verschiedene Interessen gegeneinander abzuwägen. Einerseits hat die Öffentlichkeit ein Interesse daran, Kenntnis von den Urteilen des Bundesgerichts zu erhalten. Dies unter anderem um eine gewisse Kontrolle (Transparenz der Rechtsprechung) gewährleisten zu können. Zudem ist es für Personen und Rechtsanwälte wichtig, die Jurisprudenz in ähnlichen Fällen zu kennen. Andererseits kann mit der Veröffentlichung von Urteilen die persönliche Freiheit der Parteien tangiert werden. Auch in der Literatur wurde diese Problematik bei der Veröffentlichung von Gerichtsurteilen erkannt. Für das Verständnis des einzelnen Urteils ist die genaue Beschreibung der Sachumstände des konkreten Streitfalles von entscheidender Bedeutung. Dabei lassen sich Rückschlüsse auch auf nicht namentlich genannte Prozessparteien nicht immer verhindern, z.B. wenn der betreffende Streitfall oder die beteiligten Parteien in der Öffentlichkeit bekannt sind. In der Literatur wurde diesbezüglich festgehalten, dass dies hinzunehmen sei mit Blick auf den Grundsatz der

Öffentlichkeit von Gerichtsverhandlungen sowie auf den Umstand, dass allgemein zugängliche Daten bereits gestützt auf das Datenschutzgesetz bekannt gegeben werden dürfen.

Betreffend die Publikation der Namen der Rechtsanwälte darf nicht vergessen werden, dass diese auch bezüglich des publizierten Falles dem Anwaltsgeheimnis unterstehen. Zudem hat der Anwalt – gemäss Bundesgericht – als «Diener des Rechts» und «Mitarbeiter der Rechtspflege» eine besondere Stellung.

Daraus folgt, dass die obenerwähnte Praxis des Bundesgerichts, die Frage der Publikation von Urteilen in jedem Fall einzeln zu überprüfen und dabei eine Abwägung der verschiedenen Interessen vorzunehmen, datenschutzfreundlich ist.

2.3.4. Elektronische Zutrittssysteme in Skigebieten

Bei der Verfolgung von Skipässen gelten die Bestimmungen des Datenschutzgesetzes, wenn dabei Personendaten bearbeitet werden. Liegt eine richterliche Anweisung oder eine gesetzliche Grundlage vor, darf ein Skipass für eine Ermittlung verfolgt und die Ergebnisse an die Polizei oder an ein Gericht bekannt gegeben werden. Die Verfolgung von Karten von Mitarbeitern und Mitarbeiterinnen darf nicht systematisch, sondern nur im Einzelfall und unter bestimmten Bedingungen erfolgen.

Die Koordinationsstelle von verschiedenen Bergbahnen unterbreitete uns einige Fragen betreffend ein elektronisches Zutrittssystem, bei welchem alle Skipässe erfasst werden. Wir haben festgehalten, dass Datenbearbeitungen im Zusammenhang mit der Verfolgung von Skipässen (wann wurden welche Bahnen mit einem Skipass benutzt) nur dann erfolgen dürfen, wenn dabei die Bestimmungen des Datenschutzgesetzes eingehalten werden. So müssen insbesondere die allgemeinen datenschutzrechtlichen Grundsätze – u.a. Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Zweckgebundenheit, Richtigkeit der Daten und Datensicherheit – respektiert werden. Weiter muss ein Rechtfertigungsgrund gemäss Art. 13 DSG vorliegen. Dabei spielt es keine Rolle, ob der Skipass einem Gast entgeltlich oder unentgeltlich abgegeben wurde. Bei anonymen Kartenverfolgungen werden keine Personendaten im Sinne des DSG bearbeitet. Solche Verfolgungen fallen somit nicht unter das DSG. Anonym ist eine Kartenverfolgung jedoch nur, wenn der Inhaber oder die Inhaberin nicht mehr bestimmbar ist.

Ein Skipass darf nur dann für eine Ermittlung verfolgt und die Ergebnisse an die Polizei oder an ein Gericht bekannt gegeben werden, wenn diesbezüglich eine richterliche Anweisung oder eine gesetzliche Grundlage vorliegt. Die Koordinationsstelle der be-

troffenen Bergbahnen darf Daten an die Polizei bekannt geben, wenn diese für die Einreichung einer Strafanzeige nötig sind.

Schliesslich stellte sich die Frage, inwiefern Karten von Mitarbeitenden verfolgt werden dürfen, um allfällige Missbräuche aufzudecken. Diesbezüglich ist zunächst darauf hinzuweisen, dass nebst den Bestimmungen des Datenschutzgesetzes auch noch die Bestimmungen im Arbeitsrecht und insbesondere Art. 26 der Verordnung 3 zum Arbeitsgesetz zu beachten sind. Eine systematische Überwachung des Verhaltens sämtlicher Mitarbeitenden ist nicht gestattet. Art. 26 Abs. 1 der Verordnung 3 zum Arbeitsgesetz gilt jedoch nicht absolut. Datenbanken oder Kontrollsysteme resp. elektronische Zutrittssysteme dürfen im *Einzelfall* zur Verhaltensüberwachung benutzt werden, wenn folgende kumulative Voraussetzungen erfüllt sind:

- Ein überwiegendes Interesse des Arbeitgebers liegt vor. Dies ist beispielsweise der Fall bei der Aufdeckung von Missbräuchen;
- Die Überwachung der Einhaltung der Nutzungsregelung betreffend das elektronische Zutrittssystem erfolgt stichprobenweise und ohne Namen und Adresse d.h. beispielsweise nur aufgrund der Abonnementsnummer;
- Die personenbezogene Auswertung der Abonnementsnummer erfolgt nur bei Vorliegen eines konkreten Verdachts eines Missbrauchs;
- Die Angestellten resp. Mitarbeitenden wurden vorgängig informiert.

Diese Voraussetzungen gelten unabhängig davon, ob die Mitarbeitenden Ihre Skipässe gratis erhalten haben oder nicht. Überdies sind die erwähnten Bedingungen auch dann einzuhalten, wenn die Auswertungen nur für interne Zwecke erfolgen. Wie oben erwähnt, müssen die Mitarbeiter vorgängig informiert werden – eine Zustimmung ist somit nicht nötig.

2.3.5. Anmeldeformulare für Mietwohnungen

Eine Immobiliengesellschaft zeigte sich nicht bereit dazu, das Urteil der Eidgenössischen Datenschutzkommission betreffend die Anmeldeformulare von Mietwohnungen zu berücksichtigen. Sie war der Meinung, dass der Vermieter bei der Auswahl einer neuen Mieterin oder eines neuen Mieters bedenkenlos weitere Angaben verlangen dürfe. Gegen diese Haltung haben wir eine Empfehlung erlassen und nach deren Ablehnung durch die Immobiliengesellschaft der Eidgenössischen Datenschutzkommission zum Entscheid vorgelegt. Der Text der Empfehlung und der Weiterziehung mitsamt rechtlicher Begründung ist auf S. 128 abgedruckt.

Im Zusammenhang mit der Anfrage einer Privatperson haben wir von einer Genfer Immobiliengesellschaft verlangt, uns eines ihrer Anmeldeformulare für Mietwohnungen zukommen zu lassen. Die Überprüfung ergab, dass das Anmeldeformular in mehreren Punkten gegen das Urteil der Eidgenössischen Datenschutzkommission vom 21. November 1996 (VPB 62.42B) in Sachen Mietwesen verstiess und dem im Anschluss an dieses Urteil neu verfassten EDSB-Merkblatt über die Anmeldeformulare von Mietwohnungen keine Rechnung trug. Wir informierten die Immobiliengesellschaft über die ungenügenden Punkte und verlangten eine Anpassung des Formulars im Sinne des Urteils und des Merkblatts.

Selbst nach mehreren Briefwechseln zeigte sich die Immobiliengesellschaft nicht dazu bereit, ihre Anmeldeformulare anzupassen. Sie stellte sich auf den Standpunkt, dass es für die Auswahl einer neuen Mieterin bzw. eines neuen Mieters unabdingbar sei, über zusätzliche Angaben (z.B. Adresse des bisherigen Vermieters, aktueller Mietzins, Immatrikulationsnummer des Fahrzeugs, ob und wann Betreibungen stattgefunden haben) zu verfügen, und verlangte, dass interessierte Personen bereits bei der Bewerbung für eine Wohnung ihrem Antrag u.a. folgende Dokumente beilegen müssen: Familienbüchlein oder Identitätskarte (schweizerische Staatsangehörige), Aufenthaltsbewilligung (ausländischen Staatsangehörige), aktuelle Gehaltsabrechnung, Auszug aus dem Betreibungsregister. Zudem mussten Mietinteressierte eine Einwilligungserklärung unterzeichnen, welche den Vermieter resp. die Immobiliengesellschaft ermächtigte, bei ihrem Arbeitgeber und bisherigen Vermieter jegliche Informationen zu Zahlungsfähigkeit, Arbeit, Gehalt, bisherigen Mietzinszahlungen sowie Betreibungen bzw. Verlustscheinen einzuholen. Zudem musste akzeptiert werden, dass diese Informationen auch von einer Wirtschaftsauskunftei eingeholt werden konnten.

Die Immobiliengesellschaft argumentierte, dass Mietinteressierte das Anmeldeformular letztlich ja unterschreiben und somit die Daten freiwillig abgeben. Dabei verkennt sie die Tragweite der Einwilligung der Verletzten im Sinne von Art. 13 Abs. 1 DSG. Diese Einwilligung hat nämlich als Akt wirklicher Selbstbestimmung, d.h. freiwillig und in Kenntnis der sich daraus ergebenden Konsequenzen, zu erfolgen. Mietinteressierte können es sich in der Regel nicht leisten, nur gewisse Fragen auf dem Anmeldeformular zu beantworten, da sie sonst als mögliche Kandidaten für das Wohnobjekt ausscheiden. Befinden sie sich in einer Notlage, kann demnach nicht davon ausgegangen werden, dass die Datenbearbeitung durch die Einwilligung der betroffenen Person gerechtfertigt ist. Verlangt ein Vermieter jedoch Angaben, die für den Vertragsabschluss nicht erforderlich sind, so muss er die Mietinteressierten ausdrücklich darauf hinweisen, dass die Beantwortung dieser Fragen freiwillig sei und eine Nichtbeantwortung keine negativen Auswirkungen auf das Gesuch habe.

In der Empfehlung wiesen wir u.a. auch darauf hin, dass die Immobiliengesellschaft im Zusammenhang mit der Datenbearbeitung den Grundsatz der Verhältnismässigkeit konsequent berücksichtigen muss. Angewandt auf die vorliegende Angelegenheit bedeutet dies, dass von den Mietinteressierten nur jene Daten einverlangt und in der Folge bearbeitet werden dürfen, die einerseits für die Auswahl eines Mieters bzw. einer Mieterin und andererseits für den eigentlichen Abschluss eines Mietvertrages dienlich und auch wirklich notwendig sind. Es ist nicht ersichtlich, warum bereits zum Zeitpunkt der Einreichung des Anmeldeformulars eine Aufenthaltsbewilligung bzw. ein Identitätsausweis präsentiert werden muss. Einzig unter der Bedingung, dass eine gesetzliche Bestimmung dies vorsieht (z.B. bei einer gesetzlichen Meldepflicht), können diese Ausweise dann einverlangt werden, wenn sich der Vermieter bzw. die Immobiliengesellschaft definitiv für einen Mieter bzw. eine Mieterin entschieden hat. Des Weitern dürfen zusätzliche Dokumente nur dann eingefordert werden, wenn sie für den Abschluss eines Mietvertrages unabdingbar sind oder wenn dazu eine gesetzliche Verpflichtung besteht. In jedem Fall dürfen diese Dokumente aber erst zum Zeitpunkt des unmittelbaren Vertragsabschlusses von der definitiv ausgewählten Person einverlangt werden. Dokumente, die nicht in einem direkten Zusammenhang mit dem Abschluss des Mietvertrages stehen, dürfen nur dann verlangt werden, wenn eine klare und eindeutige Zustimmung des Betroffenen vorliegt, indem die Beilage der Dokumente auf dem Anmeldeformular klar als fakultativ bezeichnet wird.

Unsere Empfehlung im oben ausgeführten Sinne wurde von der Immobiliengesellschaft abgelehnt. Wir haben die Angelegenheit der Eidgenössischen Datenschutzkommission zum Entscheid vorgelegt.

3. Justiz/Polizei/Sicherheit

3.1. Polizeiwesen

3.1.1. Erfahrungen mit dem indirekten Auskunftsrecht

Im Zeitraum 2001/2002 ist die Anzahl der indirekten Auskunftsgesuche im Polizeibereich gestiegen. Die Behandlung der Gesuche im Zusammenhang mit der inneren Sicherheit und der Bekämpfung der Geldwäscherei verläuft ohne Hindernisse. Diejenige im Zusammenhang mit der organisierten Kriminalität, dem illegalen Drogenhandel, der Falschmünzerei, des Menschenhandels und der Pornografie bereitet jedoch einige Schwierigkeiten, die auf die Natur des Systems JANUS zurückzuführen sind.

Die Anzahl der gemäss dem Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) für das Staatsschutz-Informationssystem ISIS eingereichten indirekten Auskunftsgesuche ist im Zeitraum 2001/2002 deutlich gestiegen. Dies liegt grösstenteils an der Behandlung zahlreicher Personendaten im Rahmen des G8-Gipfels in Genua durch den Dienst für Analyse und Prävention (DAP) des Bundesamtes für Polizei (BAP) (siehe dazu auch Text G8 S. 49). Auch die Anzahl der indirekten Gesuche laut Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes (ZentG) ist angestiegen, jedoch in geringerem Masse.

Die Behandlung der Gesuche betreffend das System ISIS verläuft nach wie vor reibungslos. Dies gilt ebenfalls für die Gesuche nach ZentG betreffend das System GEWA bei der Meldestelle für Geldwäscherei.

Was das System JANUS betrifft, so hat sich die in unserem letzten Tätigkeitsbericht beschriebene Lage (S. 13 und 14) nicht wesentlich geändert. Wir haben daher erneut eine Empfehlung an das BAP gerichtet mit der Aufforderung, dafür zu sorgen, dass sämtliche durch die Bundeskriminalpolizei (BKP, ehemals kriminalpolizeiliche Zentralstellen des Bundes) bearbeiteten Personendaten des Gesuchstellers unter Einhaltung des ZentG geprüft werden. Diese Empfehlung wurde zunächst durch das BAP zurückgewiesen, obwohl es zuvor die in unserem letzten Tätigkeitsbericht erwähnte Empfehlung zum selben Thema akzeptiert hatte. Um einen Ausweg zu finden, ohne sofort das EJPD einzuschalten, fand Ende Dezember 2001 eine Sitzung zwischen dem Eidgenössischen Datenschutzbeauftragten und der Direktion des BAP statt. In Folge dieser Sitzung verpflichtete sich das BAP, die in unseren Empfehlungen erwähnten Unstimmigkeiten zu korrigieren.

3.1.2. Personensicherheitsprüfungen innerhalb der Bundesverwaltung

Von der neuen Verordnung über die Personensicherheitsprüfungen sind zahlreiche Mitarbeiter der Bundesverwaltung betroffen. Die Datenbehandlung muss daher umso mehr mit dem Verhältnismässigkeitsprinzip im Einklang stehen. Die neue Verordnung soll demnächst ergänzt werden, namentlich durch eine Liste der im elektronischen Informationssystem für Sicherheitsprüfungen behandelten Personendaten.

Der Bundesrat hat das VBS mit der Revision der Verordnung über die Personensicherheitsprüfungen (PSPV) beauftragt. Das VBS hat dazu eine interdepartementale Arbeitsgruppe eingesetzt, deren Entwurf für die Gesamtrevision der PSPV hauptsächlich folgende drei Aspekte betrifft: ein neues dreistufiges Sicherheitsprüfungsverfahren, die Wiederholung der Sicherheitsprüfung und eine neue Definition der Ämter und Funktionen, die nach einer Sicherheitsprüfung verlangen.

Aus datenschutzrechtlicher Sicht haben uns vor allem zwei Fragen interessiert. Erstens, da eine sehr hohe Anzahl von Personen einer Sicherheitsprüfung unterzogen werden, haben wir daran erinnert, dass bei der Behandlung von Personendaten grundsätzlich das Verhältnismässigkeitsprinzip zu wahren ist. Zweitens sieht die PSPV auf der Grundlage des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) die Einrichtung eines elektronischen Informationssystems für die Sicherheitsprüfungen vor. Dieses Informationssystem bedarf zwar keiner spezifischen Rechtsgrundlage, doch muss das VBS die PSPV relativ schnell ändern, insbesondere um die Liste der Personendaten einzufügen, die in dem obengenannten System bearbeitet werden sollen.

Die PSPV ist am 1. Januar 2002 in Kraft getreten. Wir werden unsere Begleit- und Beratungstätigkeiten fortsetzen, insbesondere bei der Ergänzung der erwähnten Liste.

3.1.3. Revision von Artikel 179quinquies StGB zum «Schutze des Geschäftsverkehrs»

Die Aufzeichnung von Telefongesprächen ohne die Einwilligung der daran beteiligten Personen ist nur erlaubt, wenn es sich um Notrufe beispielsweise auf die Notrufnummern 117 oder 118 handelt. Aufzeichnungen, die im Zusammenhang mit dem Geschäftsverkehr ohne die Kenntnis der betroffenen Personen vorgenommen werden, stellen eine ungerechtfertigte Verletzung der Privatsphäre dar.

Gemäss Artikel 179quinquies StGB ist ohne die Einwilligung der Beteiligten einzig die Aufzeichnung von Notrufen für Hilfs-, Rettungs- und Sicherheitsdienste nicht strafbar. Jede andere ohne Zustimmung der Beteiligten vorgenommene Aufzeichnung eines Telefongespräches ist auf Antrag strafbar. In Folge einer parlamentarischen Initiative betreffend die Revision von Artikel 179quinquies StGB zum «Schutze des Geschäftsverkehrs» beauftragte der Ständerat seine Kommission für Rechtsfragen mit der Ausarbeitung eines Gesetzesentwurfs. Zusammen mit dem Eidgenössischen Justiz- und Polizeidepartement schlug die besagte Kommission vor, die in Artikel 179quinquies StGB vorgesehene Ausnahme auf die Aufzeichnung von Fernmeldegesprächen unter Beteiligung einer Geschäftsperson auszudehnen, vorausgesetzt die Aufzeichnung dient einzig dazu, über den geschäftlichen Inhalt des Gesprächs Beweis zu führen.

Der in der gegenwärtigen strafgesetzlichen Bestimmung verwendete Begriff des «Notrufes» stellt die Hilfs-, Sicherheits- und Rettungsdienste vor das Problem, eine Aufzeichnung unterbrechen oder die betroffenen Personen über die Aufzeichnung des Gesprächs informieren zu müssen, wenn sich herausstellt, dass es sich bei dem Anruf nicht um einen Notruf handelt. Obgleich wir die Schwierigkeit dieser Situation erken-

nen, sind wir der Auffassung, dass der Lösungsvorschlag, grundsätzlich alle Fernmeldegespräche mit Hilfs-, Sicherheits- oder Rettungsdiensten aufzuzeichnen, weit über das Ziel hinaus schiesst. Der Revisionsentwurf erlaubt nämlich die Aufzeichnung von Fernmeldegesprächen mit sämtlichen Stellen der Hilfs-, Sicherheits- und Rettungsdienste (d.h. auch von Anrufen auf die Nummern von Verwaltungseinheiten, Auskunftsstellen oder auf die internen Nummern der Mitarbeiter dieser Dienste) unabhängig davon, ob es sich um einen Notruf handelt oder nicht. Aus der Sicht des Verhältnismässigkeitsprinzips darf sich die straffreie Aufzeichnung ohne die Einwilligung der Beteiligten nicht auf alle Anrufe beziehen. Die Aufzeichnung ohne Zustimmung der beteiligten Personen darf nur im Falle von Notrufen stattfinden, die beispielsweise bei den Notrufnummern 117 oder 118 eingehen.

Der Entwurf der Kommission für Rechtsfragen des Ständerats sieht ebenfalls die Möglichkeit vor, ein Fernmeldegespräch ohne vorherige Information der Beteiligten aufzuzeichnen, wenn einer der Beteiligten eine Geschäftsperson ist. Im Entwurf wird erläutert, dass die Aufzeichnung nur zur Beweisführung hinsichtlich des geschäftlichen Inhalts des Gesprächs oder zur Ausräumung eventueller Missverständnisse verwendet werden darf. Die Aufzeichnung eines Telefongesprächs, ohne den Gesprächspartner darüber in Kenntnis zu setzen, bildet eine Verletzung der Privatsphäre, die auch im Zusammenhang mit dem Geschäftsverkehr, mit geschäftlichen Verhandlungen oder dem Abschluss von Verträgen nicht gerechtfertigt ist. Die Aufzeichnung mit der Einwilligung aller Beteiligten reicht in der Geschäftswelt zur Beweisführung oder Ausräumung eventueller Missverständnisse vollkommen aus. Darüber hinaus liegt es durchaus im Interesse der Akteure des Wirtschaftslebens, minimale Anforderung für grössere Transparenz zu erfüllen, wenn sie auf ihr gutes Image Wert legen. Der Revisionsentwurf zu Artikel 179^{quinquies} StGB wird gegenwärtig durch das Parlament geprüft.

3.1.4. Revision der Verordnungen im Polizeiwesen

Zur Reform der Strukturen im Polizeibereich (StruPol) im Eidgenössischen Justiz- und Polizeidepartement war die Ausarbeitung neuer Verordnungen und die Änderung bestehender Verordnungen notwendig. Im Rahmen der Ämterkonsultation haben wir die Entwürfe geprüft und festgestellt, dass sie den datenschutzrechtlichen Anforderungen grösstenteils gerecht werden.

Wie bereits in unserem letzten Tätigkeitsbericht (S. 9 – 11) erwähnt, wurde in Folge des Reorganisationsprojektes (StruPol) des Eidgenössischen Justiz- und Polizeidepartements (EJPD) das Bundesamt für Polizei (BAP) umstrukturiert. Dazu waren Änderungen der Gesetzestexte notwendig, insbesondere der Bestimmungen über den Datenschutz. In diesem Zusammenhang haben wir mehrere Verordnungen des Bundesrates

geprüft, die alle insgesamt die datenschutzrechtlichen Anforderungen erfüllen. In den meisten Fällen waren daher keine Bemerkungen von unserer Seite notwendig, bzw. wurden die Unstimmigkeiten beseitigt.

In drei Fällen wurden die Unstimmigkeiten in unserer Stellungnahme an den Bundesrat erwähnt, der sich letztlich zugunsten des betroffenen Amtes aussprach. Im ersten Fall ging es um die Verordnung über Massnahmen zur Wahrung der inneren Sicherheit. Hierzu vertraten wir den Standpunkt, dass Informationen aus dem Ausland, welche die im BWIS festgelegten Bedingungen nicht erfüllen (unrichtige oder nicht notwendige Informationen), nicht einfach unbearbeitet abgelegt werden dürfen, sondern zu vernichten oder an den Absender zurückzusenden sind. Der zweite Fall betrifft die Verordnung über die Bearbeitung erkennungsdienstlicher Daten, für die wir forderten, dass bei Freispruch die Löschung der Daten nicht auf Gesuch der betroffenen Person sondern automatisch erfolgen sollte. Im dritten Fall ging es um die Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS-Verordnung), die eine in unseren Augen unverhältnismässig lange Datenaufbewahrungsdauer von acht Jahren vorsieht.

Im Rahmen der Ämterkonsultation zur Verordnung über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei, welche die Verordnung über kriminalpolizeiliche Zentralstellen im Bundesamt für Polizeiwesen ersetzt, vertraten wir die Auffassung, dass die Aufgaben der Bundeskriminalpolizei (BKP) ähnlich wie die der ehemaligen kriminalpolizeilichen Zentralstellen des Bundes in einem formellen Gesetz geregelt werden sollten. Das BAP hat sich verpflichtet, demnächst ein solches Gesetz auszuarbeiten.

3.1.5. Weitergabe von Polizeidaten im Rahmen des G8-Gipfels in Genua

Die Sozialdemokratische Partei der Schweiz hat uns ersucht, die Voraussetzungen zu prüfen, unter welchen die schweizerischen Behörden den italienischen Behörden im Rahmen des G8-Gipfels in Genua Polizeidaten übermittelten. Wir nahmen eine rechtliche Analyse der Lage vor und führten beim Bundesamt für Polizei zwei Kontrollen durch. Wir stellten fest, dass die Weitergabe gesetzeskonform erfolgte.

Die schweizerische sozialdemokratische Partei wandte sich per Schreiben vom 18. Juli 2001 an uns im Zusammenhang mit der Übermittlung von Personendaten durch das Bundesamt für Polizei (BAP) an die italienischen Behörden im Zusammenhang mit dem G8-Gipfel in Genua. Die sozialdemokratische Partei wollte insbesondere erfahren, nach welchen Kriterien der Begriff gewalttätiger Globalisierungsgegner definiert wur-

de. Ausserdem erkundigte sie sich nach der Herkunft der an die italienischen Behörden weitergeleiteten Daten, nach den Gesetzesgrundlagen der Datenübermittlung und nach den Datenschutzgarantien bei dieser Bearbeitung.

Bei der Prüfung des Gesuchs führten wir zunächst eine detaillierte rechtliche Analyse der Situation durch. Anschliessend fanden zwei Kontrollen direkt beim BAP statt. Ausserdem ersuchten wir die italienische Datenschutzbehörde, die Bearbeitung der vom BAP gelieferten Personendaten durch die italienischen Polizeibehörden im Rahmen ihrer Befugnisse zu prüfen. Dieses Gesuch wird derzeit noch bearbeitet.

Aus unserer rechtlichen Analyse ging hervor, dass der Dienst für Analyse und Prävention (DAP) des BAP für die Datenregistrierung im Staatsschutz-Informations-System (ISIS) verantwortlich ist. Die Registrierung muss in Übereinstimmung mit den Bestimmungen des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) und der ISIS-Verordnung erfolgen. Dabei muss der DAP insbesondere die genauen Kriterien definieren, die eine Registrierung gemäss dem BWIS rechtfertigen. Die Datenbearbeitungsvorgänge werden auf mehreren Ebenen kontrolliert: interne Kontrollstelle des DAP, Eidgenössisches Justiz- und Polizeidepartement, Delegation der Geschäftsprüfungskommissionen und Eidgenössischer Datenschutzbeauftragter. Wir wiesen darauf hin, dass Personen, die auf nicht gewalttätige Weise und ohne Delikte zu begehen an einer Demonstration teilnehmen, nicht im ISIS registriert werden dürfen. Zur Weitergabe der Daten zeigt unsere Analyse, dass die übermittelten Daten aus dem ISIS stammen und dass die Weitergabe nur im Einklang mit Artikel 17 Absätzen 3 bis 5 bzw. 7 BWIS erfolgen kann. Der DAP ist für die Rechtmässigkeit der Weitergabe an ausländische Behörden verantwortlich. Die Weitergabe der Daten sowie ihr Adressat, Gegenstand und Grund müssen im ISIS registriert werden. Auf der Grundlage der Registrierung kann die Einhaltung der gesetzlichen Bestimmungen untersucht werden. Der Datenempfänger darf sie nur zu den Zwecken, für welche sie übermittelt wurden, verwenden. Er wird über die Grenzen der Verwendung informiert. Der DAP kann Auskunft über die vorgenommene Datenverwendung verlangen. Kontrollen beim Empfängerland dürfen nur durch die Datenschutzbehörden des fraglichen Staates durchgeführt werden, sofern solche existieren, was in Italien der Fall ist.

Im Anschluss an die rechtliche Analyse führten wir am 24. Juli und am 9. August 2001 zwei Kontrollen in den Räumlichkeiten des DAP durch. Dabei überprüften wir, ob die italienischen Behörden den DAP tatsächlich um Informationen ersucht hatten, welche italienischen Behörden impliziert waren, welche Rolle der vom DAP nach Genua entsandte Verbindungsbeamte in der Datenweitergabe spielte, welche Daten weitergegeben wurden (Anzahl der betroffenen Personen oder Organisationen, Schweizer oder Ausländer usw.); wir prüften die Gesetzesgrundlagen der Datenweitergabe, die Einhaltung der Bestimmungen des BWIS und der ISIS-Verordnung sowie die Registrierung der

Übermittlungen im ISIS. Ausserdem kontrollierten wir, ob der DAP von den italienischen Behörden Personendaten erhalten hatte.

Der DAP stellte uns sämtliche Unterlagen (Akten und Auszüge aus dem ISIS) betreffend die Weitergabe von Personendaten an die italienischen Behörden zur Verfügung. Auch dem DAP übermittelte Informationen bzw. an den DAP gerichtete Gesuche wurden uns zugänglich gemacht.

Auf der Grundlage der vom DAP gelieferten detaillierten Informationen sowie unserer Feststellungen gelangten wir zum Schluss, dass die Übermittlung von Personendaten an die italienischen Behörden anlässlich des G8-Gipfels in Genua im gesetzlichen Rahmen laut Artikel 3 und 17 BWIS sowie Artikel 13 der ISIS-Verordnung erfolgte. Die Weitergabe war zur Wahrung erheblicher Sicherheitsinteressen der Schweiz oder des Empfängerstaates unerlässlich (Art. 17 Abs. 3 Buchst. d BWIS). Ausserdem wurden die Empfänger gemäss Artikel 13 Abs. 4 und 5 der ISIS-Verordnung über die Zuverlässigkeit und die Aktualität der Daten in Kenntnis gesetzt. Sie wurden darauf hingewiesen, dass die Daten nur für den Zweck verwendet werden dürfen, für den sie weitergegeben wurden. Die Weitergabe sowie ihr Adressat, Gegenstand und Grund wurden verordnungskonform im ISIS registriert. Die Daten wurden durch einen Verbindungsbeamten vor Ort oder in einem verschlüsselten Fax weitergegeben.

Anlässlich der Anhörung vom 21. August 2001 informierten wir die Delegation der Geschäftsprüfungskommissionen des Parlaments ausführlich über unsere Schritte in dieser Angelegenheit sowie über die Ergebnisse unserer Untersuchungen.

3.1.6. Das Schengener Abkommen aus dem Blickwinkel des Datenschutzes

Nachdem das Schengener Abkommen im Laufe des Jahres 2001 wegen der Verhandlungsmandate für den Beitritt der Schweiz an politischer Bedeutung gewann, befassten wir uns mit der Untersuchung des Abkommens aus dem Blickwinkel des Datenschutzes. Unsere Analyse ergab, dass die Schweiz hinsichtlich der einzuführenden Datenschutznormen die Anforderungen auf angemessene Weise erfüllt. Dagegen müssen vor dem Beitritt zum Schengener Abkommen noch bestimmte Probleme geprüft und mehrere Gesetzesänderungen vorgenommen werden.

Im Rahmen unserer Analyse erinnerten wir daran, dass ein Beitritt der Schweiz zum Schengener Abkommen Konsequenzen für den Datenschutz herbeiführen wird. So betonten wir, dass die Probleme im Zusammenhang mit dem Beitritt nicht als Schwächung des Datenschutzes wegen der Teilnahme an einem internationalen Zusammen-

arbeitssystem gesehen werden sollen; ein Beitritt bietet im Gegenteil für den Datenschutz den Vorteil, dass die für den Informationsaustausch mit den Vertragsparteien erforderliche Datenbearbeitungen in einen klar definierten und abgesteckten Rahmen gestellt würden, welcher anspruchsvollen und mit dem Standard der europäischen Datenschutzrechtes übereinstimmenden Anforderungen genügt. Der Beitritt würde - insbesondere wegen der strengen Begrenzung der möglichen Verwendungszwecke und Verwendungen der Daten - bessere Rahmenbedingungen für die Informationsflüsse und damit bessere Garantien für die betroffenen Personen schaffen.

In unserer Analyse wiesen wir auf drei Konsequenzen hin, die im Fall eines Beitritts der Schweiz zum Schengener Abkommen aus dem Blickwinkel des Datenschutzes zu berücksichtigen sind:

Erstens betonten wir, dass die Schweiz generell und auf Bundesebene den Gesetzesstandards und den Anforderungen, welche das Schengener Abkommen festlegt, genügt. Die Schweiz verfügt über ausreichende Rechtsnormen im Datenschutzbereich. Zu erwähnen sind im wesentlichen Artikel 13 der Bundesverfassung, welcher den Anspruch jeder Person auf Achtung ihrer Privatsphäre verankert, das Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, die Empfehlung Nr. (87) 15 über die Verwendung von personenbezogenen Daten im Polizeiwesen, das Bundesgesetz über den Datenschutz und die entsprechende Verordnung, die spezifischen formellen Gesetze zu den Polizei-Informatiksystemen, welche vom Schengener Abkommen betroffen sein könnten, sowie die diesbezüglichen Datenschutzbestimmungen.

Zweitens erstellten wir eine Liste der Probleme, die vor dem Beitritt zum Schengener Abkommen zu regeln sind. Die heikle Frage der Kantone – die durch den Beitritt zum Schengener Abkommen so oder so betroffen werden – sollte untersucht werden. Die meisten Kantone verfügen heute zwar über ein kantonales Datenschutzgesetz, aber nicht alle haben eine unabhängige Kontrollbehörde eingeführt. Die Effizienz variiert ausserdem je nach verfügbaren Strukturen und Mitteln sehr stark. Das Datenschutzniveau ist unter den Kantonen bzw. zwischen Bund und Kantonen bisweilen unterschiedlich. Daneben müssten mit Blick auf die Bestimmungen des Schengener Abkommens zur Verarbeitung von Personendaten die Situation in Bezug auf die verschiedenen schweizerischen Polizeidatenbanken genau beleuchtet werden. Es ist zu ermitteln, welche Informationssysteme betroffen sind (RIPOL, IPAS, AUPER, ZAR, ISIS, JANUS usw.). Ausserdem müssen die Informationsflüsse und die Zusammenschaltung zwischen den bestehenden Systemen und dem nationalen Schengener Informationssystem (SIS) bzw. dem gemeinsamen SIS als technischer Support präzise geregelt werden. Schliesslich ist darauf zu achten, dass für die Datenbearbeitung kraft des Schengener

Abkommens identische Datenschutzbestimmungen greifen, ganz gleich, ob die Daten aus Datensammlungen des Bundes oder aus kantonalen Datensammlungen stammen und ob die Bearbeitung durch Bundes- oder Kantonsorgane erfolgt.

Drittens zeigte unsere Analyse, dass bestimmte Gesetzesänderungen vorgenommen werden müssen, um Folgendes zu regeln: Schaffung eines nationalen schweizerischen SIS (Ausarbeitung einer formellen Gesetzesgrundlage), Verbindungen zwischen dem nationalen schweizerischen SIS und den übrigen Datenquellen (Datenbanken wie RIPOL, IPAS, AUPER, ZAR, ISIS, JANUS usw.), Beteiligung an einer oder mehreren internationalen Datenbanken, grenzüberschreitender Austausch von Polizeidaten, Mechanismen zur Kontrolle der Genauigkeit und der Qualität der Daten, Ausübung der Rechte der betroffenen Personen, vor allem des Auskunftsrechts (Abgrenzung zwischen direktem und indirektem Auskunftsrecht) und Informationsaustausch im Zusammenhang mit dem ergänzenden Verfahren SIRENE (Supplementary Information Request at the National Entry). Diese Gesetzesänderungen haben auch den Fragen im Zusammenhang mit den kantonalen Polizeikompetenzen (insbesondere der Polizeizusammenarbeit zwischen dem Bund und den Kantonen, Zugang zu SIS usw.), den Befugnissen der Datenschutzkontrollorgane (Eidgenössischer Datenschutzbeauftragter und kantonale Datenschutzbehörden) sowie der Mitwirkung des Eidgenössischen Datenschutzbeauftragten in der gemeinsamen Kontrollbehörde Rechnung zu tragen.

Aufgrund unserer Analyse gelangten wir zum Schluss, dass die Schweiz hinsichtlich der einzuführenden Datenschutznormen die Anforderungen auf angemessene Weise erfüllt. Um dem Schengener Abkommen beizutreten, müssen dagegen die oben erwähnten Probleme untersucht und die notwendigen Gesetzesänderungen in die Wege geleitet werden.

Die Ergebnisse und Schlussfolgerungen unserer Analyse wurden namentlich an die Koordinationsgruppe PESEUS (Projektgruppe-EJPD-Strategie-EU-Schweiz) des Eidgenössischen Justiz- und Polizeidepartements weitergeleitet. Ausserdem teilten wir unseren Standpunkt im Rahmen der Vernehmlassungsverfahren bezüglich Parlamentarischer Vorstösse zum Schengener Abkommen sowie bei unserer Anhörung durch die Aussenpolitische Kommission des Ständerates im August 2001 mit.

3.1.7. Geldwäscherei und Pflicht der Post Ausweispapiere zu kopieren

Die Post verlangt von den Inhabern und Inhaberinnen von Postcheckkonten einen amtlichen Ausweis, von dem sie eine Kopie aufbewahrt. Zu diesem Thema haben wir das im Anhang auf Seite 123 publizierte Informationsblatt «Die Post und das Geldwäschereigesetz» erstellt. Darin wird aufgezeigt, weshalb die Post gestützt auf das

Geldwäschereigesetz die amtlichen Identitätsausweise nicht nur zu prüfen, sondern auch deren wesentlichen Inhalt aufzunehmen und aufzubewahren hat.

3.2. Weitere Themen

3.2.1. Die Revision des Asylgesetzes

Die Revision des Asylgesetzes sieht die Möglichkeit vor, zur Klärung von Familienverhältnissen genetische Untersuchungen anzuordnen. Wir sind der Auffassung, dass dies unverhältnismässig ist. Wir wiesen darauf hin, dass zumindest verschiedene Punkte betreffend die genetischen Untersuchungen geregelt werden müssten.

Im Rahmen der Revision des Asylgesetzes wurden auch wir zur Stellungnahme aufgefordert. Dabei haben wir uns hauptsächlich zur vorgesehenen Einführung von genetischen Untersuchungen geäussert. Im Familienzusammenführungsverfahren geht es unter anderem darum, die genauen Familienverhältnisse zu klären. Dabei soll es nach der Revision des Asylgesetzes neu möglich sein, genetische Untersuchungen anzuordnen. Wir sind der Auffassung, dass dies unverhältnismässig ist. Zu bedenken ist dabei, dass genetische Untersuchungen für die betroffenen Personen einen äusserst schweren Eingriff in deren Persönlichkeit bedeutet. Weder aus dem Gesetzestext, noch aus den diesbezüglichen Erklärungen ergibt sich die Notwendigkeit der Durchführung einer solchen Massnahme. Zudem ist zu beachten, dass die betroffene Person keine Möglichkeit hat, sich der Durchführung einer genetischen Untersuchung zu widersetzen. Die Weigerung führt – gemäss Gesetzestext – dazu, dass in der Regel auf das Asylgesuch der betroffenen Person nicht eingetreten wird. Aus diesen Gründen lehnen wir die Einführung von genetischen Untersuchungen im Asylgesetz nachdrücklich ab.

Zudem führten wir diejenigen Punkte auf, die in der Revision berücksichtigt werden müssten, falls die Möglichkeit der Anordnung von genetischen Untersuchungen trotzdem beibehalten werden sollte. Zunächst müssten die verschiedenen zugelassenen genetischen Untersuchungen abschliessend aufgezählt werden. Je nach genetischer Untersuchung müssten zudem auf Gesetzesstufe verschiedene Modalitäten (handelt es sich beispielsweise um genetische Untersuchungen oder lediglich um DNA-Profile) geregelt werden. Das Gesetz müsste beispielsweise bei DNA-Analysen vorsehen, dass das Resultat nicht für einen anderen Zweck verwendet werden darf und unmittelbar nach Klärung des Familienverhältnisses vernichtet werden muss.

In den Erläuterungen wird auf den Vorentwurf des Bundesgesetzes über genetische Untersuchungen beim Menschen verwiesen. Dies erachten wir als nicht adäquat. Denn im Unterschied zum Asylgesetz geht der erwähnte Gesetzesvorentwurf von einer freien Einwilligung der betroffenen Person aus. Beim Asylgesetz kann, wie erwähnt, keine freie Einwilligung vorliegen, da bei einer Verweigerung auf das Gesuch der betroffenen Person nicht eingetreten wird.

3.2.2. Videoüberwachung im Hauptbahnhof Zürich

Im Herbst 2001 haben wir die Videoüberwachungsanlagen der SBB im stark frequentierten Zürcher Hauptbahnhof einer Kontrolle unterzogen. Die Überwachung ist für die Passanten nicht transparent. Die unterschiedlich gut sichtbaren rund 100 Kameras selbst lassen eine Überwachung erahnen, eine weitere Information etwa mit Hinweisschildern fehlt jedoch gänzlich.

Die Videoüberwachung erlebt in letzter Zeit einen regelrechten Boom. Auf den ersten Blick stellt sie ein Patentrezept zum Erlangen von Sicherheit für Personen und zur Verhinderung von Sachbeschädigungen dar, potenzielle Delinquenten werden abgeschreckt und im Notfall ist Hilfeleistung leichter zu organisieren. Allerdings ist für uns keineswegs erwiesen, dass mehr Videoüberwachung automatisch mehr Sicherheit bringt.

Ausgehend von den allgemeinen Datenschutzprinzipien darf die Videoüberwachung nur dann eingesetzt werden, wenn sie nötig und geeignet ist, die verfolgten Zwecke zu erreichen. Wenn dieser Zweck durch einen weniger tiefen Eingriff in die Persönlichkeit der betroffenen Personen erreicht werden kann, ist die Videoüberwachung unzulässig. Angemessene technische und organisatorische Massnahmen sind gegen die unbefugte Bearbeitung der Videodaten zu ergreifen. Derartige Überwachungsmassnahmen müssen also sorgfältig abgewogen werden.

Wir wählten den Hauptbahnhof Zürich für eine Kontrolle, da hier ein grosser Publikumsverkehr herrscht und umfangreiche Videoüberwachungsanlagen existieren. Die Kontrolle umfasste lediglich die Videoüberwachungsanlagen der Schweizerischen Bundesbahnen (SBB) sowie die Bekanntgabe von Personendaten, die mit dieser Anlage erhoben wurden, an Dritte.

Im Folgenden erwähnen wir die Videoanlage «Knoten Zürich» und diejenige des Bahnreisezentrums der SBB, die sich beide in öffentlich zugänglichen Bereichen befinden.

Neben einiger Kameras umliegender Bahnhöfe, die an der Anlage «Knoten Zürich» angeschlossen sind, sind allein im Hauptbahnhof selber über 80 Kameras (Tiefbahnhof, Passagen, Zutritt Nordtrakt und zentrale Anlieferung) in Verantwortung der SBB Divisi-

on Infrastruktur in Betrieb. Die Anlage wurde von der Kantonspolizei Zürich erstellt, die selber Zugriff auf einen Teil der Kameras hat und als Mitbetreiberin der Anlage anzusehen ist. Eine Aufzeichnung findet bei dieser Anlage seitens der SBB nicht statt. Es existiert auch keine Verbindung zu einer Datensammlung. Die Transparenz für die betroffenen Personen ist sehr niedrig, Hinweisschilder oder ähnliches sind nicht vorhanden. Die Kameras sind teilweise schlecht ersichtlich und nur bei genauerem Hinsehen erkennbar. Die Betroffenen wissen nicht, welchem Zweck die Anlage dient, wer Zugang zu den Bildern hat, ob eine Aufzeichnung stattfindet und ob die Anlage mit einer Datensammlung verbunden ist.

Eine weitere Videoanlage ist im Bahnreisezentrum installiert, welche die Fahrkartenschalter sowie das Reisebüro zusätzlich mit 16 fix montierten Farbkameras überwacht. Die Bilddaten aller Kameras werden mit einem speziellen System auf Videokassetten aufgezeichnet. Der Raum, in dem das Aufzeichnungssystem installiert ist, ist abgeschlossen. Es arbeitet kein Personal in diesem Raum. Eine Echtzeit-Visionierung im Kontrollraum ist technisch möglich, findet aber normalerweise nicht statt. Tritt ein Ereignis ein, wird die Polizei avisiert. Ein Mitarbeiter der Kantonspolizei, der Zugang zum Überwachungssystem hat, holt die aktuelle Videokassette ab, um eine Auswertung des Bildmaterials vorzunehmen. Verantwortlich für diese Anlage ist die Division Personenverkehr der SBB. Die Kameras sind besser ersichtlich als diejenigen im Knoten Zürich, aber auch hier fehlen jegliche Hinweisschilder. So ist den Betroffenen insbesondere die Tatsache verborgen, dass eine Bildaufzeichnung erfolgt.

Für keine der durch die SBB betriebenen Videoüberwachungsanlagen besteht eine ausdrückliche gesetzliche Grundlage. Im Eisenbahngesetz und im SBB-Gesetz ist eine allgemeine Grundlage vorhanden. Eine konkretere gesetzliche Grundlage ist in Vorbereitung.

Inwiefern die untersuchten Videoüberwachungsanlagen den gewünschten Zweck erreichen und ob dieser nicht auch mit anderen Massnahmen, die weniger stark in die Persönlichkeit der betroffenen Personen eingreifen, erreicht werden kann, konnte bisher nicht abschliessend geklärt werden. Für jede konkrete Gefahrenstelle muss sorgfältig analysiert werden, welche Massnahmen zur Minimierung der Risiken ergriffen werden, um insbesondere die Zweck- und Verhältnismässigkeit zu klären. Bei Redaktionsschluss dieses Tätigkeitsberichts lag der definitive Kontrollbericht noch nicht vor, da der Sachverhalt bei der Kontrolle nicht abschliessend festgestellt werden konnte. Wir warten noch auf Antworten zu dem von uns zusätzlich gestellten Fragekatalog.

4. IT und Telekommunikation

4.1. Erhebung von Radio- und Fernsehgebühren

Die Erhebung der Radio- und Fernsehgebühren warf auch in diesem Berichtsjahr erneut Datenschutzfragen auf. Neben kleineren Anfragen ging es einerseits um einen von der Inkassostelle Billag gewünschten erleichterten Zugriff auf kommunale Adressdaten sowie um Datenbearbeitungen im Zusammenhang mit der Gebührenbefreiung von Bezügerinnen und Bezügern von AHV/IV-Ergänzungsleistungen.

Die vom Bund beauftragte Inkassostelle Billag hat uns über Schwierigkeiten bei der Beschaffung von Adressdaten informiert und uns gebeten, diesbezüglich nach Erleichterungen für die Kontaktierung der Gebührenpflichtigen zu suchen. Insbesondere möchte die Billag einen besseren Zugang zu Einwohnerdaten der Gemeinden.

Die Datenbearbeitungen kantonaler oder kommunaler Behörden unterliegen deren eigenen Datenschutzbestimmungen und werden somit auch nicht von uns beaufsichtigt. Gemäss den aktuellen gesetzlichen Grundlagen des Bundes erteilen die kommunalen und kantonalen Behörden dem BAKOM oder der Inkassostelle auf Anfrage Auskunft über Namen und Adresse von registrierten Personen für punktuelle Kontrollen über die Einhaltung der Meldepflicht. Eine regelmässige Bekanntgabe von Adressen (beispielsweise der Neuzuzüger einer Gemeinde) ist in der heutigen Radio- und Fernsehgesetzgebung nicht abgedeckt.

Wir unterstützen Bestrebungen, welche es der Billag ermöglichen, das Gebühreninkasso zu erleichtern und somit namentlich der SRG SSR idée suisse die für ihren gesetzlichen Auftrag nötigen finanziellen Mittel zukommen zu lassen. Eine Lösung, die wohl in einer Anpassung der gesetzlichen Bestimmungen liegen wird, muss sich jedoch im Rahmen der allgemeinen Datenschutzgrundsätze, insbesondere der Verhältnismässigkeit, bewegen. Wir wurden zu dieser Problematik zu einem Gespräch mit dem BAKOM, der Billag, der Swisscom und der SRG gebeten, das im März 2002 stattfand

Das Bundesgericht entschied im Januar 2001, dass jeder Bezug von AHV- oder IV-Ergänzungsleistungen des Bundes – unabhängig von deren Höhe oder anderer Bedingungen – zu einer Gebührenbefreiung führt. In der Folge wurde die Radio- und Fernsehverordnung per 1. August entsprechend angepasst. Auf schriftliches Gesuch hin werden AHV- oder IV-Berechtigte, die Leistungen nach dem Bundesgesetz über Ergänzungsleistungen zur AHV und IV erhalten, von der Gebührenpflicht befreit. Gesuchstellende haben der Inkassostelle Billag einen rechtskräftigen Entscheid über den Anspruch auf Ergänzungsleistung beizubringen. Diese Regelung ist aus Sicht des Datenschutzes zu begrüssen, da keine weiteren Daten über die wirtschaftlichen Verhältnis-

se oder gar Daten über die Gesundheit an die Inkassostelle bekannt gegeben müssen. Allerdings ersehen wir aus mehreren Rückmeldungen, dass offensichtlich Unklarheiten bestehen. Betroffene haben uns mitgeteilt, sie seien (z.B. von ihrer Gemeinde) aufgefordert worden, zur Gebührenbefreiung die vollständige Ergänzungsleistungsverfügung an die Inkassostelle zu senden. Zu begrüssen wäre die Schaffung eines schweizweit einheitlichen Formulars, auf dem die zuständige kommunale oder kantonale Behörde lediglich bestätigt, dass die Betroffenen Ergänzungsleistungen des Bundes bezieht und somit ein Anspruch auf Gebührenbefreiung besteht.

5. Gesundheit

5.1. Verschiedene Themen

5.1.1. Mindestanforderungen für die Einführung einer Gesundheitskarte

Anlässlich einer vom Eidgenössischen Departement des Inneren organisierten Tagung wurden verschiedene Szenarien für die Einführung einer Gesundheitskarte in der Schweiz geprüft. Unabhängig vom Modell, das letztlich gewählt wird, hängen die Einführung und die Akzeptanz einer Gesundheitskarte weitgehend davon ab, wie die Datenschutzauflagen erfüllt werden. Wir äusserten uns bei dieser Gelegenheit zu den wichtigsten Kriterien, die es zu berücksichtigen gilt.

Die vom EDI am 30. August 2001 organisierte Tagung zum Thema Gesundheitskarte verfolgte das Ziel, einen Konsens über Zweck, System und Inhalt einer Karte sowie über die diesbezügliche Rolle des Bundes zu erzielen. Verschiedene Szenarien wurden untersucht (siehe http://www.hospvd.ch/public/ise/carte_sante/). Der Bund wird eine Rolle in der Koordination und Zusammenarbeit mit allen interessierten Partnern spielen. Zu fördern ist insbesondere die Vereinfachung der Bearbeitung von Versichertendaten. Zunächst sollte die Gesundheitskarte im Minimum die Versichertenadministration erleichtern und so zu Einsparungen führen. So wird empfohlen, als erster Schritt eine Karte zur Identifikation der Versicherten einzuführen, welche Zugriff auf die Stammdaten ermöglicht (Name, Vorname, Krankenversicherer, Versicherungstyp usw.). Diese Karte sollte freiwillig sein. Längerfristig könnte ein globales System für den Transfer und den Zugriff auf medizinische Daten entwickelt werden. Dazu müssen Studien und Untersuchungen durchgeführt werden, um die Vor- und Nachteile des Systems für die betroffenen Personen abzuwägen.

Nach unserer Auffassung darf eine Gesundheitskarte nicht unter beliebigen Voraus-

setzungen eingeführt werden. Es ist vor allem unverzichtbar, dass die Datenschutzauflagen von Anfang an berücksichtigt und dass das Grundrecht jeder Person auf Selbstbestimmung im Informationsbereich umfassend gewahrt werden. Zumal nicht fest steht, dass die Gesundheitskarte unbedingt zu einer besseren Achtung der Persönlichkeitsrechte des Patienten in der Bearbeitung seiner Personendaten und insbesondere im Informationsfluss zwischen Leistungserbringern (Ärzten, Spitälern usw.) und Versicherern führt, gaben wir eine bedingte Stellungnahme zu den Szenarien ab, die anlässlich der Tagung vorgetragen wurden. Besondere Aufmerksamkeit ist dem Inhalt der Karte und deren Verwendungszwecken zu widmen. Insofern müssen bei der Einführung einer Gesundheitskarte vor allem folgende Voraussetzungen erfüllt sein:

- Demokratische Basis: Schaffung der erforderlichen Rechtsgrundlagen in einem formalen Gesetz.
- Achtung des Rechts des Einzelnen, über seine Daten bestimmen zu können. Deshalb muss die Karte freiwillig sein. Patienten/Versicherte, die auf die Karte verzichten, dürfen nicht benachteiligt werden. Ausserdem müssen die Patienten/Versicherten den Kartentyp frei auswählen können (Versichertenkarte und/oder Karte mit Zugriff auf medizinische Daten).
- Klare Definition der gespeicherten Daten auf der Gesundheitskarte. Die Karte ist zur Identifikation des Patienten bzw. des Versicherten, gegebenenfalls zum Zugriff auf weitere Datenbanken, zu konzipieren; sie darf keine medizinischen Daten, sondern nur Daten zur Identifikation der betroffenen Person sowie administrative Daten enthalten.
- Gewährleistung der Transparenz in der Bearbeitung von Personendaten. Die betroffenen Personen müssen über die auf der Karte gespeicherten Daten, die Verwendung, die verfolgten Zwecke sowie über die Personen, die Zugang zu diesen Informationen haben, umfassend informiert werden und auch über die technischen Merkmale der Karte Bescheid wissen.
- Garantie des Zugriffs der betroffenen Personen auf ihre Daten. Betroffene Personen müssen jederzeit auf den Karteninhalt, auf Speicherdaten in mit der Kartennutzung verbundenen Datenbanken sowie auf die entsprechenden Bearbeitungen zugreifen können. Ausserdem müssen sie eine Berichtigung oder Löschung falscher Daten erwirken können.
- Klare Definition der Zugriffsrechte, falls die Karte zum Zugriff auf Datenbanken verwendet wird. Die Zugriffsrechte müssen so geregelt werden, dass die verschiedenen Beteiligten nur auf die zur Aufgabenerfüllung erforderlichen Daten zugreifen können und dass das Arztgeheimnis gewahrt bleibt.

- Gewährleistung der Datensicherheit bei der Bekanntgabe und bei der Speicherung von Daten.
- Konfiguration der Gesundheitskarte und Bearbeitung der entsprechenden Personendaten unter Einsatz von datenschutzfreundlichen Technologien und Pseudonymisierungs-Techniken, insbesondere in den Datenflüssen zwischen Leistungserbringern und Versicherern.

Wir ziehen ein Szenario vor, das die freiwillige Nutzung der Karte gewährleistet. Der Bund sollte die Möglichkeit haben, den technischen Standard der Karte sowie die Auflagen betreffend den Datenschutz und den selektiven Datenzugang festzulegen.

5.1.2. Aufbewahrung von Patientendaten im Privatbereich

Für Berufe des Gesundheitswesens ist in den kantonalen Gesundheitsgesetzen in der Regel eine Aufbewahrungsfrist für die Patientendossiers festgelegt. Besteht weder eine berufsspezifische noch sonst eine ausdrückliche gesetzliche Bestimmung, so bestimmt sich die Dauer der Aufbewahrung fallweise nach dem Grundsatz der Verhältnismässigkeit, d.h. die Unterlagen sind so lange aufzubewahren, wie dies notwendig und zweckmässig erscheint. Für den Privatbereich kann aus Beweissicherungsgründen gestützt auf die allgemeine obligationenrechtliche Verjährungsfrist eine Aufbewahrungsdauer von zehn Jahren als angemessen vermutet werden.

Wir wurden verschiedentlich mit der Frage konfrontiert, wie lange Patientendossiers aufbewahrt werden müssen bzw. dürfen. Diese Frage ist sowohl für diejenigen, die Patientendossiers führen, wie auch für die betroffenen Personen von Bedeutung, da diese Dossiers Angaben über die Gesundheit der behandelten Person enthalten, welche als besonders schützenswerte Daten im Sinne des Bundesgesetzes über den Datenschutz (DSG) gelten.

Wer in Berufen des Gesundheitswesens tätig ist, findet in der Regel eine ausdrückliche Aufbewahrungsfrist im entsprechenden kantonalen Gesundheitsgesetz bzw. in einer der dazu gehörenden Verordnungen. In zahlreichen Kantonen gilt im Privatbereich (z.B. Privatspital, Arztpraxis) für die meisten Medizinalberufe eine Aufbewahrungsfrist von zehn Jahren. Im öffentlichen Bereich (z.B. Kantonsspitälern) ist diese Frist oft länger und kann 20 Jahre oder mehr betragen.

Wer in Berufen tätig ist, für die keine spezifische Regelung bezüglich Aufbewahrungsdauer besteht, muss sich nach allgemeinen Bestimmungen richten. Solche Bestimmungen betreffend die Aufbewahrung von Akten (z.B. Aufbewahrung von Geschäftsbüchern) finden sich u.a. im Obligationenrecht. Hier beträgt die Frist ebenfalls zehn

Jahre. Wenn es um die Bearbeitung von Personendaten geht – wozu auch die Aufbewahrung gehört – so verweisen die meisten Gesetze direkt auf das DSG, welches jedoch keine ausdrücklichen Aufbewahrungsfristen enthält. Die zweckmässige Aufbewahrungsfrist muss somit im Einzelfall gestützt auf den Grundsatz der Verhältnismässigkeit (Art. 4 DSG) bestimmt werden. Personendaten dürfen einerseits nicht zu früh vernichtet, andererseits aber auch nicht einfach beliebig lange aufbewahrt werden. Begründen lässt sich die Pflicht zur Aufbewahrung von Patientendossiers unter anderem mit der Beweissicherung. Solange Verjährungsfristen laufen, kann es vorkommen, dass Unterlagen, z.B. im Rahmen eines Haftpflichtprozesses, als Beweismittel benötigt werden. Die allgemeine Verjährungsfrist beträgt zehn Jahre (Art. 127 OR). Es darf also vermutet werden, dass eine Aufbewahrungsfrist von zehn Jahren angemessen ist. Nach Ablauf dieser Frist ist anzunehmen, dass die Daten nicht mehr benötigt werden und vernichtet oder allenfalls anonymisiert werden müssen.

In Ausnahmefällen kann das Bedürfnis bestehen, Patientendossiers über die vorgeschriebene Aufbewahrungsfrist hinaus aufzubewahren. Dies ist z.B. in der Psychiatrie denkbar, wo bei einer Behandlung die frühere Krankengeschichte bedeutsam sein kann, selbst wenn die Patientin bzw. der Patient in der Zwischenzeit viele Jahre lang nicht in Behandlung war. Selbst wenn eine solche über die Verjährungsfrist hinaus gehende Aufbewahrung durchaus im Interesse der betroffenen Person sein kann, ist sie nicht ohne weiteres zulässig, sondern bedarf mindestens der stillschweigenden Einwilligung der betroffenen Person.

Schliesslich sei hier nochmals erwähnt, dass die Patientin bzw. der Patient jederzeit auf eigene Verantwortung die Herausgabe oder die Vernichtung seines Dossiers verlangen kann, denn die Dossiers enthalten seine Daten und die Aufbewahrung erfolgt in erster Linie in seinem Interesse. Ist die gesetzliche Aufbewahrungsfrist im Zeitpunkt der Herausgabe oder Vernichtung noch nicht abgelaufen, so muss der Patient diejenigen, die zur Aufbewahrung verpflichtet sind, schriftlich von dieser Pflicht befreien und auf Ansprüche aus dem Behandlungsvertrag verzichten, sofern er die Originale verlangt und verbietet, dass Kopien zu Beweiszwecken zurückbehalten werden (vgl. 8. Tätigkeitsbericht 2000/2001, S. 43ff).

5.1.3. Ungenügende Adressierung vertraulicher Postsendungen

Die versendende Stelle ist dafür verantwortlich, dass der Inhalt einer Sendung vertraulich bleibt. Bei der Zustellung von vertraulicher Post an Institutionen muss die Adressierung so genau sein, dass diese ungeöffnet zur zuständigen Person gelangt. Um dies zu gewährleisten, muss der Name der zuständigen Person in der Adresse erscheinen. Eine zu allgemein gehaltene

Adressierung kann dazu führen, dass eine vertrauliche Sendung von unzuständigen Personen geöffnet wird und diese unbefugt Kenntnis von deren Inhalt erhalten.

Wir wurden von einer Privatperson angefragt, ob eine Sendung mit vertraulichem Inhalt, die an eine Institution adressiert wird, in der Adresse den Namen des zuständigen Arztes und eine spezielle Kennzeichnung, wie «persönlich» oder «vertraulich», enthalten müsse. Im konkreten Fall hatte ein Labor einen Untersuchungsbefund an ein Spital gesandt, ohne in der Adresse den Namen des zuständigen Arztes zu erwähnen. Als allgemein ans Spital adressierte Sendung wurde der Umschlag wie normale Post behandelt, d.h. der Laborbefund gelangte offen in die interne Postverteilung.

Wir haben uns schon früher zu diesem Thema geäussert und festgehalten, dass die versendende Stelle dafür verantwortlich ist, dass der Inhalt einer Sendung vertraulich bleibt. Dies bedeutet, dass sie dafür sorgen muss, dass in der Adresse weder zu viele noch zu wenige Daten enthalten sind (vgl. 4. Tätigkeitsbericht 1996/97, S. 87ff). Fehlen der versendenden Stelle die notwendigen Angaben für eine korrekte Adressierung, so muss sie diese beim Empfänger erfragen. Dies gilt speziell dann, wenn es sich um eine vertrauliche Sendung handelt, was bei einer Laboranalyse immer der Fall ist. Es empfiehlt sich zudem, solche Sendungen mit dem Vermerk «vertraulich» oder «persönlich» zu kennzeichnen.

Die persönliche und vertrauliche Adressierung ist eine einfache aber wirkungsvolle Massnahme, die gewährleistet, dass vertrauliche Sendungen direkt zu den zuständigen Personen gelangen. Die betroffenen Personen, im vorliegenden Fall die Patienten, haben ein datenschutzrechtliches Interesse daran, dass die Anzahl der Personen, die ihre Gesundheitsdaten zur Kenntnis nehmen, möglichst klein bleibt. Dies gilt besonders innerhalb von grossen Institutionen, wie beispielsweise bei Versicherungen, Spitälern oder Ämtern. Die weit verbreitete Praxis, generell auf die persönliche Adressierung zu verzichten, ist bei Sendungen mit vertraulichem Inhalt aus datenschutzrechtlicher Sicht nicht haltbar, weil sich dadurch die Gefahr erhöht, dass das Patientengeheimnis verletzt wird. Die Tatsache, dass die Personen, die vom Inhalt Kenntnis nehmen, selber einer beruflichen Schweigepflicht unterstehen, ist dabei irrelevant.

5.1.4. Der Arzttarif Tarmed

In den Vertragsentwürfen zum Arzttarif Tarmed ist festgehalten, dass auf allen Arztrechnungen genaue Diagnosecodes anzugeben sind. Es handelt sich dabei um die so genannten ICD-10 Codes bzw. die damit kompatiblen ICPC-Codes. Die systematische Weitergabe von detaillierten Diagnoseangaben an die Versicherer ist jedoch mit dem Datenschutzgesetz nicht vereinbar. Wir sind zur Zeit daran, mit den verschiedenen Tarifpartnern nach datenschutzkonformen Lösungen zu suchen.

In den Tarifverträgen zum Tarmed ist vorgesehen, die Leistungserbringer zu verpflichten, den Versicherern Arztrechnungen mit genauen Diagnosecodes weiterzugeben. Dies betrifft den Krankenversicherungsbereich einerseits und den Militär-, Invaliden- und Unfallversicherungsbereich andererseits. Nebst den ICD-10 Codes sollen auch Diagnoseangaben nach ICPC auf den Arztrechnungen erscheinen. Wir haben uns bereits seit Jahren gegen die Weitergabe von ICD-10 Diagnosecodes an die Versicherer ausgesprochen (Verstoss gegen das Verhältnismässigkeitsprinzip). Die ICD-10 Kodierung wurde zu globalen Statistik- und Forschungszwecken geschaffen und ist nicht geeignet für die Kosten- und Wirtschaftlichkeitskontrolle (vgl. auch 8. Tätigkeitsbericht 2000/2001, S. 42). ICPC ist die Abkürzung für «International Classification of Primary Care» und ist grundsätzlich mit ICD vergleichbar. Tatsache ist, dass der Arzttarif Tarmed in der geplanten Version nicht den Anforderungen des Datenschutzgesetzes genügt. Insbesondere bekämen die Krankenversicherer umfassende Informationen über die Versicherten. Aufgrund der Vernetzung der einzelnen Versicherungen (Kranken-, Unfall-, Zusatz-, Lebensversicherungen etc.) würden somit die Persönlichkeits- und Patientenrechte der Versicherten verletzt.

Ein weiteres Problem im Zusammenhang mit Tarmed liegt in der elektronischen Rechnungsstellung. Es besteht die Gefahr, dass die Rechnungen direkt vom Leistungserbringer an die Versicherer weitergeleitet werden ohne Wissen der Patienten. Das sogenannte System des «Tiers garant», bei dem der Patient der Schuldner ist und selber entscheiden kann, ob er die Rechnung bezahlen will, wird auf diese Weise aufgehoben (vgl. auch 8. Tätigkeitsbericht 2000/2001, S. 40). Zusätzlich dürften die Datensicherheitsaspekte beim geplanten elektronischen Datenaustausch noch zu zusätzlichen Problemen führen.

Wir haben im Berichtsjahr sämtliche Tarifpartner eingeladen und diese aufgefordert, uns über den Stand des Projekts zu informieren, die Datenbedürfnisse konkret nachzuweisen und konstruktive Lösungsvorschläge zu unterbreiten. Gleichzeitig sind einzelne Gespräche mit diversen Fachleuten im Gange, um sich einen besseren Überblick zu verschaffen.

Unserer Ansicht nach sind Lösungen zu suchen, welche die Persönlichkeitsrechte der Versicherten wahren und die Entstehung des «gläsernen Patienten» verhindern. Eine Möglichkeit bestünde darin, dass die Versicherer die Patientendaten nicht in personenbezogener, sondern in «pseudonymisierter Form» erhalten. Auch anhand von pseudonymisierten Daten können die Versicherer die Rechnungen auf ihre Richtigkeit sowie die Wirtschaftlichkeit und Qualität der Leistungen überprüfen.

Schliesslich sei noch auf die Interpellation Sommaruga (01.3594) vom 5. Oktober 2001 verwiesen, welche sich kritisch zu den geplanten Diagnose-Codes äussert. In seiner Antwort sprich sich der Bundesrat klar gegen die systematische Weitergabe von detaillierten Diagnose-Codes an die Versicherer aus.

5.1.7. Publikation der Taxpunktwerte von Zahnärzten im Internet

Die Redaktion Kassensturz von SF DRS publizierte im August 2001 im Internet eine Liste von Taxpunktwerten, die sie bei rund tausend zufällig ausgesuchten Zahnärztinnen und -ärzten mittels verdeckter Recherche erhoben hatte. Da nach unserer Ansicht in diesem Falle die Beschaffung und die Publikation der Daten gegen die Grundsätze des Bundesgesetzes über den Datenschutz (DSG) verstiess, verlangten wir die Entfernung der Liste aus dem Internet.

Im Rahmen einer verdeckten Recherche erhob die Redaktion Kassensturz Taxpunktwerte von rund tausend zufällig ausgewählten Zahnärztinnen und -ärzten. Diese Werte wurden in einer Liste auf der Homepage der Redaktion Kassensturz publiziert. In der Liste sind Name, Postleitzahl, Ort, Kanton und Taxpunktwert bzw. die Anmerkung «k.A.» für «keine Antwort» enthalten. Wir sind der Ansicht, dass die Art und Weise der Datenerhebung gegen Treu und Glauben verstösst, weil die angerufenen Zahnärzte bezüglich der Identität der Anrufenden und des Zweckes der Datenerhebung im Unklaren gelassen bzw. falsch informiert wurden. Nach der heutigen Rechtslage sind Zahnärzte nicht verpflichtet, ihre Taxpunktwerte offen zu legen. In der Praxis sind diese Werte zwar soweit zugänglich, als die Zahnärzte sie in der Regel auf Anfrage hin bekannt geben. Dies bedeutet aber nicht, dass sie auch ohne weiteres, und insbesondere ohne Zustimmung der Betroffenen, in einem Massenmedium publiziert werden dürfen.

Die Redaktion Kassensturz machte für ihr Vorgehen den Rechtfertigungsgrund des überwiegenden öffentlichen Interesses an der Offenlegung dieser Werte geltend. Wir bezweifeln, dass das öffentliche Interesse im vorliegenden Fall überwiegt. Aber selbst wenn dieses Interesse als überwiegend eingestuft würde, müssten bei der Datenbearbeitung immer noch die Grundsätze des Bundesgesetzes über den Datenschutz eingehalten werden. Dazu gehört insbesondere das Prinzip der Verhältnismässigkeit. Die-

ses ist immer einzuhalten, auch dann, wenn ein Rechtfertigungsgrund für die Datenbearbeitung gegeben ist, im vorliegenden Falle also unabhängig davon, ob ein öffentliches Interesse die verdeckte Erhebung und die Publikation der Daten rechtfertigt oder nicht. Unserer Ansicht nach verstösst die Publikation der Taxpunktwerte in der erfolgten Form gegen diesen Grundsatz. Das Verhältnismässigkeitsprinzip verlangt unter anderem, dass bei Rechtseingriffen stets dasjenige Mittel zu wählen ist, welches am wenigstens in die Rechte der betroffenen Personen eingreift. Aus der Tatsache, dass der Gesetzgeber nur gewisse Dienstleistungsbereiche einer Preisbekanntgabepflicht unterstellt hat, können die anderen Bereiche, zu denen auch die Zahnärzte gehören, primär ein Recht auf Nichtoffenlegung ableiten. Wenn in dieses Recht aus Gründen des öffentlichen Interesses eingegriffen wird, so muss dies möglichst schonend erfolgen. Das Bedürfnis der Öffentlichkeit, über Taxpunktwerte der Zahnärzte informiert zu werden, hätte mittels einer Publikation der Umfrageergebnisse in anonymisierter Form, d.h. ohne Namensnennung, befriedigt werden können. Um den angestrebten Zweck zu erreichen, war die Namensnennung nicht notwendig.

In der Zwischenzeit wurde vom EVD die Revision der Preisbekanntgabeverordnung in die Wege geleitet. Damit wird die gesetzliche Grundlage für die transparente Veröffentlichung der Zahnarzttarife geschaffen.

5.1.6. Die Verwendung von medizinischen Daten bei klinikübergreifenden Qualitätssicherungsprojekten

Im Bereich der Chirurgie haben wir ein Projekt analysiert, welches den beteiligten Kliniken sowohl die Qualität ihrer eigenen Leistung messbar machen, als auch einen Vergleich mit dem Qualitätsniveau anderer Kliniken ermöglichen soll. Die Voraussetzungen zur Beschaffung und Bearbeitung von Gesundheitsdaten haben wir im 8. Tätigkeitsbericht 2000/2001, S. 75 beschrieben. Das vorliegende Beispiel behandelt mehrheitlich die organisatorischen Fragestellungen, die Richtigkeit der Daten und den Umgang mit einem Pseudonym.

Das Projekt hat zum Ziel, ein Verfahren zu implementieren, welches eine Qualitätsmessung und ein Benchmarking (qualitative Gegenüberstellung von vergleichbaren Bereichen) für chirurgische Kliniken ermöglicht. Das Verfahren gliedert sich in vier Phasen:

- Erhebungsphase: Die Daten werden von den beteiligten Kliniken auf einem Formular erfasst und per Post oder auf elektronischem Weg an eine zentrale Stelle gesendet.

- Korrekturphase: Die Angaben werden auf ihre Richtigkeit überprüft und gegebenenfalls zur Korrektur an die Klinik zurück gesendet.
- Erfassungsphase: Die geprüften Daten werden in die zentrale Datenbank eingegeben.
- Qualitätskontrollphase: Die bearbeiteten Daten werden jährlich den Kliniken auf CD-ROM zur Verfügung gestellt.

An jede Phase und vor allem an jeden Phasenwechsel werden vom Datenschutz spezifische Anforderungen gestellt:

- Erhebungsphase: Patientinnen und Patienten werden über den Zweck der Datenerfassung und die Datenweitergabe unterrichtet. Die Daten auf dem Formular dürfen keinen direkten Rückschluss auf eine Person zulassen, d.h. sie müssen pseudonymisiert sein. Es dürfen weder der Name, Geburtsdatum, Wohnadresse oder Nationalität auf dem Formular erwähnt werden. Das gewählte Pseudonym, eine Patientennummer, darf nur spitalintern bekannt sein.
- Erhebungsphase/Korrekturphase: Das Formular muss auf dem Postweg eingeschrieben an die Auswertzentrale geschickt werden. Die elektronische Übertragung hat verschlüsselt zu erfolgen (z.B. mit PGP, mindestens 1024 Bit).
- Korrekturphase: Für allfällige Korrekturen wird das Formular unter den gleichen Bedingungen wie oben beschrieben an die Klinik zurückgeschickt. Zusätzlich gilt die Anforderung, dass der Versand im 4-Augenprinzip zu erfolgen hat. Dadurch wird das Risiko einer Falschadressierung nahezu ausgeschlossen.
- Korrekturphase/Erfassungsphase: Die Formulare werden zur Erfassung in die zentrale Statistikdatenbank an Mitarbeiter der Auswertzentrale weitergegeben, welche nicht aus dem Einzugsgebiet der zu erfassenden Klinik kommen.
- Erfassungsphase: Die Daten der Kliniken müssen in separaten Datenbanken gespeichert werden, um eine unbeabsichtigte Vermischung der Daten zu verhindern.
- Qualitätskontrollphase: Die jährlich den Kliniken zur Verfügung gestellte CD-ROM darf nur die klinikeigenen Daten und die anonymisierten Falldaten der anderen beteiligten Kliniken enthalten. Alle Pseudonyme müssen aus den Datensätzen entfernt und Attribute, welche Rückschlüsse auf Personen oder andere Kliniken zulassen könnten, dürfen nicht verwendet werden.

Das Projekt zeigt wie wichtig es ist, die beteiligten Instanzen organisatorisch sauber voneinander zu trennen. Die Pseudonymisierung hat an der richtigen Stelle zu erfolgen und die Relationstabelle, welche die Verbindung zwischen Pseudonym und Person er-

möglicht, muss vor dem Zugriff von Drittpersonen geschützt werden (vgl. 8. Tätigkeitsbericht 2000/2001, S. 75).

Der elektronische und postalische Versand von besonders schützenswerten Personendaten hat sehr sorgfältig zu erfolgen (chiffriert, eingeschrieben, 4-Augenprinzip). Es muss verhindert werden, dass Beteiligte durch eine zufällige Kombination von Attributen eine Person wiedererkennen.

5.2. Genetik

5.2.1. Grundsätzliche Anforderungen für den Umgang mit genetischen Untersuchungen

Die Entschlüsselung des menschlichen Genoms stellt eine neue Herausforderung für den Gesetzgeber dar. Insbesondere gilt es, die informationelle Selbstbestimmung zu garantieren und jegliche Diskriminierung aufgrund des Erbgutes zu vermeiden. Nachfolgend sind einige wichtige Grundsätze des Datenschutzes wiedergegeben, die im Umgang mit genetischen Untersuchungen zu beachten sind.

Der Umgang mit genetischen Untersuchungen ist gesetzlich zu regeln. Für den Bereich der Strafverfolgung gibt es z.T. schon gesetzliche Grundlagen in der Schweiz. Für genetische Untersuchungen im Medizinal-, Arbeits-, Versicherungs-, und Haftpflichtbereich existiert ein Gesetzesentwurf, der in naher Zukunft vom Parlament behandelt werden dürfte.

Genetische Untersuchungen dürfen grundsätzlich nur auf freiwilliger Basis durchgeführt werden. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck ist zu vermeiden. Gentests sind nur dann zulässig, wenn die betroffene Person ihre Einwilligung dazu gegeben hat. Die freie und jederzeit widerrufbare Einwilligung ist erst dann rechtsgültig, wenn die betroffene Person eine umfassende genetische Beratung erhalten hat. Sie muss insbesondere über den Zweck der genetischen Untersuchung und die damit zusammenhängenden Risiken informiert werden.

Genetische Untersuchungen müssen zweckorientiert vorgenommen werden. Die verschiedenen Zwecke sind gesetzlich festzuhalten. Es ist dabei diejenige Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Diese sind sofort zu vernichten.

Der betroffenen Person steht auch das sogenannte Recht auf Nichtwissen zu und darf die Kenntnisnahme des Untersuchungsergebnisses verweigern. Dem Recht auf Nicht-

wissen kommt besondere Bedeutung zu, weil viele Erkrankungen bzw. Erkrankungsrisiken wohl diagnostizierbar aber noch nicht behandelbar sind.

Ein besonderer Schutz im Zusammenhang mit Gentests ist Minderjährigen und nicht Urteilsfähigen zu gewähren. Genetische Untersuchungen bei urteilsunfähigen Personen etwa dürfen nur dann durchgeführt werden, wenn sie zum Schutz ihrer Gesundheit absolut notwendig sind. Ausnahmsweise kann dies auch der Fall sein, wenn sich eine schwere Erbkrankheit in der Familie nicht anderweitig abklären lässt. Auf jeden Fall ist die Meinung des Urteilsunfähigen, soweit dies möglich ist, vorher einzuholen.

Im Bereich der pränatalen Diagnostik sollten nur Informationen über eine heilbare Schädigung erhoben werden können, oder wenn diese auf eine schwerwiegende Gesundheitsschädigung des Kindes schliessen lassen. Reihenuntersuchungen an Neugeborenen dürfen sich nur auf Erbdispositionen erstrecken, die geheilt werden können.

Im Arbeits- und Versicherungsbereich sind genetische Untersuchungen grundsätzlich zu untersagen. Mögliche Diskriminierungen sind gerade hier nicht auszuschliessen. Ausnahmen sollen nur erlaubt sein, wenn dies zwingend notwendig ist.

Es sind schliesslich Qualitätsstandards einzuführen, die den sicheren Umgang mit Gendaten garantieren. In einem solch sensiblen Bereich sind auch Straftatbestände zu schaffen.

Die vorgenannten Grundsätze sind nicht abschliessend, und die datenschutzrechtlichen Konsequenzen, welche die Entschlüsselung des menschlichen Genoms mit sich bringen, bedürfen weiterer Überlegungen.

5.2.2. Probleme in der Praxis mit genetischen Untersuchungen

Ein Fall aus der Praxis zeigt, dass es im Zusammenhang mit genetischen Untersuchungen zu datenschutzrechtlichen Problemen kam. Insbesondere war den betroffenen Personen unklar, für welchen Zweck die genetischen Informationen verwendet werden.

Konkret ging es um eine Familie, deren Erbanlagen ein Arzt untersuchen wollte. Die Familienmitglieder stimmten der genetischen Untersuchung vor allem deshalb zu, weil der Arzt damit eine ärztliche Betreuung versprochen haben soll. In der Folge soll der Arzt zur Familie nach Hause gegangen sein und sämtlichen Familienmitgliedern Blut abgenommen haben. Im Weiteren seien alle Familienmitglieder fotografiert worden. Eine Information über den Verwendungszweck der Blutproben bzw. der darin enthaltenen genetischen Informationen sowie der Fotos sei nicht erfolgt. Die ärztliche Betreuung habe – trotz mehrmaligen Nachfragen – in der Folge nicht stattgefunden.

Die Familienmitglieder fühlten sich in ihren Persönlichkeitsrechten verletzt. Sie baten den Arzt um einen sofortigen Unterbruch der Forschungsarbeiten und untersagten jegliche Verwendung und Weitergabe ihrer Daten. Im Weiteren verlangte die Familie vom Arzt einen ausführlichen Bericht über den Ablauf der Forschung, um das weitere Vorgehen festlegen zu können.

Der vorliegende Fall zeigt deutlich, dass vor allem die genetische Beratung noch ungenügend ist. Diesbezüglich besteht insbesondere bei der Ausbildung der Ärzte Handlungsbedarf.

Auch wenn das Bundesgesetz über genetische Untersuchungen noch nicht in Kraft ist, sind die andere Bestimmungen bereits heute anwendbar. Nebst dem Datenschutzgesetz und dem Strafgesetzbuch sei hier insbesondere auf die medizinisch-ethischen Richtlinien für genetische Untersuchungen am Menschen verwiesen. Diese Richtlinien wurden von der Schweizerischen Akademie der medizinischen Wissenschaften herausgegeben. Sie umschreiben die Rahmenbedingungen für das Vorgehen des Arztes und sind in vielen Punkten mit dem vorgenannten Gesetzes-Entwurf identisch. Insbesondere sehen die Richtlinien vor, dass genetische Untersuchungen von einer umfassenden genetischen Beratung begleitet sein müssen. Die Beratung und die damit zusammenhängende ärztliche Betreuung hat vor, während und nach der genetischen Untersuchung stattzufinden. Das Recht auf Nichtwissen und die jederzeit widerrufbare Einwilligung der betroffenen Person sind ebenfalls zentrale Elemente in den Richtlinien.

6. Versicherungen

6.1. Sozialversicherungen

6.1.1. Regelungslücken im medizinischen Datenschutz

Der Bundesrat und wir wurden in einem Postulat (Postulat Kommission Rechtsfragen NR 99.093) eingeladen, einen Bericht über Regelungslücken im medizinischen Datenschutz für den ganzen Sozialversicherungsbereich zu verfassen. Das Institut für Gesundheitsrecht der Universität Neuenburg wurde beauftragt, die umfangreichen Arbeiten an die Hand zu nehmen.

Ausgangspunkt ist das Postulat der Kommission für Rechtsfragen des Nationalrates vom 27. März 2000. Dieses forderte den Bundesrat und uns auf, einen Bericht auszuarbeiten, der den medizinischen Datenschutz im gesamten Sozialversicherungsbereich untersucht. Dabei ist insbesondere die technologische Entwicklung bei der elektroni-

schen Datenbearbeitung zu berücksichtigen. In die Überlegungen einzubeziehen ist auch der strafrechtliche Geheimnisschutz von Art. 321 StGB. Der Bericht soll dazu beitragen, die nötigen Grundlagen und Standards im medizinischen Datenschutz möglichst frühzeitig zu erkennen und zu schaffen. Mit dem Bericht wurde das Institut für Gesundheitsrecht der Universität Neuenburg beauftragt, welches eine langjährige Erfahrung in diesem Bereich mitbringt.

Aus unserer Sicht gilt es v.a. zu untersuchen, ob die gegenwärtigen Abläufe im Sozialversicherungsbereich mit dem Datenschutzgesetz im Einklang stehen oder allenfalls die geltenden Datenschutzbestimmungen angepasst werden müssen (vgl. auch 7. Tätigkeitsbericht 1999/2000, S. 38). Dabei soll die künftige Entwicklung im Sozialversicherungswesen miteinbezogen sowie Chancen und Missbrauchsgefahren aufgezeigt werden (E-Health, computerbasierte Patientendossier, Gesundheitskarte etc). Im Weiteren gilt es, die Risiken im Bereich der Datensicherheit darzulegen; auch sollen die Möglichkeiten der Technik gezeigt werden, die Risiken vermindern helfen (datenschutzfreundliche Technologien, Pseudonymisierung, Kryptotechniken, digitale Signatur etc.).

Aus unserer Sicht wesentlich ist zudem, das informationelle Selbstbestimmungsrecht der Versicherten zu stärken. Dazu sind etwa Massnahmen zu verstehen, die den Patienten einen sicheren und erleichterten Zugang zu ihren medizinischen Daten ermöglichen. Schliesslich sind es die Patienten, die entscheiden, wer wann und zu welchem Zweck auf ihre Daten zugreifen darf. Der Bericht soll Ende 2002 fertig sein und dürfte der Öffentlichkeit zu einem späteren Zeitpunkt zugänglich gemacht werden.

6.1.2. Die SUVA und die Datensammlung betreffend «auffällige Leistungserbringer»

Die SUVA führt eine Datensammlung zur «Erfassung von auffälligen Leistungserbringern». Wir sind zur Zeit daran, diese Datensammlung auf ihre Datenschutzkonformität hin zu überprüfen.

Die SUVA als Dateninhaberin führt eine Datensammlung mit dem Zweck, Rechnungen von «auffälligen Leistungserbringern bzw. Rechnungsstellern» vermehrt zu kontrollieren. Es handelt sich um eine automatisierte Datensammlung, die bei uns wohl angemeldet, aber noch nicht auf ihre Datenschutzkonformität hin überprüft wurde. Ein Bürger ist in dieser Datensammlung registriert und wandte sich an uns, mit der Bitte, diese datenschutzrechtlich zu untersuchen.

Wir überwachen die Einhaltung des Datenschutzgesetzes (DSG) und der übrigen Datenschutzvorschriften des Bundes durch die Bundesorgane. Die SUVA ist als Bundesorgan im Sinne des DSG zu betrachten. Wir klären von uns aus oder auf Meldung Dritter

hin den Sachverhalt näher ab. Bei der Abklärung können wir Akten herausverlangen, Auskünfte einholen und uns Datenbearbeitungen vorführen lassen, wobei die Bundesorgane an der Feststellung des Sachverhaltes mitwirken müssen.

Die erwähnte Datensammlung nennt sich «MediData-Anwendung: Intregrale Kontrolle der Leistungserbringer». Zu den Kategorien der Datenempfänger gehören «MediData-Anwender».

Unklar ist einerseits, auf welche Rechtsgrundlagen sich die Datensammlung abstützt. Andererseits ist der Begriff der «auffälligen Leistungserbringer» und der «MediData-Anwender» nicht verständlich bzw. der genaue Zweck der Datensammlung nicht nachvollziehbar. Diesbezüglich stellt sich die Frage, ob die Erfassung von «auffälligen Leistungserbringern» tatsächlich geeignet und notwendig ist (Prinzip der Verhältnismässigkeit). Im Weiteren ist nicht geklärt, welche Daten und wie lange diese in der erwähnten Datensammlung aufbewahrt werden.

6.1.3. Merkblatt zum Thema «Austritts- und Operationsberichte»

In der Praxis gibt es häufig Probleme im Zusammenhang mit Austritts- und Operationsberichten. Die Versicherer verlangen von den Spitälern in der Regel vollständige Austritts- und Operationsberichte, um die Beurteilung ihrer Leistungspflicht abklären zu können. Diese Praxis ist jedoch mit dem Prinzip der Verhältnismässigkeit nicht vereinbar. Die Vereinigung der Schweizerischen Datenschutzbeauftragten hat aus diesem Grunde ein Merkblatt zu diesem Thema veröffentlicht (siehe im Anhang S. 120).

6.1.4. Staatsverträge im Bereich der sozialen Sicherheit und Datenschutzklausel

Im Bereich der sozialen Sicherheit werden regelmässig Staatsverträge zwischen der Schweiz und anderen Staaten abgeschlossen. Damit verbunden ist auch ein Datenaustausch von Sozialversicherungsdaten. Diese Weitergabe muss vor allem dann in einer besonderen Datenschutzklausel geregelt werden, wenn Personendaten aus der Schweiz in Länder ohne einen gleichwertigen Datenschutz übermittelt werden. Eine «Muster-Datenschutzklausel» befindet sich im Anhang auf Seite 122.

6.2. Privatversicherungen

6.2.1. Gesundheitsfragen im Zusatzversicherungsbereich

In der Praxis ist es üblich, dass Krankenversicherer nebst der sozialen Krankenversicherung auch Zusatzversicherungen anbieten. Die Krankenversicherer dürfen die Aufnahme in eine Zusatzversicherung vom Gesundheitszustand des Antragstellers abhängig machen. Gegen das Verhältnismässigkeitsprinzip verstösst es jedoch, wenn für sämtliche Zusatzversicherungen dieselben Gesundheitsfragen gestellt werden.

In der Praxis wurden wir mehrmals darauf aufmerksam gemacht, dass die Krankenversicherer für die verschiedenen Zusatzversicherungen dieselben Gesundheitsfragen stellen, obwohl der Inhalt wie auch die Leistungen der einzelnen Zusatzversicherungen sehr unterschiedlich sind.

Verlangt ein Krankenversicherer im Aufnahmeverfahren Gesundheitsangaben für die obligatorische Krankenpflegeversicherung, verstösst dies gegen das KVG und das DSG. Jeder Krankenversicherer ist verpflichtet, eine Person – unabhängig von deren Gesundheitszustand – in die obligatorische Krankenversicherung aufzunehmen (vgl. auch 6. Tätigkeitsbericht 1998/99, S. 72).

Hingegen kann die Aufnahme in die Zusatzversicherung vom Gesundheitszustand des Antragstellers abhängig gemacht werden. Die Zusatzversicherungen unterliegen – wie auch die übrigen Privatversicherungen – dem Versicherungsvertragsgesetz (VVG). Zu den Zusatzversicherungen gehören Versicherungen, die Leistungen anbieten, die über die Grundversicherung hinausgehen. So bieten z.B. Zusatzversicherungen alternative Heilmethoden bzw. gesundheitsfördernde und präventive Massnahmen an. Auch existieren Reise- und Ferienversicherungen, die Heilungskosten abdecken, die bei Krankheit oder Unfall im Ausland entstehen können. Schliesslich gibt es Zahnbehandlungsversicherungen, die Leistungen offerieren, welche die obligatorische Krankenpflegeversicherungen nicht anbieten. Dazu gehören etwa konservierende Zahnbehandlungen, Paradontal-Behandlungen oder zahnprothetische Arbeiten.

Die vorgenannten Beispiele zeigen, dass die Art und der Leistungskatalog der einzelnen Zusatzversicherungen erheblich variieren. Die Krankenversicherer dürfen nach dem Verhältnismässigkeitsprinzip nur diejenigen Personendaten beschaffen, die für die einzelne Zusatzversicherung tatsächlich erforderlich und geeignet sind. Die Angaben müssen demnach für die Risikobeurteilung in der jeweiligen Zusatzversicherung notwendig sein.

In der Praxis ist es jedoch die Regel, dass für die Aufnahme in die verschiedenen Zusatzversicherungen genau derselbe Fragebogen mit z.T. sehr detaillierten Fragen verwendet wird. Dies ist mit dem Verhältnismässigkeitsprinzip nicht vereinbar. Aus diesem Prinzip lassen sich insbesondere die Grundsätze der Datenvermeidung bzw. Datensparsamkeit ableiten. Diese Grundsätze sind umso wichtiger, als im vorliegenden Fall Gesundheitsdaten und somit besonders schützenswerte Personendaten bearbeitet werden. Es ist nicht nachvollziehbar, dass z.B. für eine Reiseversicherung die gleichen Angaben benötigt werden wie für eine Zusatzversicherung, welche alternative Heilmethoden anbietet. Aus diesem Grunde haben wir einen Krankenversicherer gebeten, die Antragsformulare entsprechend anzupassen bzw. uns die Datenbedürfnisse für die einzelnen Zusatzversicherungen nachzuweisen.

6.2.2. Die Beschaffung von Personendaten durch Haftpflichtversicherer

Im vorliegenden Berichtsjahr wurden wir vermehrt mit Fällen aus dem Bereich der Haftpflichtversicherungen konfrontiert. Im Wesentlichen ging es darum, wann und unter welchen Voraussetzungen ein Haftpflichtversicherer Personendaten der Geschädigten beschaffen kann. In jedem Fall sind die datenschutzrechtlichen Prinzipien zu berücksichtigen.

Haftpflichtversicherer, die ihre Leistungspflicht gegenüber Geschädigten abklären und deren Personendaten bearbeiten, haben die datenschutzrechtlichen Grundsätze einzuhalten (vgl. auch 6. Tätigkeitsbericht 1998/99, S. 82). Insbesondere darf ein Haftpflichtversicherer nicht ohne Rechtfertigungsgrund Personendaten entgegen den datenschutzrechtlichen Grundsätzen bearbeiten, Daten gegen den ausdrücklichen Willen der betroffenen Person bearbeiten und besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekannt geben. Eine Verletzung der Persönlichkeit durch einen Haftpflichtversicherer ist dann nicht widerrechtlich, wenn ein Rechtfertigungsgrund (Einwilligung des Verletzten, überwiegendes privates oder öffentliches Interesse oder Gesetz) vorliegt. Ob eine Persönlichkeitsverletzung gegeben ist, ist nach bundesgerichtlicher Rechtsprechung im Einzelfall und nach einer Interessenabwägung zu untersuchen.

Eine Frage war etwa, wann und unter welchen Voraussetzungen ein Haftpflichtversicherer berechtigt sei, bei einem Psychiater ein Aktengutachten einzuholen, um den Leistungsanspruch des Geschädigten abklären zu können. Wir hielten in einer Stellungnahme fest, dass dafür grundsätzlich die Einwilligung des Geschädigten erforderlich ist. Wie bereits erwähnt, ist eine Interessenabwägung im Einzelfall vorzunehmen. Solange jedoch die Einwilligung möglich ist, sollte kein anderer Rechtfertigungsgrund herangezogen werden (Prinzip der Verhältnismässigkeit). Verweigert oder widerruft

der Geschädigte die Einwilligung, steht es dem Haftpflichtversicherer grundsätzlich frei, auf mögliche finanzielle Forderungen nicht einzutreten bzw. die Abklärungen einzustellen. Eine Einwilligung ist aus unserer Sicht auch erforderlich, um den Psychiater vom Arzt- bzw. Patientengeheimnis zu entbinden. Auch ein psychiatrisches Gutachten bzw. dessen Resultate unterstehen dem Berufsgeheimnis nach Strafgesetzbuch.

In jedem Fall sind Geschädigte über die Erstellung eines Gutachtens vorab zu informieren. Dies ergibt sich aus dem Transparenzprinzip und steht im Einklang mit der geplanten Änderung des Datenschutzgesetzes. Diese sieht nämlich u.a. vor, dass das Beschaffen von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen durch eine private Person (wie einen Haftpflichtversicherer) den betroffenen Personen transparent gemacht werden muss.

7. Arbeitsbereich

7.1. Die Bekanntgabe von Personaldaten ins Ausland

Die Übermittlung von Personaldaten ins Ausland in zentralisierte Datensammlungen wird, vor allem bei Konzerngesellschaften, immer mehr zur Norm. Angestrebt wird vor allem eine bessere Wirtschaftlichkeit der Lohnbewirtschaftung und der Personalrekrutierung.

Es gibt vier Hauptarchitekturen für eine Bereitstellung von Informationen über eine globale IT-Infrastruktur. Sie unterscheiden sich hauptsächlich in der geografischen Lage der Daten und der Datenschutzregelungen.

Die erste Architektur charakterisiert sich durch eine ausschliesslich zentrale Aufbewahrung der Daten. Der Zugriff und die Bearbeitung der Daten findet durch die berechtigten Filialen auf dem zentralen Server statt. Es existieren lokal keine elektronischen Kopien der zentralen Daten. Die berechtigten Firmen definieren die Anforderungen in den Datenschutzerklärungen aus Sicht des innerstaatlichen Datenschutzes. Eine solche Architektur kommt in der Regel für Personalbewirtschaftungssysteme (HR-Systeme) zur Anwendung.

Die zweite Architektur ist eine Variation der ersten. Sie unterscheidet sich dadurch, dass die Daten grundsätzlich lokal bewirtschaftet werden und nur ein Teil je nach Zweck in die zentrale Datensammlung transferiert wird und somit Dritten zur Verfügung steht. Der Transfer der Daten kann sowohl auf Anfrage als auch automatisiert erfolgen. Zum Beispiel können statistische Lohndaten, die lokal generiert werden, für eine unternehmensweite Nutzung zentral zur Verfügung stehen. Ein weiteres häufiges Anwendungsbeispiel besteht in der zentralen Verfügbarkeit von Personendaten oder

Persönlichkeitsprofilen der Mitarbeitenden zur konzerninternen Personalsuche.

Die dritte Variante zeichnet sich durch eine strikte Trennung der Anwendung und der Daten aus. Die Daten werden ausschliesslich lokal bearbeitet. Das zentrale Anwendungssystem nimmt lediglich eine Vermittlungsfunktion zwischen einer datenliefernden Gesellschaft (Datenexporteur) und einer datenempfangenden Gesellschaft (Datenimporteur) wahr. Es verwaltet die Datenschutzerklärungen der Beteiligten und weiss somit, zwischen welchen Gesellschaften der Datenaustausch problemlos erfolgen kann. Ein Transfer der Daten erfolgt dann direkt zwischen Datenexporteur und Datenimporteur, nachdem das zentrale Anwendungssystem die Datenübermittlung gutgeheissen hat. Das zentrale Anwendungssystem verwaltet die Adressen aller beteiligten Datenbearbeitungssysteme und teilt diese bei Bedarf mit. Damit wird mit wenig Aufwand eine komplette Vermaschung (Jeder kennt Jeden) der Systeme erreicht.

Die vierte Variante entspricht der peer-to-peer Architektur. Jeder der beteiligten Partner bestimmt selber, welche Daten er an wen bekannt gibt. Eine vermittelnde Instanz wie in der dritten Variante existiert nicht. Der Datenexporteur muss aufgrund seiner lokalen Datenschutzrichtlinien entscheiden, ob er Personendaten übertragen darf. Eine zentrale Stelle, welche die Datenschutzerklärungen der Teilnehmerstaaten verwaltet, existiert nicht. Die Art und Weise der Datenübermittlung basiert auf bilateralen Abmachungen und kann sowohl auf Anfrage als auch direkt per Abrufverfahren erfolgen.

In jeder dieser Varianten wird die datenempfangende Gesellschaft im Ausland Dateninhaberin der übermittelten Daten, wenn sie über den Zweck und den Inhalt der zentralisierten Datensammlung entscheidet. Als solche ist sie für den Datenschutz und die Datensicherheit verantwortlich. In Bezug auf eine zentralisierte Datensammlung gelten die datenliefernden Gesellschaften als Zugriffsberechtigte mit besonderer Verantwortung. Sie müssen der datenempfangenden Gesellschaft Bedingungen in Bezug auf den Datenschutz aufstellen (Datenschutzregelung). Eine Muster-Datenschutzklausel hat der Europarat mit der Verabschiedung des Mustervertrages für die Sicherstellung eines gleichwertigen Datenschutzes im Rahmen des grenzüberschreitenden Datenverkehrs bereits 1992 aufgestellt (siehe http://www.edsb.ch/d/gesetz/europarat/mustervertrag.htm).

Was die Datenbekanntgabe von der datenempfangenden Firma an Drittfirmen betrifft, hat die Kommission der Europäischen Gemeinschaften in einer Entscheidung vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer klare Bedingungen festgelegt (siehe http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-16_de.pdf).

Der Zweck der Datenübermittlung ins Ausland muss einem Rechtfertigungsgrund ge-

mäss Art. 13 DSG entsprechen. Die kostengünstigere Lohnbewirtschaftung und Personalrekrutierung gilt als Rechtfertigungsgrund. Es dürfen jedoch nur jene Personendaten übermittelt werden, welche für die Erfüllung des angegebenen Zweckes nötig sind.

Bei der Datenbekanntgabe durch den Datenimporteur an Firmen in Drittstaaten hat dieser abzuklären, ob diese Drittstaaten über einen Datenschutz verfügen, der dem schweizerischen gleichwertig ist. Ansonsten ist der Datenschutz mit diesen Firmen vertraglich zu gewährleisten. Diese Verpflichtung ist insbesondere bei der Schaffung von Datenpools für die Stellenbesetzung innerhalb des Konzerns von Bedeutung.

Bei der Übertragung der Datenbearbeitung an Dritte hat der Auftraggeber dafür zu sorgen, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

Die übermittelten Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Darum empfiehlt es sich, je nach Klassifizierung der Datenkategorien besondere Schutzmassnahmen zu ergreifen. Es muss garantiert sein, dass zu jeder Zeit der unberechtigte Zugang zur Infrastruktur und zu den Datenträgern unmöglich ist. Ebenso muss der Zugriff Unberechtigter auf die Personendaten, während deren Lagerung und Transport ausgeschlossen sein, indem die Daten verschlüsselt werden. Die Verschlüsselung hat nach dem aktuellen Stand der Technik zu erfolgen. Dies gilt sowohl für die Daten als auch für die Datenschutzerklärungen. Die Identifikation der gemäss Erklärungen Empfangsberechtigten muss eindeutig gewährleistet sein. Die Identifikation hat nach den neusten technischen Stand zu erfolgen. Damit jederzeit die Verarbeitung der Daten nachvollziehbar ist, muss sie protokolliert werden.

7.2. Aufbewahrung des Personaldossiers

Nach Erstellung einer Personalakte obliegt der Arbeitgeberin resp. dem Arbeitgeber eine Aufbewahrungspflicht, welche, je nach Personalakte und Erstellungsdatum, unterschiedlich ist. Die Aufbewahrungsdauer läuft ab Zeitpunkt der Erstellung der Personalakte, nicht ab Beendigung des Arbeitsverhältnisses.

Aufbewahrung von Lohndaten

Wer zur Führung von Geschäftsbüchern verpflichtet ist, hat diese, die Geschäftskorrespondenz und die Buchungsbelege während zehn Jahren aufzubewahren. Die Aufbewahrungsfrist beginnt mit dem Ablauf des Kalenderjahres, in dem die letzten Eintragungen vorgenommen wurden bzw. in dem die letzte Korrespondenz ein- oder ausge-

gangen ist. Die Verordnung über die Aufzeichnung von aufzubewahrenden Unterlagen vom 2. Juni 1976 regelt die Einzelheiten, insbesondere die Verantwortlichkeit für die Aufbewahrung. Zu den Geschäftsbüchern gehört auch die Lohnbuchhaltung mit allen relevanten Lohndaten.

Daten zur Erstellung eines Arbeitszeugnisses

Die zehnjährige Verjährungsfrist von Art. 127 OR gilt nach vorherrschender Auffassung u.a. auch für den Anspruch auf Erstellung, Begründung, Korrektur oder Ergänzung eines Arbeitszeugnisses. Diese Ansprüche können bis zehn Jahre nach Beendigung des Arbeitsverhältnisses geltend gemacht werden. Von der Aufbewahrungspflicht des Arbeitgebers betroffen sind in erster Linie Angaben über Art und Dauer des Arbeitsverhältnisses, Aufgabenbeschreibung und Verantwortungsbereich, Beurteilungen von Leistung, Verhalten und Führung, Laufbahn und Weiterbildung, Austrittsgrund aber auch Angaben über besondere Vorkommnisse. Diese Daten sind vor allem im Pflichtenheft, in den Mitarbeiterbeurteilungen, in der Laufbahnplanung und Weiterbildungsunterlagen zu finden. Relevant für die Erstellung eines Arbeitszeugnisses sind in der Regel nur die letzten zwei Mitarbeiterbeurteilungen. Frühere Beurteilungen sind regelmässig aus dem Personaldossier zu entfernen und zu vernichten.

Akten, die den Angestellten gehören

Bewerbungsunterlagen wie z.B. Lebenslauf, frühere Arbeitszeugnisse, Ausbildungsdiplome, Arbeitsproben, Fotos und ähnliche Akten, die den Angestellten gehören und an denen der Arbeitgeber kein berechtigtes Interesse mehr hat, müssen diesen spätestens bei Beendigung des Arbeitsverhältnisses zurückgegeben werden. In der Regel sollte dies jedoch bereits nach Ablauf der Probezeit geschehen.

Akten, die dem Arbeitgeber gehören

Akten, die dem Arbeitgeber gehören, an denen er aber kein berechtigtes Interesse mehr hat, müssen spätestens bei Beendigung des Arbeitsverhältnisses vernichtet werden. Der Arbeitgeber kann solche Dokumente auch den Angestellten aushändigen. Es geht hier insbesondere um frühere Qualifikationsunterlagen, die für die Erstellung und Begründung eines Arbeitszeugnisses nicht mehr benötigt werden, aber auch um graphologische, psychologische oder medizinische Gutachten sowie um Persönlichkeitstests. Auch solche Dokumente sollten in der Regel bereits eins bis zwei Jahre nach Erstellung vernichtet bzw. zurückgegeben werden.

Allgemeine Bemerkungen

Da die Aufbewahrungsdauer vom Erstellungsdatum einer Personalakte abhängig ist, empfehlen wir, auf jedem Dokument des Personaldossiers das Erstellungsdatum sowie die entsprechende Aufbewahrungsdauer gut sichtbar anzubringen. Dadurch wird

die Kontrolle des Ablaufes der Aufbewahrungsdauer und die entsprechende, regelmässige Triage des Personaldossiers erleichtert.

Personendaten dürfen in Abweichung der oben genannten Regeln nur mit dem Einverständnis der Angestellten und nur zu deren Gunsten länger aufbewahrt werden.

Im Hinblick auf hängige Rechtsstreitigkeiten wird der Arbeitgeber bis zu deren Beendigung jene Akten aufbewahren, die er als Beweismittel braucht. Wenn z.B. Angestellte knapp vor Ablauf der zehnjährigen Verjährungsdauer eine der oben genannten Ansprüche geltend machen, so darf der Arbeitgeber die benötigten Beweismittel bis zur Beendigung der Rechtstreitigkeit, d.h. bis zum Ablauf der entsprechenden Rekursfristen, aufbewahren. Die Aufbewahrungsdauer der benötigten Beweismittel kann sich in solchen Fällen bis über die zehnjährige Aufbewahrungsdauer erstrecken.

7.3. Die Bekanntgabe von Personendaten im Rahmen von Gesamtarbeitsverträgen

Ist die Kontrolle der Lohnbestimmungen und damit die Weitergabe der Lohndaten im GAV vorgesehen, so gilt dies als Einwilligung der Vertragsparteien. Ob es andere Rechtfertigungsgründe für die Datenweitergabe als die Einwilligung der Angestellten gibt, muss der Richter im Einzelfall entscheiden. Wünschenswert ist die Schaffung eines unabhängigen Kontrollorgans durch den Gesetzgeber.

Ein GAV kann die Kontrolle seiner Lohnbestimmungen durch eine paritätische Kommission, bestehend aus Arbeitgeber- und -nehmervertretenden, vorsehen. Dazu können die Lohndaten der Angestellten an diese Kommission weitergegeben werden.

Nach Artikel 328b des Obligationenrechts (OR) darf der Arbeitgeber Daten über die Angestellten nur bearbeiten und weitergeben, soweit sie die Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Von dieser Bestimmung darf nur zu Gunsten der Angestellten abgewichen werden (Art. 362 OR).

Ein Arbeitgeber darf Daten nur bearbeitet und weiter geben, wenn ein Rechtfertigungsgrund dafür vorliegt (Art. 12 Abs. 1 und Art. 13 Abs. 1 DSG). Dieser Rechtfertigungsgrund kann ein Gesetz, die Einwilligung der Betroffenen oder ein überwiegendes privates oder öffentliches Interesse sein.

Eine gesetzliche Grundlage, welche die Datenweitergabe an eine paritätische Kommission vorsieht, liegt nicht vor. Somit bleiben nur noch die Einwilligung der Betroffenen oder ein überwiegendes privates oder öffentliches Interesse als mögliche Rechtfertigungsgründe.

Ist die Kontrolle der Lohnbestimmungen und damit die Weitergabe der Lohndaten im GAV vorgesehen, so gilt dies als Einwilligung der Vertragsparteien. In der Regel treten alle Angestellten direkt oder durch Vertretung dem GAV bei. Folglich müssen Angestellte, die dem GAV nicht unterstehen, vorgängig über die Datenweitergabe informiert werden und einzeln dazu einwilligen.

Ob ein überwiegendes privates oder öffentliches Interesse an der Weitergabe der Lohndaten besteht und ob dieses Interesse zu Gunsten der Angestellten ist, muss im Einzelfall vom Richter geklärt werden. Es scheint jedoch plausibel, dass die Angestellten als Vertragspartei des GAV ein Interesse daran haben, dass die Einhaltung der Lohnbestimmungen kontrolliert wird.

Die Weitergabe der Lohndaten durch eine generelle Offenlegung der Personalbuchhaltung ist jedoch nicht zulässig, da in dieser Buchhaltung auch Daten Dritter enthalten sind.

Es besteht die Möglichkeit den Geltungsbereich des GAV auf nicht unterstellte Arbeitgeber und -nehmer auszudehnen, die dann bei der zuständigen kantonalen Behörde die Einsetzung eines unabhängigen Kontrollorgans verlangen können. Die Behörde bestimmt Gegenstand und Umfang der Kontrolle nach Anhörung einerseits der Vertragsparteien des GAV und anderseits des Arbeitgebers bzw. Angestellten, welche die Einsetzung des besonderen Kontrollorgans verlangen (Art. 6 des Bundesgesetzes vom 28. Sept. 1956 über die Allgemeinverbindlicherklärung von Gesamtarbeitsverträgen).

Es ist wünschenswert, dass der Gesetzgeber diese Möglichkeit für jeden GAV ausdrücklich vorsieht, da bei dieser Regelung die Mitglieder des Kontrollorgans unabhängig von den beiden Vertragsparteien sind und somit in keinen Interessenskonflikt kommen.

7.4. Telefonüberwachung am Arbeitsplatz (Call Centers)

Beide Gesprächsteilnehmenden müssen über die Abhörung oder die Aufnahme telefonischer Gespräche vorgängig informiert werden und dazu einwilligen. Eine einmalige Information im Vertrag genügt, wenn die Abhörungen oder Aufzeichnungen systematisch erfolgen. Bei gelegentlichen Abhörungen oder Aufzeichnungen muss hingegen bei jedem betroffenen Telefongespräch vorgängig über die Abhörung resp. Aufzeichnung informiert werden.

Das Strafgesetzbuch setzt für eine rechtmässige Abhörung oder Aufnahme von Gesprächen die Einwilligung beider Gesprächsteilnehmenden voraus. Der Inhalt von Telefongesprächen darf nur aus Gründen der Leistungskontrolle (z.B. Qualitätskontrolle bei Telefonverkäufen, Schulungszwecke) oder aus Sicherheitsgründen (z.B. für die Be-

weissicherung) aufgezeichnet werden. Die Abhörung oder Aufnahme ist zulässig, wenn alle Personen, deren Gespräch aufgezeichnet oder mitgehört wird, damit einverstanden sind und jeweils darüber eindeutig und rechtzeitig in Kenntnis gesetzt worden sind.

Die Information über die Abhörung oder Aufzeichnung bei jedem einzelnen Gespräch ist nicht unbedingt notwendig, wenn die Telefonabhörungen bzw. -aufnahmen systematisch erfolgen und alle Gesprächsbeteiligten bereits eindeutig informiert worden sind. Diese Lösung ist beispielsweise in bestimmten Bankbereichen denkbar, wo Rechtsgeschäfte per Telefon abgewickelt werden. In einem solchen Fall genügt für die Angestellten eine ausdrückliche vorherige Information im Arbeitsvertrag und für die Kundschaft in den allgemeinen Geschäftsbedingungen. Denkbar sind auch Situationen, wo Angestellte einmalig im Arbeitsvertrag informiert werden, sämtliche Gesprächspartner jedoch durch Abspielen eines Bandes informiert werden müssen, da sie nicht in einem Vertragsverhältnis zum Anrufenden stehen. Es kann auch vorkommen, dass sowohl vertraglich informierte Kunden als auch vertraglich nicht gebundene Personen Gesprächsteilnehmende sind. Erstere werden in den allgemeinen Geschäftsbedingungen, letztere müssen jeweils mündlich über die Abhörung oder Aufnahme informiert werden.

Gelegentliche Abhörungen oder Aufzeichnungen fremder Gespräche sind beispielsweise in einem Auskunftsdienst denkbar (Call-Center). Die Information der Angestellten über die Abhörung oder Aufnahme erfolgt in der Regel bei jedem einzelnen Gespräch durch ein optisches oder akustisches Signal. Um den Interessen des Arbeitgebers, insbesondere der Wirksamkeit der Schulung, besser gerecht zu werden, ist es mit dem Persönlichkeitsschutz nicht unvereinbar, wenn die Angestellten nur über die ausgewählte Abhörungs- oder Aufzeichnungsperiode informiert werden. Diese Periode darf aus Gründen der Verhältnismässigkeit und des Persönlichkeits- und Gesundheitsschutzes am Arbeitsplatz höchstens fünf Tage betragen. Die Pflicht zur Information der anderen Gesprächsteilnehmer bleibt selbstverständlich bestehen und erfolgt in der Regel durch Abspielen eines Bandes.

7.5. Die Erstellung von «grauen» Dossiers im Arbeitsbereich

Das Personaldossier mit seinen schriftlichen Aufzeichnungen und Personalakten gilt nicht als eine Datenbearbeitung zum ausschliesslich persönlichen Gebrauch der Arbeitgeberin resp. des Arbeitgebers und unterliegt somit dem Geltungsbereich des Datenschutzgesetzes, insbesondere dem Auskunftsrecht.

Die Erstellung von grauen Dossiers, in die Angestellte keine Einsicht haben, und die Vernichtung von Personendaten entgegen den Grundsätzen des Datenschutzes, insbesondere entgegen der Verhältnismässigkeit der Aufbewahrungsdauer, umgeht die Persönlichkeitsrechte der Angestellten. Betroffen ist in erster Linie das Auskunftsrecht bezüglich Informationen, die wegen ihrer Brisanz den Angestellten verheimlicht werden sollen. Dadurch wird auch das Berichtigungs- und Bestreitungsrecht (Gegendarstellungsrecht) verunmöglicht. Der Arbeitgeber kann zwar das Auskunftsrecht einschränken, aufschieben oder verweigern, wenn der Auskunft überwiegende private oder öffentliche Interessen entgegen stehen. Das DSG verpflichtet Inhaber von Datensammlungen anzugeben, aus welchem Grund sie die Auskunft einschränken. Für die Anforderungen an diese Begründung ist massgebend, dass sie einerseits den Betroffenen ermöglichen muss, die Zulässigkeit und Stichhaltigkeit der Beschränkung zu überprüfen und andererseits den Richter befähigen muss, die wesentlichen Entscheidungsgründe des Inhabers der Datensammlung für die Nichtgewährung der Auskunft nachvollziehen zu können. Zu bemerken ist in diesem Zusammenhang, dass persönliche Notizen des Arbeitgebers, die nicht an Aussenstehende bekannt gegeben werden, nicht Gegenstand des Auskunftsrechtes bilden. So fallen weder Notizen, die jemand zwar in Ausübung seines Berufes, aber als Gedankenstütze oder Arbeitshilfe nur zum persönlichen Gebrauch macht, noch die Bearbeitung von Daten zum persönlichen Gebrauch, insbesondere zur Erstellung eines persönlichen Arbeitsinstrumentes darunter. Diese Bestimmung darf jedoch keinesfalls von der datenbearbeitenden Person angerufen werden, um die Vorschriften des DSG zu umgehen. Daten, die ursprünglich zum persönlichen Gebrauch bearbeitet wurden, unterliegen, falls sie an Aussenstehende bekannt gegeben werden, dem DSG. Diese Bekanntgabe umfasst im beruflichen Bereich auch die Bekanntgabe innerhalb des Unternehmens. Eine solche Bekanntgabe z.B. unter Kollegen hat also den Ausschluss der Ausnahme zur Folge und führt zur Anwendung des DSG.

Die Erstellung von grauen Dossiers verletzt auch den Grundsatz von Treu und Glauben. Danach dürfen Angestellte gegenüber dem Arbeitgeber das berechtigte Vertrauen haben, dass er über die sie betreffenden Datenbearbeitungen informiert werden. Gegen diesen Grundsatz verstösst z.B. derjenige, welcher heimlich Daten beschafft, ohne dabei gegen eine Rechtsnorm zu verstossen. Aus diesem Prinzip ist die Anforderung abzuleiten, dass eine Datenbeschaffung für die betroffene Person transparent, d.h. erkennbar erfolgen muss.

Betroffene Angestellte können im Falle einer Verletzung des Auskunftsrechtes und des Grundsatzes von Treu und Glauben nicht nur zivilrechtliche Ansprüche wie Berichtigung, Vernichtung oder Sperrung von Personendaten, gegebenenfalls verbunden mit Schadenersatz- oder Genugtuungsansprüchen, geltend machen, es stehen ihnen auch

strafrechtliche Mittel zu. Für die zivilrechtlichen Ansprüche ist das Arbeitsgericht zuständig, das in der Regel in einem raschen und kostenlosen Verfahren entscheidet. Für strafrechtliche Angelegenheiten ist der Richter gemäss kantonaler Strafprozessordnung zuständig.

Die Ausführungen über das Auskunftsrecht und den Grundsatz von Treu und Glauben gelten auch in Bezug auf die Beschaffung der Informationen. Danach sind Angestellte berechtigt, über den Ursprung der gesammelten Daten informiert zu werden. Unter Umständen ist der Arbeitgeber jedoch aus Persönlichkeitsschutzgründen verpflichtet, die Identität von Auskunftspersonen geheim zu halten, wenn ihre Persönlichkeitsschutzinteressen überwiegen. So ist es beispielsweise vorstellbar, dass der Arbeitgeber die gesamte Mitarbeiterschaft oder Teile davon als Auskunftsquelle angibt, ohne jedoch die einzelnen Mitarbeitenden mit bestimmten Informationen oder Aussagen zu verknüpfen.

7.6. Verletzung der Schweigepflicht durch private Arbeitsvermittler

Private Arbeitsvermittler dürfen Daten über Stellensuchende an die Regionalen Arbeitsvermittlungszentren (RAV) nur bekannt geben, wenn die betroffene Person schriftlich eingewilligt hat.

Private Arbeitsvermittler dürfen Daten über Stellensuchende und offene Stellen nur bearbeiten, soweit und solange sie für die Vermittlung erforderlich sind. Die Datenbekanntgabe wird in der entsprechenden Gesetzgebung abschliessend geregelt. Eine gesetzliche Grundlage für die Bekanntgabe von Daten über Stellensuchende von einem privaten Arbeitsvermittler an die regionalen Arbeitsvermittlungszentren besteht nicht. In diesem Zusammenhang gilt die Schweigepflicht. Der betroffenen Person stehen die Rechtsansprüche gemäss Datenschutzgesetz zur Verfügung. Die Schweigepflicht entfällt, wenn der oder die Stellensuchende schriftlich in die Datenbekanntgabe eingewilligt hat.

7.7. Kontrolle des Arbeitnehmers während der Abwesenheit

Während einer krankheitsbedingten Abwesenheit darf die Arbeitgeberin, resp. der Arbeitgeber das Verhalten der kranken Angestellten nur nach entsprechender, allgemeiner Information und nur bei konkretem Verdacht auf vertragswidriges Verhalten kontrollieren.

Eine Gewerkschaft hat uns mit folgenden Fakten konfrontiert: Ein Arbeitnehmer wurde aus gesundheitlichen Gründen während einer bestimmten Zeit arbeitsunfähig ge-

schrieben. Die Arbeitsunfähigkeit betraf die Verrichtung körperlicher Tätigkeiten. Der Arbeitnehmer informierte den Arbeitgeber über Krankheit und Dauer, verschwieg aber, während der krankheitsbedingten Abwesenheit einen Tag lang eine rein intellektuelle Arbeit bei einem Drittarbeitgeber ausgeübt zu haben. Der Arbeitgeber, welcher über den zweiten Beruf seines Angestellten in Kenntnis war, erkundigte sich beim Zweitarbeitgeber über mögliche Tätigkeiten seines Angestellten während der krankheitsbedingten Abwesenheit. Konkrete Anhaltspunkte für ein vertragswidriges Verhalten lagen nicht vor. Der Zweitarbeitgeber bestätigte die Präsenz des Angestellten während eines Tages. Der erste Arbeitgeber ergriff darauf arbeitsrechtliche Massnahmen gegen den Angestellten. Er begründete sie mit der Verletzung einer gesamtarbeitsvertraglichen Pflicht, wonach der Arbeitgeber über längere Abwesenheiten des Arbeitnehmers vom Wohnsitz informiert werden muss. Die Gewerkschaft des Arbeitnehmers fragte uns an, ob eine solche Kontrolle rechtmässig gewesen sei. Wir sind zu folgenden Schlussfolgerungen gekommen:

Der Arbeitgeber hat die Persönlichkeit der Angestellten zu schützen und zu achten. Er darf insbesondere nur jene Daten über die Angestellten bearbeiten, soweit sie deren Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Daten aus der Privatsphäre, die mit dem Arbeitsverhältnis in keinem Zusammenhang stehen, dürfen nicht bearbeitet werden. Die Datenbearbeitung durch den Arbeitgeber hat überdies auch nach Treu und Glaube zu erfolgen. Dies bedeutet, dass die Angestellten in der Regel vorgängig darüber informiert werden müssen.

Andererseits haben Angestellte die ihnen übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen des Arbeitgebers in gutem Treuen zu wahren. Während der Dauer des Arbeitsverhältnisses dürfen Angestellte insbesondere keine Arbeit gegen Entgelt für einen Dritten leisten, soweit sie dadurch ihre Treuepflicht verletzt, insbesondere den Arbeitgeber konkurrenziert. Dieser kann über die Ausführung der Arbeit und das Verhalten der Angestellten im Betrieb allgemeine Anordnungen erlassen und ihnen besondere Weisungen erteilen. Angestellte haben diese nach Treu und Glauben zu befolgen.

Von grundlegender Bedeutung im Zusammenhang mit der Verhaltensüberwachung von Angestellten ist die vorherige Information, dass die Einhaltung der vertraglichen Pflichten kontrolliert werden kann. Dies leitet man aus dem Prinzip von Treu und Glaube ab. Ohne vorherige Information dürfen Angestellte davon ausgehen, dass das Arbeitsverhältnis auf das Vertrauen basiert, die Persönlichkeit respektiert wird und er während einer Abwesenheit nicht überwacht wird. Darüber hinaus müssen konkrete Verdachtsmomente eines vertragswidrigen Verhaltens vorliegen. Wenn dem nicht so wäre, bestände das Risiko willkürlicher Kontrollen durch den Arbeitgeber. Ist eine die-

ser Voraussetzungen nicht erfüllt, so ist eine Kontrolle des Verhaltens während einer krankheitsbedingten Abwesenheit nicht gestattet.

Im vorliegenden Fall wurde weder das Konkurrenzverbot noch die Treuepflicht verletzt, da die während der krankheitsbedingten Abwesenheit ausgeübten Tätigkeit nicht körperlicher, sondern intellektueller Natur war und der Arbeitgeber über das Bestehen des zweiten Arbeitsverhältnisses in Kenntnis war und keinen Einwand dagegen hatte. Auch die gesamtarbeitsvertragliche Bestimmung über die Meldepflicht bei längerer Abwesenheit vom Wohnsitz wurde nicht verletzt, da die ausgeübte Tätigkeit nicht länger als einen Tag dauerte. Ein vertragswidriges Verhalten lag also nicht vor. Der Arbeitgeber hatte die Angestellten auch nicht über die Möglichkeit solcher Kontrollen informiert.

7.8. Drogentests in der Lehre- Weiterzug an die EDSK

Wie wir bereits im 8. Tätigkeitsbericht 2000/2001 (S. 21) erwähnt haben, hat der Chemiekonzern Hoffmann-La Roche unsere Empfehlung in Sachen Drogentests in der Lehre abgelehnt. Wir haben die Angelegenheit der Eidg. Datenschutzkommission (EDSK) zum Entscheid vorgelegt. Die Weiterziehung ist auf S. 135 wiedergegeben.

7.9 Musterreglement für die Internet und E-Mail-Überwachung am Arbeitsplatz

Nach der Veröffentlichung des Leitfadens über die Internet- und E-Mail-Überwachung am Arbeitsplatz haben wir ein entsprechendes Musterreglement publiziert (siehe S. 111). Es stellt eine Hilfe für jene Unternehmen dar, die ein Reglement für die Nutzung und Überwachung des Internet- und E-Mailgebrauchs am Arbeitsplatz erstellen möchten.

7.10. Verordnung über den Schutz von Personendaten in der Bundesverwaltung

Der Bundesrat hat am 3. Juli 2001 die Verordnung über den Schutz von Personendaten in der Bundesverwaltung verabschiedet, ohne dass unsere Bedenken im Rahmen des Mitberichtverfahrens berücksichtigt worden sind. Die Verordnung ist am 1. Januar 2002 in Kraft getreten.

Am 24. März 2000 hat die Bundesversammlung das Bundespersonalgesetz verabschiedet. Für die SBB ist es auf den 1. Januar 2001, für die Post und die Bundesverwaltung auf den 1. Januar 2002 in Kraft getreten. Eine Ausführungsverordnung regelt die

Bearbeitung der Personendaten von Angestellten, ehemaligen Angestellten sowie von Stellenbewerberinnen und Stellenbewerber bei der Bundesverwaltung. Die Verordnung sieht u.a. vor, dass eine Kopie des Beurteilungsformulars im Personaldossier abgelegt wird. Wir haben im Rahmen des Mitberichtsverfahrens festgehalten, dass Personalbeurteilungen keinesfalls in ihrer Gesamtheit dem Personaldienst systematisch zur Verfügung gestellt werden dürfen. Der Grund liegt darin, dass ein Personaldienst zur Erfüllung seiner Aufgaben (z.B. Festsetzung des Lohnes, Organisation von Weiterbildungskursen) in der Regel lediglich auf die Gesamtbewertung sowie allenfalls auf weitere organisatorische Angaben angewiesen ist. Solche Informationen können dem Personaldienst problemlos mit einem separaten Dokument bekannt gegeben werden. Deshalb haben wir empfohlen, den Verordnungsentwurf entsprechend anzupassen und auf das systematische Ablegen einer offenen Kopie des Beurteilungsformulars zu verzichten. In Frage kommt einzig das Ablegen des Beurteilungsformulars in einem verschlossenen Couvert. Der Personaldienst sollte dann in den Inhalt des Beurteilungsformulars nur in begründeten Einzelfällen Einsicht nehmen dürfen. Unsere Argumentation wurde jedoch nicht berücksichtigt.

8. Handel und Wirtschaft

8.1. Allgemeine Anforderungen zur Überprüfung von Websites (Gütesiegel)

Die Einführung von internet-basierten Geschäftsprozessen (E-Commerce), stellen Unternehmen vor neue Herausforderungen. Insbesondere muss die Frage nach den Risiken für die Privatsphäre bei der Verwendung neuer Technologien abgeklärt werden.

Die Verwendung neuer Technologien birgt spezifische Risiken. Die Vernetzung der Systeme betrifft sowohl den Datenfluss des gesamten Unternehmens als auch die konventionellen Geschäftsprozesse. Für das Unternehmen ist wesentlich, wie die Sicherheit von Aussenstehenden empfunden wird, denn Misstrauen seitens der Geschäftspartner und potenzieller Kundschaft kann den unternehmerischen Erfolg im E-Commerce insgesamt gefährden.

Mit der Einführung eines Gütesiegels und dessen Prüfung innerhalb einer IT-Revision durch eine unabhängige Organisation erhält ein Unternehmen die Möglichkeit, seine Sicherheits- und Datenschutzstandards nach Aussen zu dokumentieren.

Dabei sind folgende Aspekte zu überprüfen:

- Sicherung des Zugriffs auf die Daten

- Schutz personenbezogener Daten
- Vertraulichkeit der Daten
- Verfügbarkeit der Daten
- Integrität der Daten

Dabei ist wichtig, dass die Prüfkriterien international einheitlich gestaltet und im Internet veröffentlicht werden, damit der Qualitätsstandard objektiv nachvollzogen werden kann. Die Prüfung muss entsprechend anerkannter Prüfstandards geplant und durchgeführt werden. Die Erteilung des Gütesiegels darf nur durch dafür anerkannte Auditoren erfolgen, die prozessunabhängig sein müssen. Mehr Informationen zu Gütesiegeln finden sich auch im 8. Tätigkeitsbericht 2000/2001, S. 19.

8.2. Unerwünschte E-Mail-Werbung (Spam)

Werbekampagnen durch Massenversand via E-Mail (Spam) nehmen stetig zu. Unsere Gesetzgebung reicht noch nicht aus, um der Belästigung durch Spam entgegenzuwirken. In den letzten Monaten haben wir uns vor allem mit zwei Fällen beschäftigt. Der erste betrifft den Vertrieb einer CD-ROM mit Personendaten von über einer halben Million Einwohnerinnen und Einwohner der Schweiz, der zweite den wiederholten Massenversand unerwünschter Werbung per E-Mail durch eine in Zürich wohnhafte Person.

In der Schweizer Gesetzgebung ist das sogenannte «Opt-Out»-Prinzip verankert. Dies bedeutet, dass Werbung per E-Mail ausser im Falle der ausdrücklichen Ablehnung durch den Empfänger grundsätzlich erlaubt ist. Die Schweiz ist dabei, ihre Gesetzgebung zu revidieren, um strengere Bestimmungen über den Versand unerwünschter E-Mail-Werbung aufzunehmen. Auch die Europäische Union ist dabei, gesetzliche Bestimmungen in diesem Bereich auszuarbeiten, die mit grosser Wahrscheinlichkeit auf dem «Opt-In»-Grundsatz beruhen werden. Dieser Grundsatz ist auf europäischer Ebene bereits für automatische Telefonwerbung und für Werbung über SMS rechtsverbindlich.

Die CD-ROM «Black Book 2000»

Hierbei handelt es sich um eine CD-ROM, die in den USA hergestellt und in der Schweiz vertrieben wurde. Sie erlaubt den Zugriff anhand von bestimmten Kriterien auf Name, Vorname, Beruf, E-Mail-Adresse und Postanschrift von ca. 500'000 in der Schweiz wohnhaften Personen. Unsere Ermittlungen ergaben, dass die Informationen nicht immer auf rechtmässige Weise beschafft worden waren. So wurden manche E-Mail-Adressen beispielsweise aus der Datenbank der Domainregistrationsbehörde

Switch entnommen (obwohl die Nutzungsbestimmungen der Datenbank dies ausdrücklich verbieten). Andere E-Mail-Adressen stammten von der Website einer Person, welche die Verwendung der Informationen zu Werbezwecken ausdrücklich ausgeschlossen hatte. Schliesslich waren einige Personendaten trotz der ausdrücklichen öffentlichen Ablehnung (durch Aufnahme in die «Robinson-Liste» oder durch die Verwendung des Sternchens im Telefonbuch) der betroffenen Person gesammelt worden. Darüber hinaus waren die Angaben auf der CD-ROM mit dem Vermerk «Opt-In» versehen, obwohl die betroffenen Personen im Voraus keine ausdrückliche Zustimmung erteilt hatten. Hinzu kam, dass die CD-ROM zahlreiche falsche Personendaten enthielt, was gegen den Grundsatz der Datenrichtigkeit verstösst.

Nach Auffassung des Vertreibers der CD-ROM in der Schweiz seien keinerlei illegale Methoden zur Datenbeschaffung verwendet worden. Seiner Ansicht nach waren die Daten aus dem Public Domain zusammengetragen worden (Websites und Diskussionsforen). Dazu sei eine spezielle Suchmaschine eingesetzt worden, die in der Lage sei zu erkennen, ob eine Person die Weiterverwendung ihrer Personendaten verbietet, vorausgesetzt sie hat dies in Form von Metatags (Programmierung im Quellcode) kenntlich gemacht. Bei der betreffenden Suchmaschine habe es sich ausserdem um eine Standard-Anwendung für Internet-Benutzende gehandelt. Auch trage die CD-ROM die Aufschrift, dass sie nicht zu Spam-Zwecken verwendet werden darf.

Obwohl kein Spam nachgewiesen werden konnte, steht die CD-ROM unserer Auffassung nach nicht im Einklang mit der Schweizer Gesetzgebung über den Datenschutz. In unseren Empfehlungen forderten wir den Verkäufer der fraglichen CD-ROM in der Schweiz auf, den Verkauf der gegenwärtigen Version einzustellen, in der nächsten Version die unrechtmässig beschaffenen Daten zu entfernen, die Rechte der betroffenen Personen zu wahren (Löschung ihrer Daten, wenn sie dies verlangt haben), Fehler (Vermerk «Opt-In» und falsche Angaben) zu beseitigen und schliesslich dem Auskunftsrecht Folge zu leisten. Siehe dazu auch unsere Empfehlung auf Seite 151.

Verkauf von Waren per Spam

Seit mehreren Jahren führt eine in Zürich wohnhafte Person regelmässig für verschiedene Produkte Werbekampagnen per E-Mail durch. Das E-Mail enthält einen Antwortschein mit der Adresse für Bestellungen. Die Identität des Spam-Absenders ist jedoch nirgends deutlich angegeben. Dennoch besteht kein Zweifel daran, dass es sich immer um dieselbe Person (Spammer) handelt, da sie ihre Beteiligung am Versand der besagten Werbung nie dementierte. Sobald aber ein Empfänger von Spam sein Auskunftsrecht geltend macht, weigert sich der Spammer, diesem Folge zu leisten. Seiner Ansicht nach sind E-Mail-Adressen keine Personendaten und demzufolge fällt seine Werbung nicht in den Geltungsbereich des Gesetzes. Wir haben aber bestätigt, dass es

sich bei der Verwendung von E-Mail-Adressen sehr wohl um eine Bearbeitung von Personendaten im Sinne der Datenschutzgesetzgebung handelt. E-Mail-Adressen sind selbst im Falle der Verwendung von Pseudonymen Personendaten. Eine E-Mail-Adresse steht nämlich notwendigerweise mit einer bestimmten Person in Verbindung, die zwar nicht unmittelbar identifiziert ist, aber immerhin indentifizierbar bleibt. Wir haben den Spammer aufgefordert, die Rechte der betroffenen Personen zu wahren, d.h. ihre Personendaten aus seinem Adressbuch zu löschen und ihnen die Ausübung ihres Auskunftsrechtes zu garantieren.

9. Finanzen

9.1. Weitergabe von Personendaten aus Kontoeröffnungsanträgen

Eine Bank verspricht auf den Kontoeröffnungsanträgen ihren Kundinnen und Kunden, dass diese ihre Einwilligung zur Datenbearbeitung jederzeit widerrufen können. Geschieht dies tatsächlich, so verweigert die Bank umgehend einen Vertragsabschluss. Zudem will die Bank nicht offen legen, an wen sie die auf diese Weise erhaltenen Personendaten weitergibt. Wir haben gegen diese Praxis eine Empfehlung erlassen, welche die Bank angenommen hat. Der Text der Empfehlung mitsamt rechtlicher Begründung ist auf S. 124 abgedruckt.

Eine zu einem Versicherungskonzern gehörende Bank bietet verschiedene Formen der Kapitalanlage an. Personen, die sich dafür interessierten, erhielten von der Bank in der Regel Kontoeröffnungsanträge für die verschiedenen Arten der Kapitalanlage zugeschickt. In den allgemeinen Geschäftsbedingungen zu jedem Antrag fand sich u.a. auch die Rubrik «Datenbearbeitung», in der sich die Bank zur Bearbeitung der Personendaten äusserte. Wörtlich wurde dort ausgeführt: «Die Einwilligung zur Datenbearbeitung kann jederzeit widerrufen werden». Personen, die sich gegen eine solche Datenbearbeitung aussprachen, entgegnete die Bank, dass unter diesen Umständen kein Vertrag abgeschlossen werden könne. Zahlreiche Betroffene wandten sich an uns und baten um Rat.

Bereits 1999 intervenierten wir bei der Bank nicht nur wegen der missverständlichen Einwilligungsklausel, sondern sprachen uns auch dagegen aus, dass als weitere mögliche Datenempfänger die unbestimmte Umschreibung «zu der X Services Group gehörende Gesellschaften» verwendet wurde. Erst nach mehreren Briefwechseln erklärte sich die Bank im Herbst 1999 bereit, auf die missverständliche Einwilligungsklausel zu verzichten, und gestand den Kundinnen und Kunden das Recht zu, bei der Bank eine Aufstellung der zur X Services Group gehörenden Gesellschaften zu verlangen. Die

Bank versprach, die Rubrik Datenbearbeitung umgehend in diesem Sinne anzupassen.

Im Frühling 2001 konnten wir in mehreren Fällen feststellen, dass die Bank entgegen ihrer Zusage noch immer Antragsformulare mit dem ursprünglichen Text zur Datenbearbeitung benützte. Auf diesen Umstand angesprochen, versprach die Bank erneut, auf die missverständliche Einwilligungsklausel ab sofort zu verzichten. Gleichzeitig unterrichtete sie uns, dass sie sich entschieden habe, ihrer Kundschaft keine Aufstellung jener Unternehmen abzugeben, an welche die Bank die Personendaten weitergebe. Als uns nur wenige Wochen später wieder Kontoeröffnungsanträge mit dem ursprünglichen Text zur Datenbearbeitung vorgelegt wurden, wandten wir uns erneut an die Bank und wiesen bei dieser Gelegenheit nochmals darauf hin, dass der Verzicht auf eine Aufstellung aller zur X Services Group gehörenden Gesellschaften in verschiedenster Hinsicht gegen das Datenschutzrecht verstosse.

Wir legten der Bank dar, dass eine betroffene Person ohne genaue Kenntnis der künftigen Datenempfänger nicht frei entscheiden kann, ob und wem die Personendaten zugetragen werden sollen. Damit wird das Recht der informationellen Selbstbestimmung verletzt. Zudem verkannte die Bank, dass das Transparenzprinzip als fundamentaler datenschutzrechtlicher Grundsatz seine Wirkung nicht erst im Zeitpunkt einer allfällig verlangten Auskunftserteilung zu entfalten hat, sondern bereits ab dem Moment, in dem die Bearbeitung von Personendaten aufgenommen wird, uneingeschränkt berücksichtigt werden muss. Unsere Empfehlung in diesem Sinne hat die Bank angenommen.

10. Statistik und Forschung

10.1. Durchführung der Volkszählung 2000

Seit dem 5. Dezember 2000 bezogen sich unsere Kontrolltätigkeiten im Rahmen der Bearbeitung der Daten der Volkszählung 2000 auf folgende Aspekte: Plausibilität, Vervollständigung, Vollzähligkeitserhebung, Datenrückfluss an die Kantone zum Zweck der Harmonisierung, Anonymisierung und Vernichtung der Daten.

Der rechtliche Rahmen, der Vordruck der Fragebögen für die Volkszählung 2000, die Tätigkeiten des Dienstleistungszentrums DCL und der Kontrollgruppe Kantone/Bund sowie unsere ersten Besuche bei den verschiedenen Datenbearbeitungsstellen wurden in den vorangegangenen Tätigkeitsberichten beschrieben (5. Tätigkeitsbericht 1997/1998, S. 58, 6. Tätigkeitsbericht 1998/1999, S. 113, 7. Tätigkeitsbericht 1999/2000, S. 63 und 8. Tätigkeitsbericht 2000/2001, S. 54).

Die weiteren Kontrolltätigkeiten fanden im Bundesamt für Statistik (BFS), im Dienstleistungszentrum DCL und in dem von der Firma Demoscope AG betriebenen Call Center statt.

BFS

Um die Produktion und die Entwicklung des Projektes überwachen zu können, verfügt das BFS über einen Zugang zur Datenbank des Dienstleistungszentrums DCL. Im März 2001 haben wir die Anlagen besichtigt und festgestellt, dass sie vom Informatiknetz des BFS physisch getrennt sind. Darüber hinaus sind die Daten, auf die das BFS in diesem Rahmen zugreifen kann, anonymisiert. Unserer Ansicht nach waren dies geeignete Massnahmen zur Gewährleistung des Datenschutzes.

DCL

Der Betrieb der Anlagen und die Arbeit im Dienstleistungszentrum DCL wurden im April 2001 nochmals kontrolliert. Dabei haben wir die Verbesserung der Protokollierung vor allem für Mitarbeiter mit besonderen Zugriffsrechten verlangt. Im Übrigen haben wir eine Zwischenbilanz erstellt und zusammen mit dem externen Kontrollorgan die Auffassung vertreten, dass angesichts der vorhandenen Datenschutzmassnahmen die Missbrauchsgefahr äusserst gering ist.

e-census

Ungefähr 4% der Bevölkerung hat das System e-census verwendet, das zum ersten Mal die Möglichkeit bot, die Fragebögen der Volkszählung per Internet auszufüllen und einzureichen. Ein Bearbeitungsreglement wurde aufgestellt und das System durch ein externes Kontrollorgan überprüft. Kurz nach seiner Inbetriebnahme ist das System aufgrund von Netzüberlastung zusammengebrochen. In Folge dieser Funktionsstörung war der Zugang zum System nicht mehr möglich. Doch war die Panne nur von kurzer Dauer und wiederholte sich später auch nicht mehr. Ende März 2001 wurde das System unter der Aufsicht der Einheit für Informatikstrategie des Bundes und des externen Kontrollorgans vom Netz genommen. Generell wurden keine Anomalien festgestellt, welche die Datensicherheit gefährden könnten.

Plausibilität und Vervollständigung

Im April 2001 haben wir die Einrichtungen des Call Centers der Firma Demoscope AG besucht, die mit dem Einholen fehlender Informationen und der Korrektur unglaubwürdiger Angaben in den Fragebögen der Volkszählung 2000 beauftragt war. Für diese Tätigkeiten waren unserer Ansicht nach ausreichend Schutzmassnahmen getroffen worden. Die Tätigkeiten wurden kurz danach begonnen und Mitte Oktober 2001 abgeschlossen.

Vollzähligkeitserhebung

Zum ersten Mal sah die Schweizer Gesetzgebung nach der Durchführung der Volkszählung eine Vollzähligkeitserhebung vor, um die Qualität der erhobenen Daten zu prüfen. Das BFS hat das Unternehmen IHA GfM mit dieser Aufgabe betraut. Für die Erhebung galten dieselben datenschutzrechtlichen Vorschriften wie für die Volkszählung. Sie wurde hauptsächlich durch Stichproben per Telefon bei 27'000 Haushalten (ca. 60'000 Personen) durchgeführt.

Befragung per Telefon und Datenschutz

Manche der von IHA GfM oder Demoscope AG telefonisch befragten Personen haben sich bei unserem Sekretariat erkundigt, ob die weiter oben erwähnten telefonischen Nachforschungen (Vervollständigung, Plausibilität und Vollständigkeitserhebung) offiziell und legal seien. Insbesondere interessierte sie die Frage, wie sie sich vor Hochstaplern schützen konnten. Um auf derartige Fragen zu antworten, richtete das BFS eine Hotline ein. Die Telefonisten und Telefonistinnen erhielten präzise Anweisungen, wie sie sich zu melden hatten, um sich zu legitimieren. Sie mussten insbesondere ihren Namen und den Namen des Unternehmens nennen und den durch das BFS erteilten Auftrag erklären. Wo nach wie vor Zweifel bestanden, prüfte das BFS anhand der Uhrzeit des fraglichen Anrufs, ob dieser tatsächlich von einem Angestellten geführt worden war. Nachdem wir es selbst getestet hatten, wurde das System von uns für sicher befunden.

Anonymisierung und Vernichtung der Daten der Volkszählung 2000

Laut dem Bundesgesetz über die Volkszählung müssen die Nachführung und Korrektur kommunaler und kantonaler Einwohnerregister sechs Monate nach Abschluss der Datenerhebung beendet sein. Der Aufbau des eidgenössischen Gebäude- und Wohnungsregisters ist gleichzeitig mit der Datenbereinigung abgeschlossen.

Nach unseren Informationen wurde die Datenerhebung Ende 2001 abgeschlossen (Ende des Vervollständigungsverfahrens). Die Anonymisierung und Vernichtung der Daten der Volkszählung 2000 haben daher in der Zwischenzeit und spätestens ab Erreichung des Bearbeitungsziels zu erfolgen. Ein Konzept für die Vernichtung und Anonymisierung der Daten befindet sich im Bearbeitungsreglement für die Volkszählung 2000.

Das externe Kontrollorgan hat uns mehrere Bestätigungen über die Vernichtung der Daten zukommen lassen, die sich noch im Besitz der an den Vordrucken der Fragebögen beteiligten Unternehmen befanden. Dasselbe gilt für die Daten im Besitz der Firma Bee Company (Betreiberin der Hotline während der Volkszählung, siehe 8. Tätig-

keitsbericht 2000/2001, S. 54) und der Firma Demoscope AG. Die Vernichtung der Daten bei der Firma IHA GfM hat noch nicht begonnen, da die Vollständigkeitserhebung erst im Laufe von 2002 abgeschlossen wird und die in diesem Rahmen erhobenen Daten noch mit jenen der Volkszählung abgeglichen werden müssen.

Unsere Aufgabe wird somit darin bestehen, darüber zu wachen, dass das Anonymisierungskonzept und die Datenvernichtung ordnungsgemäss und innerhalb der gesetzlich vorgeschriebenen Frist durchgeführt werden.

Datenrückfluss an die Kantone und Gemeinden zum Zweck der Harmonisierung

Der Rückfluss der Daten der Volkszählung 2000 an Kantone und Gemeinden zur Harmonisierung der Register hat Ende 2001 begonnen. Im Rahmen der Nachführung der kantonalen und kommunalen Register können Einzelpersonen keine Strafe auferlegt werden. Das System für den Datenrückfluss zum Zweck der Harmonisierung der kantonalen und kommunalen Register wurde durch das externe Kontrollorgan überprüft. Für die Kontrolle der Bearbeitung der Daten der Volkszählung 2000 durch die kantonalen und kommunalen Stellen hingegen sind die zuständigen kantonalen Behörden verantwortlich.

10.2. Harmonisierung der Personenregister

In der neuen Bundesverfassung wurde im Sinne einer Klarstellung die Bundeskompetenz für die amtliche Statistik statuiert. Im gleichen Statistikartikel wurde eine neue Bundeskompetenz geschaffen, wonach der Bund Vorschriften betreffend amtliche Register erlassen darf, um den Erhebungsaufwand gering zu halten.

Das Anliegen der Statistiker, Erhebungen möglichst rationell zu gestalten ist wohl allseitig unbestritten. Dem entspricht die Folgerung, und das ist der Grund für die Bundeskompetenz bezüglich Registerharmonisierung, dass die in kantonalen Registern schon vorhandenen Daten nicht durch spezielle Erhebungen mittels Fragebogen nochmals erhoben werden sollen. Wie geht man nun aber vor beim Harmonisieren der Register? Um gleich auf den für uns zentralen Punkt hinzuweisen: Als erstes schafft man eine Nummer für jede Einwohnerin und jeden Einwohner, um diese eindeutig und lebenslänglich zu identifizieren (PIN). Das allein schon ist sehr schwer verständlich und ein widersprüchliches Verhalten des Bundesamtes für Statistik, welches im Anschluss an die Volkszählung 2000 verlauten lässt, eine PIN entspreche nicht der schweizerischen Kultur und bereits mit dem jetzt angestrebten Methodenwechsel könne ein grösseres Sparpotential realisiert werden. Diese Aussage ist auch heute noch Im WWW präsent (vgl. http://www.census.ch/chap02/dmodernisierung.html). Für

den Datenschutz wiegt aber die Tatsache ebenso schwer, dass das Bundesamt unter dem Titel «Koordination mit anderen Projekten» die weitere Verwendung des angestrebten PIN in nicht-statistischen Anwendungen vorantreibt. Dass diese administrativen Bearbeitungen unter persönlichkeitsrechtlicher Betrachtung von ganz anderer Qualität sind als die statistischen wird einfach übergangen und die erforderliche politische Diskussion über die Frage, ob ein universeller PIN für administrative Zwecke in der Schweiz eingeführt werden soll, schlicht ausgelassen. Wichtigste Folgerung aus dieser Situation ist, dass die PIN-Frage aus dem Projekt des Bundesamts für Statistik zu entfernen ist.

11. International

11.1. Europarat

11.1.1. Arbeiten der CJPD: Datenschutz und Videoüberwachung, Datenschutz, Polizeidaten und gerichtliche Daten in Strafsachen

Die Projektgruppe für den Datenschutz (CJPD) tagte vom 10. bis zum 12. Oktober 2001 und setzte die Arbeiten im Bereich Videoüberwachung und Chipkarten fort.

Die CJPD beendete die erste Lesung des Entwurfs zu Leitgrundsätzen zum Schutz der Personen bei der Datenbeschaffung und -bearbeitung per Videoüberwachung (siehe 8. Tätigkeitsbericht 2000/2001, S. 86). Die Arbeiten der CJPD standen im Zeichen der Ereignisse vom 11. September 2001. So forderten bestimmte Staaten, die Videoüberwachungstätigkeiten der Polizeibehörden vom Anwendungsbereich der Leitgrundsätze auszuklammern. Mit der Mehrheit der anwesenden Sachverständigen sprachen wir uns gegen diesen Ansatz aus, zumal die Leitgrundsätze ja den Einsatz der Videoüberwachung zu polizeilichen Zwecken nicht grundsätzlich verbieten, sondern garantieren sollen, dass bei diesen Tätigkeiten das Gleichgewicht zwischen Sicherheitsbedürfnis und Achtung der Rechte und grundlegenden Freiheiten – vor allem des Rechts auf Privatleben – gewahrt bleibt.

Die CJPD nahm den Sachverständigenbericht über den Schutz von personenbezogenen Daten betreffend die Verwendung von Chipkarten zur Kenntnis und beschloss, auch in diesem Bereich Leitgrundsätze aufzustellen. Daneben wurde die CJPD über die Fortschritte der Arbeitsgruppe über den Schutz von Polizeidaten und gerichtlichen Daten in Strafsachen informiert (siehe unten). Es ist nicht ausgeschlossen, dass die CJPD die Empfehlung Nr. (87) 15 zur Regelung der Verwendung personenbezogener

Daten im Polizeibereich überarbeitet. Ausserdem wurde die CJPD über den Stand der Fortschritte der Arbeitsgruppe über Humangenetik, welche ein Zusatzprotokoll zum Übereinkommen des Europarates über Menschenrechte und Biomedizin ausarbeiten soll, informiert. Schliesslich erörterte sie zusammen mit dem T-PD anlässlich einer gemeinsamen Sitzung die Zukunft der Ausschüsse des Europarates, die sich um den Datenschutz kümmern. Langfristig sollten die beiden Ausschüsse zusammen gelegt werden und einen erweiterten konventionellen Ausschuss bilden.

11.1.2. Arbeiten des T-PD: Vertragsklauseln, Auswertung des Übereinkommens 108, Konsequenzen der Attentate vom 11. September 2001

Der Beratende Ausschuss des Übereinkommens 108 (T-PD) hielt vom 8. bis zum 9. Oktober 2001 seine 17. Tagung ab, auf welcher er die Arbeiten zu den Vertragsklauseln und die Evaluation des Übereinkommens fortsetzte.

Der T-PD setzte – unter schweizerischem Vorsitz – die Evaluation des Übereinkommens 108 fort. Dabei soll ermittelt werden, ob diese internationale Urkunde, die ihr 20-jähriges Bestehen feierte, per Änderungen oder per Annahme von Zusatzprotokollen aktualisiert werden muss. Diese Evaluation stand im Mittelpunkt der Europäischen Konferenz über den Datenschutz mit dem Thema «Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten: Gegenwart und Zukunft», die am 19. und 20. November 2001 in Warschau tagte (siehe http://www.legal.coe.int/dataprotection). Die Konferenz gelangte zum Schluss, dass das Übereinkommen nach wie vor relevant bleibt und dass im Moment keine substantielle Überarbeitung in Betracht zu ziehen ist.

Der T-PD verzichtete auf eine Revision des im Jahr 1992 angenommenen «Mustervertrags für die Sicherstellung eines gleichwertigen Datenschutzes im Rahmen des grenzüberschreitenden Datenverkehrs», um Doppelspurigkeiten zu den Arbeiten anderer internationaler Gremien, insbesondere der Kommission der Europäischen Gemeinschaften, zu vermeiden. Dagegen beschloss er, Leitlinien oder -grundsätze auszuarbeiten, die in den Verträgen über den Transfer von Personendaten zwischen den Vertragsparteien des Übereinkommens 108 und Drittstaaten ohne angemessenes Schutzniveau zu berücksichtigen sind. Diese Leitlinien sollen in einen Leitfaden aufgenommen werden.

Der T-PD führte ausserdem einen Meinungsaustausch zur Situation nach den Anschlägen vom 11. September 2001 durch. Dabei nahm er die Erklärung des Präsidenten mit folgendem Wortlaut zur Kenntnis:

«Wir sind alle erschüttert über die schrecklichen terroristischen Anschläge, die Amerika am 11. September 2001 in Trauer stürzten. Ebenso unerträglich war das Attentat in der Schweiz vom 27. September gegen das Parlament des Kantons Zug sowie jenes, das am 1. Oktober gegen das indische Parlament begangen wurde. Neben den Tausenden unschuldiger Opfer und ihren Familien treffen und betreffen diese verheerenden und grauenvollen Verbrechen uns alle, denn sie verletzen die Menschenrechte und die Demokratie. Die Brutalität und Sinnlosigkeit der Verbrechen haben die Welt dauerhaft verändert. Kriminalität und Cyberkriminalität sind wirklicher denn je. Wir sind uns alle einig, dass der Terrorismus bekämpft werden muss, aber die einzusetzenden Mittel und die Analyse der Bedürfnisse unterscheiden sich. Eine Intensivierung des Kampfs gegen den Terrorismus – vor allem durch verbesserte Mechanismen und Mittel der Zusammenarbeit unter den Staaten und den internationalen Organisationen – erweist sich womöglich als unumgänglich. Diese legitime Schlacht muss jedoch mit den Waffen der Demokratie und des Rechtes geschlagen werden.

Nach den tragischen Ereignissen forderten mehrere Stimmen in den Vereinigten Staaten und in Europa, den Schutz der Privatsphäre zu hinterfragen, und hielten dem Datenschutz vor, Verbrecher zu schützen und die Attentate überhaupt zugelassen zu haben. Es wurden restriktive Massnahmen vorgeschlagen. Gesetzesentwürfe sind in Vorbereitung. Anlässlich der 23. Internationalen Konferenz der Beauftragten für den Datenschutz, die vom 24. bis zum 26. September unter dem Motto «Privatsphäre – Menschenrecht» in Paris stattfand, wurde gefordert, eine vorsichtige und verantwortliche Haltung zu bewahren. Wir müssen das Gleichgewicht zwischen der Sicherheit von Menschen und Gütern und der Achtung der individuellen Freiheiten – vor allem Privatleben und Datenschutz – gewährleisten. Dabei handelt es sich sicherlich um eine Gratwanderung, wobei jedoch zu bedenken ist, dass exzessive Beschränkungen der Grundrechte unsere Freiheiten dauerhaft beeinträchtigen, die Demokratie nachhaltig schwächen und damit dem Terrorismus Vorschub leisten würden.

Der Europarat steht mehr denn je in der Pflicht, insbesondere mit unserem Ausschuss eine aktive Rolle in der Förderung und Verteidigung des Rechts auf Datenschutz zu spielen. Privatsphäre ist ein Menschenrecht. Der Datenschutz wird zu einem nicht wegzudenkenden Bestandteil des universalen Bürgerseins und stellt als solcher ein Menschenrecht dar. Artikel 9 des Übereinkommens 108 gestattet Ausnahmen von einigen Konventionsbestimmungen, falls sie im Gesetz vorgesehen sind und in einer demokratischen Gesellschaft eine notwendige Massnahme zum Schutz der Staatssicherheit, zur inneren Sicherheit und zur Verfolgung von Straftaten bilden. Bereits heute verfügen die Polizeibehörden und die Behörden, die das organisierte Verbrechen bekämpfen, über umfassende Untersuchungsmittel und sind legitimiert, die für ihre in Anwendung von Artikel 9 ergriffenen Aktionen notwendigen Personendaten zu bear-

beiten. Bevor neue Ausnahmen in Betracht gezogen werden, ist zu überprüfen, ob die Attentate wirklich mit dem Fehlen von Mitteln zusammenhängen: Alles deutet darauf hin, dass die festgestellten Defizite beim Einsatz der existierenden Mittel und bei der Analyse der verfügbaren Informationen, nicht dem Datenschutz angelastet werden dürfen. Sollten zusätzliche Massnahmen künftig erforderlich sein, so dürfen sie keinen Blankoscheck darstellen, sondern müssen gründlich überprüft werden, dem Verhältnismässigkeitsprinzip genügen, einem allgemeinen Interesse von überwiegender Bedeutung entsprechen und den Grundsatz der Gesetzmässigkeit beachten.

Angesichts der Globalisierung des Handels, der weltweiten Entwicklung der Kommunikationsnetze und der dadurch hervorgerufenen Risiken haben wir beim Streben nach dem richtigen Gleichgewicht zwischen den Imperativen Sicherheit und Garantie des Rechts auf Datenschutz, das immer universaler werden muss, eine Schlüsselrolle zu spielen. Wir müssen gegenüber den Versuchungen Einiger, unbedachte und übereilte Massnahmen zu ergreifen, die ein unumkehrbares Ungleichgewicht auslösen könnten, auf der Hut sein. Wir haben nicht das Recht, im Namen der Sicherheit über Grundsätze und Grundfreiheiten hinwegzusehen, die Wesensmerkmale der Rechtsstaaten bilden. Sollten neue Einschränkungen eingeführt werden, so müssten sie zeitlich befristet sein und mit Garantien einhergehen, damit nicht unschuldige Bürger darunter leiden. Eine Schwächung des Datenschutzes führt nicht unbedingt zu grösserer Sicherheit für die Einzelnen. Im Rahmen der Tagung könnte der T-PD die wichtige Rolle des Datenschutzes bei der Verteidigung der Demokratie erneut betonen und an die Rolle des T-PD erinnern. Zur Garantie des Gleichgewichts zwischen Achtung von Rechten und Grundfreiheiten und Sicherheit könnten wir damit unseren Willen bekunden, konstruktiv an der Prüfung von möglichen Massnahmen zur Stärkung des Kampfs gegen den Terrorismus und das organisierte Verbrechen mitzuwirken, falls sich solche Massnahmen als notwendig erweisen».

Der T-PD wies darauf hin, dass der Schutz von Personendaten die Untersuchung und Verfolgung von Straftaten und den Kampf gegen den Terrorismus nicht ausschliesse; die Notwendigkeit der Terrorismusbekämpfung und die Achtung der Grundrechte und -freiheiten, vor allem des Rechts auf Privatsphäre, müssen jedoch im Gleichgewicht bleiben. Unverhältnismässige Massnahmen könnten diese Rechte nachhaltig, ja unwiderrufbar beeinträchtigen. Daher plädierte der T-PD für die Berücksichtigung der Datenschutzregelung im Rahmen der Prüfung der von den Europäischen Justizministern vorgeschlagenen Normativmassnahmen.

11.1.3. Arbeitsgruppe des Europarates für den Datenschutz bei Polizeidaten und gerichtlichen Daten in Strafsachen

Die Arbeitsgruppe für den Datenschutz bei Polizeidaten und gerichtlichen Daten in Strafsachen (CJPD/GTPJ) wurde von der Projektgruppe für Datenschutz des Europarates (CJPD) beauftragt, die Auswirkung der Datenschutzgrundsätze auf die Gerichts- und Polizeizusammenarbeit in Strafsachen zu untersuchen.

Im Rahmen des ersten Mandatsteils prüfte die Arbeitsgruppe die Folgen der Datenschutzprinzipien für die gerichtliche Zusammenarbeit in Strafsachen und entwickelte gemeinsame Grundsätze, die bei Rechtshilfeersuchen an Länder ohne angemessenen Datenschutz zu berücksichtigen sind.

Daneben führte die Arbeitsgruppe im Jahr 2002 die dritte Evaluation der Empfehlung Nr. (87) 15 des Europarates über die Verwendung von personenbezogenen Daten im Polizeiwesen durch. Diese dritte Beurteilung muss die beiden ersten Evaluationen sowie die Ergebnisse des Seminars über den Datenschutz im Polizeiwesen, das im Dezember 1999 in Strassburg stattfand, berücksichtigen. Die Evaluation darf sich nicht auf die Themen beschränken, die in der Empfehlung Nr. (87) 15 aufgeführt werden, sondern muss auch die neuen aktuell gewordenen Themen und die neuen Polizeitechnologien erfassen.

11.1.4. Entwurf eines Protokolls über genetische Untersuchungen beim Menschen

Die Arbeiten zum Protokoll über genetische Untersuchungen beim Menschen wurden fortgeführt. Es wurde definitiv entschieden, dass der Geltungsbereich des Protokolls auch den Arbeits- und Versicherungsbereich umfassen soll.

Das Protokoll über genetische Untersuchungen ist ein Zusatzprotokoll zum Übereinkommen des Europarates über Menschenrechte und Biomedizin (Konvention von Oviedo). Das Protokoll hat zum Ziel, jegliche Diskriminierung aufgrund des Erbgutes auszuschliessen (siehe auch 8. Tätigkeitsbericht 2000/2001, S. 89). Die sechste und siebte Tagung der Arbeitsgruppe fand vom 3. bis 5. April bzw. vom 17. bis 19. Oktober 2001 in Strassburg statt.

An diesen beiden Tagungen wurde das Kapitel über den Gesundheitsbereich nochmals überarbeitet. Die Arbeitsgruppe erkannte schliesslich, dass genetische Untersuchungen nur dann zulässig sein sollen, wenn diese mit einer genetischen Beratung beglei-

tet werden. In einem solch sensiblen Gebiet muss die betroffene Person umfassend aufgeklärt werden. Die Forderung nach Transparenz ist nicht nur ein datenschutzrechtliches Postulat, sondern auch aus medizinisch-ethischer Sicht unabdingbar. Insbesondere ist die betroffene Person über den Zweck und die Natur der Datenbearbeitung, mögliche Risiken und die Diagnose zu informieren. Entscheidend ist auch, der betroffenen Person Möglichkeiten der Unterstützung aufzuzeigen, die sich im Zusammenhang mit dem Untersuchungsergebnis ergeben können.

Bis anhin fehlen Bestimmungen im Protokollentwurf, welche den Staaten die Einrichtung von Ethikkommissionen im Bereich der Human-Genetik vorschreiben würde. Solchen Ethikkommissionen käme etwa die Aufgabe zu, Massstäbe für die Qualitätskontrolle von genetischen Untersuchungen zu erarbeiten.

Im Weiteren beschloss die Arbeitsgruppe, dass der Geltungsbereich des Protokolls auch den Versicherungs- und Arbeitsbereich einschliessen soll. Aus datenschutzrechtlicher Sicht ist dies zu begrüssen, ist doch die Gefahr von möglichen Diskriminierungen gerade in diesen Bereichen nicht von der Hand zu weisen. Der gegenwärtige Protokollentwurf sieht vor, dass genetische Tests im Arbeitsbereich grundsätzlich verboten sind. Ausnahmen davon sollen nur dann möglich sein, wenn gewisse Gesundheitsrisiken, welche im Zusammenhang mit der Arbeitsstelle zusammenhängen, nicht anderweitig vermieden werden können.

An den nächsten Sitzungen soll definiert werden, ob und unter welchen Voraussetzungen Gentests im Versicherungsbereich erlaubt sein sollen. Weitere Kapitel im Protokoll sind der Privatsphäre und der Information der Öffentlichkeit gewidmet.

11.2. Europäische Union

11.2.1. Europäische Konferenz der Beauftragten für den Datenschutz

Die Europäischen Datenschutzbeauftragten versammelten sich am 10. und 11. Mai 2001 zur Frühjahrskonferenz in Athen. Wir nahmen als Beobachter daran teil. Die Konferenz verabschiedete zwei Erklärungen: Die erste betrifft die Speicherung von Verkehrsdaten durch Internet Service Provider, die zweite bezieht sich auf die Grundrechtscharta der Europäischen Union, in welcher der Datenschutz als grundlegendes Menschenrecht anerkannt wird.

Zur Europäischen Konferenz der Beauftragten für den Datenschutz gehören die Datenschutzbeauftragten der Mitgliedsstaaten der Europäischen Union, Norwegens und Islands. Ungarn, Polen, die Tschechische Republik und die Schweiz haben einen Beob-

achterstatus inne. Die Konferenz bot Gelegenheit zu einem vertieften Meinungsaustausch zur Datenschutzpolitik und zur Entwicklung der Gesetzgebungen in den verschiedenen europäischen Ländern. Ausserdem mündete sie in der Ausarbeitung gemeinsamer Lösungen.

Die Konferenz von Athen befasste sich mit den Themen Kriminalität im Cyberspace, Telekommunikation, Internet, Schutz der Arbeitnehmer, Technologien zur Verstärkung der Vertraulichkeit von Informationen, Einwilligung, Schwarze Listen und E-Commerce. Die vorgängige Einwilligung in die Bearbeitung von Personendaten spielt im europäischen Datenschutzrecht eine Schlüsselrolle. Die Beauftragten beschäftigten sich mit der Frage, ob die Einwilligung als Ausdruck des Selbstbestimmungsrechts in Informationsbelangen im Bedarfsfall als Garantie zur Rechtfertigung der Bearbeitung von Personendaten ausreiche. Sie kam zum Schluss, dass die Einwilligung nicht alles rechtfertigt. Ihre Tragweite wird durch die Grundprinzipien des Datenschutzes wie Verhältnismässigkeit und Zweckbindung relativiert. Die Einwilligung darf die individuellen Rechte und Grundfreiheiten nicht verletzen oder die Rechte anderer Personen beeinträchtigen.

Im Zusammenhang mit dem Sektor Telekommunikation und Internet äusserten die Datenschutzbeauftragten Skepsis an Projekten, wonach Internet Service Provider die Randdaten länger aufbewahren, als für die Rechnungsstellung erforderlich ist, um den Vollzugsbehörden gegebenenfalls den Zugriff auf diese Daten zu ermöglichen. Die von der Konferenz verabschiedete Erklärung betont, dass eine solche Datenaufbewahrung die Grundrechte, welche Artikel 8 des Europäischen Menschenrechtskonvention jeder Person garantiert, und das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten aus dem Jahr 1981 beeinträchtigen würde; wenn Verkehrsdaten in Einzelfällen aufbewahrt werden müssen, muss der Bedarf nachgewiesen werden, die Aufbewahrungsfrist so kurz wie möglich sein und die Praktik gesetzlich klar geregelt werden.

Ausserdem verabschiedete die Konferenz eine Erklärung zu Artikel 8 der Grundrechtscharta der Europäischen Union. Darin unterstreichen die Datenschutzbeauftragten, dass diese Chartabestimmung die in jüngster Vergangenheit verabschiedeten Datenschutzbestimmungen stärkt, so dass der Datenschutz endlich als grundlegendes Menschenrecht anerkannt wird.

11.2.2. Europäische Arbeitsgruppe über die Behandlung von Klagen und den Informationsaustausch

Im Rahmen der Europäischen Konferenz der Beauftragten für den Datenschutz wurde eine Arbeitsgruppe eingesetzt, welche die Mittel zur Zusammenarbeit und Kooperation unter den Datenschutzkontrollbehörden bei der Prüfung der Klagen, die sie behandeln, und bei der Durchführung von Kontrollen untersuchen soll.

Die Europäische Konferenz der Beauftragten für den Datenschutz setzte eine Arbeitsgruppe ein (Complaints Handling Workshop), welche die unterschiedlichen Bearbeitungsmethoden von bei Datenschutzbehörden eingereichten Klagen untersuchen und die Zusammenarbeit der Behörden vorantreiben soll. Nach dem Beschluss, auch Staaten mit einzubinden, für welche eine Entscheidung der Kommission der Europäischen Gemeinschaften zur Angemessenheit des Datenschutzes existiert, nimmt die Schweiz auch an diesen Arbeiten teil.

Die Arbeitsgruppe verfolgt das Ziel, die Mittel zur Zusammenarbeit und Kooperation unter den Kontrollbehörden bei der Prüfung der Klagen, die sie behandeln, und bei der Durchführung von Kontrollen zu untersuchen. Dabei ist namentlich der exponentielle Anstieg der grenzüberschreitenden Datenbearbeitungsvorgänge zu berücksichtigen. In diesem Zusammenhang stellten wir anlässlich der Tagung von Lissabon im November 2001 das Kontrollprozesskonzept vor, das wir für unsere eigenen Überwachungstätigkeiten ausgearbeitet hatten. Mehrere nationale Datenschutzbehörden, die in der Durchführung der Kontrollen mit ähnlichen Problemen konfrontiert sind, beschlossen, zahlreiche Elemente aus unserem Konzept in ihre Überwachungsmechanismen zu übernehmen. Ausserdem wurde auf der Grundlage des schweizerischen Kontrollkonzepts eine vergleichende Studie zu den Kontrollverfahren in den verschiedenen Staaten eingeleitet. Die Arbeiten an den Etappen und Kontrollprozessen sollen anlässlich der nächsten, für das Jahr 2002 in Dublin geplanten Tagung fortgesetzt werden.

Zur Erleichterung des Informationsaustausches unter den Mitgliedsstaaten benutzt die Arbeitsgruppe das Informatiksystem CIRCA (Communication & Information Resource Centre Administrator). Es handelt sich um ein mit dem Programm IDA (Interexchange of Data between Administrations) der Europäischen Kommission verknüpftes gesichertes Extranetsystem mit eingeschränktem Zugang (Passwort). Ziel ist es, den Informationsaustausch über grenzüberschreitende Klagen, über die Ergebnisse vorgenommener Kontrollen und über nationale, für die übrigen Datenschutzbehörden interessante Erfahrungen zu fördern. Zahlreiche Teilnehmende an der Konferenz von Lissabon forderten, den Informationsaustausch nicht ausschliesslich auf die Mitglieder der

Europäischen Union zu beschränken, sondern das CIRCA-Informationssystem auch Staaten mit angemessenem Schutzniveau, wie die Schweiz, zu öffnen.

11.3. OECD

11.3.1. Arbeitsgruppe über die Informationssicherheit und Schutz der Privatsphäre (WISP)

Im vergangenen Geschäftsjahr konzentrierte sich die Arbeitsgruppe auf Online-Streitbeilegungsmechanismen, datenschutzfreundliche Technologien, genetische Untersuchungen, Verhaltensregeln im E-Commerce und auf die Konsequenzen der Ereignisse vom 11. September 2001.

Verschiedene Modelle für die aussergerichtliche Beilegung von Online-Streitigkeiten wurden der Arbeitsgruppe in Paris präsentiert und analysiert. Zuerst müssen Rechtsfragen im Zusammenhang mit grenzüberschreitenden Transaktionen analysiert werden, um insbesondere die Frage des anwendbaren Rechts bei auftretenden Streitigkeiten zu klären. Diese Aufgabe wir dadurch erschwert, dass einige Mitgliedstaaten bestrebt sind, mittels solcher Streitbeilegungsmechanismen den ordentlichen Rechtsweg auszuschliessen. Deshalb wird in einer ersten Phase anhand von bestimmten Richtwerten und Standards ein Inventar über alle Online-Streitbeilegungsmechanismen erstellt. In einer zweiten Phase wird die Tauglichkeit der verschiedenen Modelle abgeklärt.

Die Arbeitsgruppe betonte die Wichtigkeit von datenschutzfreundlichen Technologien (Privacy Enhacing Technologies PET) beim Schutz der Privatsphäre im Internet. An einem speziell dafür veranstalteten Forum wurden verschiedene PET vorgestellt. In letzter Zeit, sind sich Unternehmen zunehmend bewusst geworden, dass der Schutz der Privatsphäre ein wichtiger Faktor ist, um das Vertrauen der Konsumentinnen und Konsumenten in den E-Commerce zu gewinnen. Deshalb entwickeln Unternehmen zunehmend PET und stellen diese auch kostenlos zur Verfügung. Solche Technologien wurden der Arbeitsgruppe vorgestellt und die wesentlichsten Vorteile für Konsumenten und Internetbenutzer aufgezeigt. Gleichzeitig erkannte die Arbeitsgruppe, dass PET alleine für den Schutz der Privatsphäre nicht ausreichen. Zum einen können solche Technologien den gesetzlichen Schutz nicht ersetzen, zum anderen sind sie der breiten Öffentlichkeit zu wenig bekannt.

Bei den meisten PET-Produkten fehlen Informationen über den Hersteller und über die Funktionalität. Dies zwingt Anwendende solchen Technologien blindes Vertrauen zu schenken. Die Arbeitsgruppe bemängelte auch, dass die verschiedenen Sicherheits-

bedürfnisse der Internetbenutzenden von den Herstellern zu wenig berücksichtigt werden. Deshalb forderte die Arbeitsgruppe, dass bei der Entwicklung von datenschutzfreundlichen Technologien diese Voraussetzungen erfüllt und die unterschiedlichen Bedürfnisse der Anwendenden verstärkt berücksichtigt werden.

Die Arbeitsgruppe wird nun nach Lösungen suchen, wie die Aufmerksamkeit von Konsument und Internetnutzern für PET gewonnen werden kann. Dazu erstellt sie ein Dokument mit dem Ziel, über den sinnvollen Einsatz von PET-Technologien beim Schutz der Privatsphäre zu informieren.

Die Arbeitsgruppe hat sich auch mit genetischen Untersuchungen befasst. Sie hob hervor, dass genetische Daten viel sensibler sind und deshalb nicht in die Kategorie von medizinischen Daten eingeteilt werden dürfen, sondern besonders gehandhabt und geschützt werden müssen. Die Tatsache, dass genetische Daten nicht allein für den Betroffenen, sondern für die ganze Familie Konsequenzen haben können, wurde besonders hervorgehoben. Ein Stearing Commitee wird eine Übersicht erstellen, welche die verschiedenen Probleme bei der Bearbeitung von genetischen Daten unter Berücksichtigung der bereits geleisteten Arbeiten des Europarates zusammenfasst, um die zukünftigen Arbeiten der Arbeitsgruppe sinnvoll zu planen.

Im Zusammenhang mit den Arbeiten über Verhaltensregeln im E-Commerce hielten wir erneut fest, dass solche Regeln keine Alternative zu gesetzlichen Bestimmungen sind. Die Arbeitsgruppe erkannte aber, dass Verhaltensregeln die Umsetzung von gesetzlichen Verpflichtungen transparenter gestalten können. Um die Effektivität solcher Regeln analysieren zu können, wird ein Inventar der verschiedenen Modelle erstellt. Dieses Inventar wird abklären helfen, welche Verhaltensregeln den Prinzipien der OECD genügen, um die Wirksamkeit der Durchsetzungsmechanismen zu analysieren und die Voraussetzungen, die für die Erstellung von Verhaltensregeln notwendig sind, zu bestimmen. Wir haben die Arbeitsgruppe informiert, dass der EDSB bereits zu Verhaltensregeln und zur Privatsphäre im E-Commerce Stellung genommen hat (siehe http://www.edsb.ch/d/themen/e-commerce/index.htm).

Die Arbeitsgruppe diskutierte ausführlich über die Konsequenzen der Ereignisse vom 11. September 2001. Es bestand Einigkeit, dass trotz dieser terroristischen Ereignisse die Ziele und Arbeiten der Arbeitsgruppe von Pragmatismus und Sachlichkeit geprägt sein müssen. Deshalb konzentriert sich die Arbeitsgruppe auf die Überarbeitung der Richtlinie über die Datensicherheit, weil sich die Situation im Sicherheitsbereich seit der Verabschiedung der Richtlinien im Jahr 1992 radikal geändert hat. Die technologieneutralen Prinzipien der Richtlinie werden beibehalten, sie wird aber dem heutigen Umfeld der globalen und vernetzten Systeme angepasst.

11.4. Weitere Themen

11.4.1. Internationale Konferenz der Beauftragten für den Datenschutz

Die XXIII. Internationale Konferenz der Datenschutzbeauftragten fand vom 24. bis zum 26. September 2001 in Paris statt. An der Veranstaltung unter dem Motto «Privatsphäre – Menschenrecht» beteiligten sich Delegationen aus rund 50 Staaten von fünf Kontinenten. Die Konferenz bestätige die Universalität des Rechts auf Datenschutz. Die Datenschutzbeauftragten verabschiedeten ein neues Akkreditierungsverfahren für an der internationalen Konferenz teilnahmeberechtigte Datenschutzbehörden.

Die XXIII. Internationale Konferenz der Datenschutzbeauftragten wurde in der Universität Sorbonne in Paris abgehalten. Mehr denn je stand der Mensch als Bürger, Arbeitnehmer, Patient, Verbraucher, Internetnutzer und Einzelperson im Mittelpunkt der Diskussionen. Die Konferenz war als breites Forum für Grundrechte und Freiheiten konzipiert. Obwohl die tragischen Ereignisse vom 11. September bei den Teilnehmenden stark präsent waren und auch die Diskussionen überschatteten, wies die Konferenz nachdrücklich darauf hin, dass Privatleben ein Menschenrecht sei, dass der Datenschutz sich zu einem unverzichtbaren Bestandteil des Bürgerseins entwickle und mithin ein Menschenrecht darstelle. Angesichts der Globalisierung und der weltweiten Dimension der Bearbeitung von Personendaten sollte das Grundrecht auf Datenschutz durch die Entwicklung gemeinsamer Regeln zur Universalität tendieren. Die Sicherheit von Personen und Gütern, insbesondere der Kampf gegen den Terrorismus, sind legitime und unumstrittene Anliegen, dürfen aber nicht zu unbedachten Massnahmen führen, welche die individuellen Rechte und Freiheiten untergraben würden. Das Recht auf Privatleben braucht nicht eingeschränkt zu werden, um die Sicherheit zu stärken; die strikte Anwendung der Datenschutzgesetze kann im Gegenteil grössere Sicherheit bieten. Unter den aktuellen Umständen müssen bestimmte unüberlegte oder übereilte Entgleisungen im Spannungsfeld Sicherheit und Freiheit aufmerksamer und wachsamer mitverfolgt werden. Solche Entgleisungen könnten die Basis unserer Demokratien dauerhaft schädigen. Daher muss unbedingt das richtige Gleichgewicht zwischen Sicherheitsbedürfnis und Achtung der individuellen Freiheiten gefunden werden.

Anlässlich der in Plenarsitzungen und Workshops organisierten Konferenz wurde die Bilanz zur Entwicklung des Einsatzes von Informationstechnologien generell und nach Sektoren gezogen. Ausserdem bot die Konferenz den Datenschutzbeauftragten die Gelegenheit, sich mit den Anliegen zahlreicher Akteure der Informationsgesellschaft vertraut zumachen. Neue Risiken wurden identifiziert, insbesondere in Bezug auf die Videoüberwachung mit Gesichtserkennung, Cyberüberwachung, Ortungstechniken

und Biometrie. Ausserdem wurde daran erinnert, dass die Technologien auch eine Chance für den Schutz des Privatlebens bieten. In diesem Sinne haben die Datenschutzbeauftragten in der Ausbildung, der Sensibilisierung und Förderung dieser Technologien und der Schutzinstrumente, deren Entwicklung sie begleiten sollen, eine aktive Rolle zu spielen. Dazu müssen die Konzeptentwickler die Auflagen des Datenschutzes rechtzeitig einbeziehen und die zuständigen Behörden konsultieren.

Anlässlich der Plenarsitzung «Privatsphäre – Arbeitsleben» hatten wir die Gelegenheit, die Ergebnisse unserer Untersuchungen zu den Drogentestes am Arbeitsplatz vorzustellen. Dabei erinnerten wir an Folgendes:

- Zahlreiche Unternehmen führen bei ihren Beschäftigten bzw. bei bestimmten Kategorien Drogentests durch. Diese bilden einen Eingriff in das Privatleben des Betroffenen, einen Verstoss gegen das Arbeitsrecht und sie setzen sich über die geltende Drogenpolitik hinweg. Ausserdem ist die Zuverlässigkeit der Testresultate nicht erwiesen. Mit dem Test werden nicht die Verhaltensänderungen wegen Drogenkonsum gemessen, weshalb sie nicht zur Beurteilung der Arbeitstauglichkeit einer Person eingesetzt werden können.
- Der Akzent sollte vorrangig auf Information und Schulung liegen, um den Verantwortungssinn der Angestellten, die Schlüsselposten in der Sicherheit besetzen, zu schärfen.
- Angezeigt sind ausserdem Begleit- und Sensibilisierungsprogramme, um positive Entwicklungen zu erzielen, ohne Drogentests einzusetzen.
- Drogentests werden nur bei Vorliegen eines wesentlichen Sicherheitsrisikos für Personen, Güter oder die Umwelt geduldet, sofern andere Präventionsmittel nicht ausreichen und sofern mit Massnahmen, die das Privatleben weniger stark tangieren (insbesondere Supervision), nicht sichergestellt werden kann, dass der Arbeitnehmer kein Sicherheitsrisiko darstellt.
- Drogentests rechtfertigen sich nicht für Stellen, die für die Sicherheit nicht entscheidend sind.
- Die Tests sind unter Schutz der Vertraulichkeit und Achtung des Arztgeheimnisses durchzuführen. Mangels Gesetzesbestimmungen ist die freie, spezifische und ausdrückliche Einwilligung der betroffenen Personen erforderlich.
- Die Tests dürfen jedoch nicht allein auf der Einwilligung der betroffenen Personen beruhen. Der Gesetzgeber sollte den entsprechenden Rahmen festlegen. Ausserdem sollten alle Gruppen von Beschäftigten, die einen Arbeitsplatz mit einem wesentlichen Sicherheitsrisiko besetzen, erfasst werden.

- Der Gesetzgeber müsste zudem die Substanzen präzisieren, die zu einem erhöhten Risiko führen, die Berufsgruppen definieren, für welche ein Leistungsabfall wegen Drogenkonsums eine gravierende Gefahr bildet, und die Liste der Drogen erstellen, die kurz- oder langfristig erwiesenermassen zu einem Leistungsabfall führen.

Anlässlich einer Sitzung im ausschliesslichen Kreis der Datenschutzbeauftragten wurde ein neues Akkreditierungsverfahren für Datenschutzbehören im Rahmen der internationalen Konferenz verabschiedet (siehe Anhang, S. 124). Die Konferenzunterlagen können an folgender Adresse abgerufen werden: http://www.paris-conference-2001.org .

11.4.2. 30. Sitzung der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation

Der EDSB hat an der Herbstsitzung der Arbeitsgruppe, die zweimal jährlich tagt, vom 27. bis 30 August 2001 in Berlin teilgenommen. Neben dem Austausch der neusten nationalen Entwicklungen im Telekommunikationsrecht und im Bereich des Internets standen namentlich die Themen electronic voting, online-profiling sowie die Überwachung der Internetaktivitäten am Arbeitsplatz zur Diskussion.

Traditionsgemäss veranstaltete der Berliner Beauftragte für Datenschutz und Informationsfreiheit im Rahmen der Internationalen Funkausstellung ein Symposium, das unter dem Titel «Datenschutz und geistiges Eigentum im Internet» stand. Weitere Informationen finden Sie im Internet unter
http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm sowie
http://www.datenschutz-berlin.de/infomat/heft29/index.htm.

12. Der Eidgenössische Datenschutzbeauftragte

12.1. Die achte schweizerische Konferenz der Datenschutzbeauftragten

Die achte schweizerische Konferenz der Datenschutzbeauftragten fand am 22. November 2001 in Bern statt, organisiert vom Datenschutzbeauftragten des Kantons Bern. Teilgenommen haben Vertreter kantonaler Datenschutzbehörden sowie Datenschutzberater eidgenössischer Departemente.

Wir erläuterten die Situation im Bereich der inneren Sicherheit nach den Ereignissen vom September und hielten fest, dass die Privatsphäre der Bürgerinnen und Bürger durch die Erweiterung der öffentlichen Aufgaben zunehmend gefährdet ist, da mehr

Informationen bearbeitet werden. Um Missbräuche bei diesen neuen Aufgaben zu vermeiden, verlangten wir nebst dem Ausbau der Aktivitäten im Bereich der inneren Sicherheit auch die Verstärkung der Kontrollmechanismen.

Der Schwerpunkt der Konferenz galt der Rolle der Datenschutzbeauftragten bei Informatikprojekten. Projektleiter und -sicherheitsleute hielten fest, dass der frühe Einbezug der Datenschutzbeauftragten in Informatikprojekte von erheblicher Bedeutung ist. Dadurch können Gefahren für die Persönlichkeitsrechte der Betroffenen rechtzeitig erkannt, Zugriffsrechte verhältnismässig definiert, Datensicherheit gewahrt und die Kosten geringer gehalten werden. Die Referenten betonten, dass Informatikprojekte heute in den meisten Fällen ohne Datenschutzvorgaben entwickelt werden und deshalb auch schwer zu kontrollieren sind. Die Datenschutzbehörden verlangten eine stärkere Einflussnahme bei der Entwicklung von solchen Projekten, was aber grössere Informatikressourcen bei den Aufsichtsstellen voraussetzt.

12.2. Publikationen des EDSB – Neuerscheinungen

- Newsletter des EDSB 2/2001
- Newsletter des EDSB 1/2002

Die neue Website des EDSB

Wir haben per 1. Februar 2002 unser Angebot auf dem Internet grundsätzlich überarbeitet. Texte zu ausgewählten Themen sind jetzt an einer Stelle zusammengefasst und wer sich für eine bestimmte Frage interessiert, findet die Antwort leichter durch das Glossar. Zudem gibt es die Möglichkeit, sich in eine Mailingliste einzutragen, um regelmässig über Neuerscheinungen des EDSB informiert zu werden. (www.edsb.ch)

Weitere Informationen in folgenden Bereichen:

- Die Post und das Geldwäschereigeset - Warum die Post Identitätskarten kopieren darf (www.edsb.ch/d/themen/weitere/post-gwg.htm)
- Datenschutz in der Familienforschung (www.edsb.ch/d/themen/weitere/genealogie.htm)
- Beurteilung des leistungsorientierten Abgeltungsmodells für kassenpflichtige Medikamente (LOA) aus datenschutzrechtlicher Sicht (www.edsb.ch/d/themen/gesundheit/loa.htm)

12.3. Statistik über die Tätigkeit des Eidgenössischen Datenschutzbeauftragten vom 1. April 2001 bis 31. März 2002

Konferenzteilnahmen:

National	International
13	23

Anzahl von Sitzungen

	Bund	**Private**	**Kantone**
Intern	119	80	11
Extern	151	44	29
Total	**270**	**124**	**40**

Anzahl der Stellungnahmen

	Eingänge	Schriftliche Stellungnahmen	Empfehlungen des EDSB	Keine Einwendungen
Zu Gesetzen	55	51		8
Zu Verordnungen	63	60		5
Zu internationalen Vereinbarungen	34	32		4
Anfragen aus dem öffentlichen Bereich:				
Bundesorgane	283	187	1	5
Kantone	60	33		
Ausländische Datenschutzbehörden	28	26		
Anfragen aus dem privaten Bereich:				
Privatpersonen	202	172	1	9
Banken	27	26	1	
Adresshandel / Direktmarketing	64	35		
Kreditwesen	33	33		
Buchhandel / Publikationen	10	10		
EDV - Bereich	27	23		
Personalwesen	256	224		
Telekommunikation	39	39		
Versicherungen	55	47		
Polizeiwesen	106	106		
Gesundheit	132	106		
Mietrecht	8	7		
Kundenkarten	8	3		
Sekten	6	3		
Umwelt /Bauten	1	1		
Vereine	21	21		
Steuern	6	6		
Statistik / Forschung	2	2		
Total	**1526**	**1253**	**3**	**31**

Telefon Liste	Privat-personen	Bundes-organe	Kantone	Vereine / Verbände	EDV-Bereich	Anwalt- u. Treu-handbüros	Industrie / Gewerbe Dienstleistungen	Medien
Datenschutz allgemein	243	59	52	15	16	119	159	40
Auskunftsrecht	120	27	1	6		2		11
Anmeldung Datensammlungen	37	13				88	56	
Datenbekanntgabe	58	10	5	54	18	39	94	42
Übermittlungen ins Ausland	68	11		10	39	103	72	9
Kompatibilität mit E.U. Länder	85	8	2		14	56	40	12
Arbeitsbereich/ Arbeitsvermittlung	178	11	2		32	59	97	39
Gesundheit/ Versicherungen/	177	54	22	7	14	49	31	33
Mietrecht/ Mietformulare	18							
Marketing direkt Werbung	28			11		28	32	34
Banken/Kreditkarten Kreditauskünfte	65	1		8	2	32	10	9
Post	16	2		6	4	1		
Forschung	3	1		1		1		1
Statistik	29	29	6					38
Videoüberwachung Bildmaterial	52	3		1	9		2	37
Telefon-Daten	31	4		8		3	28	27
INTERNET	75	5	2	5	6	7	12	43
Datensicherheit Cryptografie	22	15	1		23	8	9	20
Polizeiwesen	36	39	5					21
Ausländer / Asyl.	9	18	1			2		
Total	**1352**	**317**	**101**	**132**	**177**	**597**	**642**	**416**

12.4 Das Sekretariat des EDSB

Eidgenössischer Datenschutzbeauftragter:	Thür Hanspeter, Fürsprecher
Stellvertreter:	Walter Jean-Philippe, Dr. iur.

Sekretariat:

Leiter:	Walter Jean-Philippe, Dr. iur.
Stellvertreter:	Buntschu Marc, lic. iur.
Informations- und Pressedienst:	Eggli Liliane, lic. phil. Tsiraktsopulos Kosmas, lic. iur.
Rechtsdienst:	8 Personen
Informatikdienst:	5 Personen
Kanzlei:	3 Personen

13. Anhang

13.1. Musterreglement für die Internet- und E-Mail- Überwachung am Arbeitsplatz

Musterreglement für die Internet- und E-Mail-Überwachung am Arbeitsplatz

In diesem Musterreglement ist der Text in normaler Schrift verfasst, die Erklärungen und Hinweise zu notwendigen Ergänzungen in kursiver Schrift.

Weitere Erläuterungen finden Sie in unserem «Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz», der im Sekretariat des EDSB bezogen werden kann.

1. Allgemeine Bemerkungen

1.1 Interessen der Firma

Durch Benutzung des vernetzten Computers am Arbeitsplatz können folgende Interessen und technische Einrichtungen unserer Firma beeinträchtigt werden:

- Speicherkapazität und Netzwerkbandbreite durch übermässige Internet- und E-Mail-Nutzung;
- Daten- und Anwendungssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) durch Einfuhr von Viren, Würmern, Trojanischen Pferden oder Installation von fremden Programmen;
- Arbeitszeit und andere finanzielle Interessen (Produktivitätsverluste, Kostensteigerung für zusätzliche Mittel und/oder Leistungen, Netzkosten usw.);
- weitere rechtlich geschützte Interessen, wie Ruf, Fabrikations- und Geschäftsgeheimnisse oder Datenschutz.

1.2 Interessen des Arbeitnehmers/der Arbeitnehmerin

Unsere Firma achtet und schützt im Arbeitsverhältnis die Persönlichkeit des Arbeitnehmers, nimmt auf dessen Gesundheit gebührend Rücksicht und sorgt für die Wahrung der Sittlichkeit.

Unsere Firma wird Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind und wird die Angestellten über die bestehenden oder beabsichtigten Datenbearbeitungen informieren.

Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen, werden nicht eingesetzt. Sind Überwachungs- oder Kontrollsysteme aus anderen Gründen erforderlich, werden sie so gestaltet und angeordnet, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer nicht beeinträchtigt werden.

2. Nutzungsregelung

2.1 Berechtigung zur Internet- und E-Mail-Nutzung am Arbeitsplatz

Folgende Kategorien von Angestellten erhalten einen Zugang zu Internet und/oder E-Mail:

- ...
- ...
- ...

Angabe der entsprechenden Kategorien von Angestellten und des Zugriffszwecks, Zugriff entsprechend den tatsächlichen beruflichen Bedürfnissen der einzelnen Angestellten-Kategorien.

2.2 Umfang der Internet- und E-Mail-Nutzung am Arbeitsplatz

Ob Angestellte das Recht haben, am Arbeitsplatz Internet und E-Mail für private Zwecke zu nutzen, hängt in erster Linie vom Willen des Arbeitgebers ab. Ähnlich wie in anderen Bereichen des Arbeitsverhältnisses hat er ein Weisungsrecht. Der Umfang der Internet- und E-Mail-Nutzung kann je nach Angestelltenkategorie unterschiedlich sein. Die private Benutzung der netzbasierten Anwendungen kann je nach Unternehmen entweder zugelassen, eingeschränkt oder ganz verboten werden. Kapitel 5 unseres Leitfadens gibt einige Anhaltspunkte, wie ein Unternehmen die Nutzung des Internet und E-Mail am Arbeitsplatz regeln kann.

In diesem Kapitel sind konkrete und unmissverständliche Regeln aufzustellen.

3. Überwachungsregelung

3.1 Vorrang technischer Schutzmassnahmen

Unsere Firma verpflichtet sich, in erster Linie technische Schutzmassnahmen gegen Missbrauch und technischen Schaden einzusetzen.

Sie passt die technischen Schutzmassnahmen regelmässig dem neuesten Stand der Technik an. Die Anpassung erfolgt auch nach jeder technischen Störung.

Sie verpflichtet sich, die Arbeitnehmer über die mit der Benutzung des vernetzten Computers verbundenen Gefahren zu informieren.

Nur wenn ein Missbrauch trotz technischen Schutzmassnahmen nicht verhindert werden kann, darf sie personenbezogene Auswertungen der Internet- und E-Mail-Spuren vornehmen (vgl. § 3.5.1 – 3.5.6).

3.2 Technische Schutzmassnahmen

Folgende technische Schutzmassnahmen werden in unserer Firma eingesetzt:

- ...
- ...
- ...

Technische Schutzmassnahmen können die Risiken im Zusammenhang mit der Internet- und E-Mail-Nutzung reduzieren. Die präventive Wirkung dieser Massnahmen soll den Einsatz repressiver Mittel wie die personenbezogene Überwachung weitgehend ersetzen. Zu den wichtigsten technischen Schutzmassnahmen gehören Backups (Datensicherungen), Antivirus- und Diskquotaprogramme, Firewalls mit Positivlisten der erlaubten resp. Negativlisten der unerlaubten Websites und Intrusion Detection Systems, Verschlüsselung, zeitgerechte Einschaltung des Bildschirmschoners mit Passwortschutz, genügende Komplexität und Unübermittelbarkeit der Passwörter, Regelung der Stellvertretung und Weiterleitung beim E-Mail-Verkehr. Zusätzlich sollen die Surf- und Mailprogramme nach dem letzten Stand der Technik installiert und in einer sicherheitsmässigen Form konfiguriert werden. Kapitel 3 unseres Leitfadens listet die wichtigsten technischen Schutzmassnahmen auf.

3.3 Protokollierung

Die Protokollierung definiert sich als fortlaufende Aufzeichnung der Randdaten «wer», «was», «wann» und findet in unserer Firma an folgende Stellen statt:

Hier muss das Unternehmen die für ihn in Frage kommenden Protokollierungsarten, deren Zweck und Aufbewahrungsdauer angeben. Kapitel 4 unseres Leitfadens informiert über die wichtigsten Protokollierungsarten. Je nach bestehender oder beabsichtigter Protokollierungsart und unter Berücksichtigung ihrer konkreten Eigenschaften sind folgende Präzisierungen in der Überwachungsregelung nötig:

- Auf der Ebene der Netzkopplungselemente werden Protokollierungen, bestehend aus der IP-Adresse («wer»), der Zeitangabe («wann») und der abgerufenen URL («was»), generiert. Obschon die URL ein Randdatum ist, kann der abgerufene Inhalt

in der Regel nachträglich wiederhergestellt werden.

- Beim Zugriff auf Intranet-Dienste besteht die Protokollierung aus dem Benutzernamen (USERID, «wer») und der IP-Adresse (wenn letztere dynamisch vergeben wurde). Die Zeitangabe («wann») wird ebenfalls protokolliert sowie der Gegenstand («was») wie Ein- und Ausloggen, Ausdrucken, Applikationsabruf usw.
- In den E-Mail-Servern (Schnittstelle Intra-/Internet) werden Absender- und Empfängeradresse, Zeitangabe und Betreffzeile der E-Mails protokolliert sowie der Zeitpunkt, wann ein E-Mail gelesen bzw. versandt wurde.
- Das eingesetzte Surfprogramm (Browser) gestattet während einer bestimmbaren Zeit *(bestimmte Zeit angeben)* die Protokollierung aller Internet-Zugriffe auf der Festplatte des Computers (Verlauf/History). Diese Surfprogramme erstellen auch temporäre Dateien der Inhalte (Cache) und permanente Spuren-Dateien (Cookies) über die besuchten Seiten.
- *usw. (vgl. Kapitel 4 des Leitfadens).*

3.4 Verzicht auf den Einsatz von Spionprogrammen

Unsere Firma verzichtet auf den Einsatz von Programmen, die die systematische und dauerhafte Erfassung sämtlicher Aktivitäten am vernetzten Computer erfassen.

3.5 Voraussetzungen der Überwachung

3.5.1 Anonymität der Protokollierungen und Schutz des Inhalts privater E-Mails

Sind Benutzername und Protokollierung nicht trennbar, z.B. in der Proxy-Firewall, empfiehlt es sich, erstere zu pseudonymisieren.

Die Protokollierungen der E-Mails betreffen die Adressierungselemente (darunter vor allem die Absender- und Empfängeradresse), weswegen diese Protokollierung notwendigerweise personenbezogen ist. Unsere Firma nimmt aber keine Einsicht in den Inhalt privater E-Mails. Um den privaten E-Mail-Verkehr vertraulich zu halten, empfiehlt unsere Firma, diesen über einen separaten, nach Möglichkeit verschlüsselten E-Mail-Dienst abwickeln. *Ob internetbasierte, verschlüsselte E-Mail-Dienste überhaupt benutzt werden dürfen, hängt von der Nutzungsregelung ab. Ist die private Internetnutzung verboten, so fällt diese Möglichkeit weg.*

Unsere Firma verpflichtet die Informatikdienste, die Vertraulichkeit der Protokol-lierungen und Korrespondenzlisten zu respektieren.

3.5.2 Auswertung der Protokollierungen

Als Missbrauch versteht unsere Firma eine Verletzung der Nutzungsregelung (§ 2.2).

Unsere Informatikdienste identifizieren den fehlbaren Mitarbeiter, wenn sein Benutzername (oder Pseudonym) in der Protokollierung steht, oder sie identifizieren den Arbeitsposten, von welchem der Missbrauch begangen worden ist, aufgrund der IP-Adresse in der Protokollierung. Im letzten Fall benötigt die Identifikation des fehlbaren Mitarbeiters eingehendere Untersuchungen, wenn der Arbeitsposten durch mehrere Mitarbeiter benutzt wird.

Es empfiehlt sich für das Unternehmen, eine einzige zuständige Person für die personenbezogenen Auswertungen zu ernennen.

Das Resultat der Auswertungen wird durch die Informatikdienste an den Vorgesetzten zur Sanktionierung des fehlbaren Mitarbeiters weitergeleitet.

Falls die E-Mails aufgrund der Adressierungselemente nicht deutlich als privat oder beruflich eingestuft werden können, muss dies mit dem betroffenen Arbeitnehmer geklärt werden.

Sowohl die Leitung als auch die Informatikdienste behandeln die bearbeiteten Personendaten vertraulich.

Wenn ein Missbrauch keine technische Störung zur Folge hat, entscheidet der Vorgesetzte zusammen mit den Informatikdiensten aufgrund der Schwere des Missbrauchs, ob die personenbezogene Auswertung der Protokollierungen sofort oder erst nach wiederholter Feststellung eines Missbrauchs erfolgen soll. Im letzteren Fall informiert der Vorgesetzte die Angestellten über den festgestellten Missbrauch und kündigt personenbezogene Auswertungen bei Wiederholung von Missbräuchen an.

3.6 Überwachungsarten

3.6.1 Die Kontrolle der Sicherheit und Funktionstüchtigkeit der technischen Mittel

Unsere Informatikdienste sind für die Gewährleistung der Sicherheit und Funktionstüchtigkeit der technischen Mittel zuständig. Die Gewährleistung der Sicherheit erfolgt durch Einsatz von technischen Schutzmassnahmen.

Bei technischen Störungen, die durch die technischen Schutzmassnahmen nicht verhindert werden konnten, können die Protokollierungen beigezogen werden, um deren Ursache zu klären.

Die Informatikdienste passen die technischen Schutzmassnahmen an und melden der Leitung, wenn die Nutzungsregelung angepasst werden muss.

Wenn die Ursache einer technischen Störung in einem unerlaubten Surfen oder E-Mailen besteht, gelten die Regeln unter § 3.5.2.

3.6.2 Die Kontrolle der Einhaltung der Nutzungsregelung

Falls ein Arbeitgeber dies wünscht, kann er Kontrollen über die Einhaltung der Nutzungs-regelung vorgenehmen. Die Überwachungsregelung lautet dann wie folgt:

Unsere Informatikdienste dürfen kontrollieren, ob das Verbot (oder die Einschränkung) der privaten Internet- und E-Mail-Nutzung eingehalten wird.

Die Kontrollen erfolgen nur stichprobenartig und anonym und decken nur eine beschränkte Benutzungsdauer ab.

Hier hat das Unternehmen anzugeben, wie viele Tage pro Monat es die Kontrollen durchführen wird. Zu bemerken ist, dass die Kontrolle der gesamten Zeitspanne seit der letzten Stichprobe einer ständigen Verhaltensüberwachung gleichkommt und deswegen nicht zulässig ist.

Ergeben die Kontrollen, dass ein Missbrauch begangen wurde, gelten die Regeln unter § 3.5.2.

3.6.3 Die Vorgehensweise bei Verdacht auf Straftat

Wenn unsere Firma den konkreten Verdacht schöpft, dass eine Straftat per Internet oder E-Mail begangen wurde, so kann sie die entsprechenden Beweise, bestehend aus den Protokollierungen und eventuellen Backups, durch die Informatikdienste sichern lassen.

Der Entscheid, ob Anzeige erstattet wird oder nicht, liegt beim Vorgesetzten, nicht bei den Informatikdiensten. *Es besteht keine Anzeigepflicht. Es ist jedoch empfehlenswert, zumindest im Zusammenhang mit Offizialdelikten, Anzeige zu erstatten, um die Gefahr der Mittäterschaft zu verhindern.*

Wenn der Missbrauch zugleich eine technische Störung zur Folge hat, kann unsere Firma bei Verdacht auf eine Straftat selber die Identität der betroffenen Person ausfindig machen und Anzeige gegen diese Person erstatten. Ansonsten erstattet der Arbeitgeber Anzeige gegen Unbekannt und die Auswertungen werden von der Strafjustiz vorgenommen. Die weitere Überwachung des Internetverhaltens ist in jedem Fall Sache der zuständigen Strafjustizbehörde.

Unsere Firma verpflichtet sich, das Resultat der Ermittlungen gegenüber Dritten, insbesondere gegenüber den anderen Angestellten, vertraulich behandeln.

Vorbehalten bleiben die arbeitsrechtlichen Sanktionen wegen Verletzung der Nut-zungsregelung (vgl. § 2.2).

3.6.4 Leistungsüberwachung

In bestimmten Unternehmen ist es denkbar, dass eine Leistungsüberwachung stattfindet. Sie kann wie folgt geregelt werden:

Mit Leistungsüberwachung wird die systematische, qualitative und/oder quantitative Produktionserfassung gemeint.

Unsere Firma führt die Leistungsüberwachung nur während einer beschränkten Dauer durch *(beabsichtigte Dauer angeben).*

Falls im Rahmen der Leistungsüberwachung ein Missbrauch der Nutzungsregelung festgestellt wird, gelten die Regeln unter § 3.5.2.

3.6.5 Geschäftskontrolle

Eingehende geschäftliche E-Mails, wie z. B. Anfragen von Kunden, dürfen aus Geschäftskontrollgründen von unserer Firma eingesehen werden. Deswegen ist sie berechtigt, in den E-Mail-Briefkasten abwesender Arbeitnehmer Einsicht zu nehmen.

Wenn kein Unterscheidungsvermerk zwischen privaten und beruflichen E-Mails besteht und die private Natur eines E-Mails aufgrund der Adressierungselemente nicht erkennbar oder nicht anzunehmen ist, darf unsere Firma – analog den traditionellen Postsendungen – davon ausgehen, dass das E-Mail beruflich ist. Bestehen berechtigte Zweifel an der beruflichen Natur eines E-Mails, so hat sie dies mit dem Arbeitnehmer abzuklären. Die Einsicht in den Inhalt des fraglichen E-Mails ist in diesem Fall nicht gestattet *(unabhängig davon, ob private E-Mails erlaubt sind oder nicht).*

Die gleichen Regeln gelten auch für den Fall, dass ein einziger, gemeinsamer E-Mail-Briefkasten für mehrere Arbeitnehmer besteht.

Falls im Rahmen der Geschäftskontrolle ein Missbrauch der Nutzungsregelung festgestellt wird, gelten die Regeln unter § 3.5.2.

4. Sanktionen bei Missbrauch

Wenn die Voraussetzungen und die Regeln der Überwachung eingehalten worden sind, kann die Firma im Falle eines erwiesenen Missbrauchs arbeitsrechtliche Sanktionen gegen den fehlbaren Arbeitnehmer aussprechen.

Hier hat das Unternehmen die Sanktionen aufzulisten, die es im Falle eines Missbrauchs zu treffen gedenkt. In Frage kommen z. B. Abmahnungen, Sperrungen des Internetzugriffs, Schadenersatzforderungen, Streichung von Sonderprämien, usw. [vgl. dazu Kapitel 11 unseres Leitfadens]. In extremen Fällen, wie bei wiederholtem Missbrauch mit technischer Störung trotz Abmahnung oder bei erwiesenen Straftaten kann der Arbeitgeber sogar die Entlassung aussprechen. Die fristlose Entlassung eines Arbeitnehmers kann nur ausgesprochen werden, wenn dem Arbeitgeber nach Treu und Glauben die Fortsetzung des Arbeitsverhältnisses nicht mehr zugemutet werden kann. Die Sanktionen müssen der Schwere des jeweiligen Missbrauches angepasst und in ihrem Umfang bereits in dieser Überwachungsregelung bestimmt sein.

Für das Aussprechen von Sanktionen ist der Vorgesetzte des fehlbaren Arbeitnehmers zuständig.

Die IP-Adresse und somit in der Regel auch die Identität des fehlbaren Arbeitnehmers kann bewusst vertuscht werden. Unsere Firma verpflichtet sich, arbeitsrechtliche Sanktionen nur bei 100%-iger Sicherheit über die Identität des fehlbaren Arbeitnehmers zu treffen *(Die Gefahr der Identitätsvertuschung kann durch Einsatz eines zeitgerechten Bildschirmschoners mit Passwortschutz stark vermindert werden).*

Vor einer Löschung missbräuchlich erworbenen Dateien werden die betroffenen Arbeitnehmer informiert und, sofern es technisch zumutbar ist, wird ihnen die Möglichkeit gegeben, die betreffenden Dateien, z.B. E-Mails, auf privaten Datenträgern zu speichern.

5. Ansprüche des Arbeitnehmers/der Arbeitnehmerin bei unzulässiger Überwachung durch die Firma

Bei Verletzung der Voraussetzungen und Regeln der Überwachung der Internet- und E-Mail-Aktivitäten, stehen dem betroffenen Arbeitnehmer die zivilrechtlichen Ansprüche wegen Persönlichkeitsverletzung zu (vgl. Art. 28 ff ZGB).

Der betroffene Arbeitnehmer kann im Falle einer missbräuchlichen Überwachung durch die Firma auch strafrechtliche Mittel ergreifen. Zu denken ist insbesondere an die Anzeige wegen Verletzung des Geheim- oder Privatbereiches durch Aufnahmegeräte (Art. 179^{quater} StGB) oder wegen unbefugten Beschaffens von Personendaten (Art. 179^{novies} StGB).

Zu den unzulässigen Überwachungen gehören auch die personenbezogene Aus-wertung der Protokollierungen ohne Feststellung eines Missbrauchs, die Einsicht in den Inhalt privater E-Mails sowie der Einsatz von Spionprogrammen.

6. Weitere Bestimmungen

Sowohl die Informatikdienste als auch die Vorgesetzten unserer Firma haben die Personendaten, die sie im Zusammenhang mit einer Überwachung bearbeiten, durch angemessene technische Massnahmen gegen unbefugte Zugriffe zu schützen.

Sie sorgen insbesondere für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Personendaten.

Der Arbeitnehmer darf von der Firma jederzeit Auskunft darüber verlangen, ob Daten über ihn bearbeitet werden.

Personendaten dürfen nicht ohne Einwilligung der betroffenen Personen oder einen anderen Rechtfertigungsgrund an unberechtigte Dritte bekannt gegeben werden. Die Arbeitskollegen der betroffenen Person gelten in Bezug auf den Datenschutz als Dritte.

Der Firma obliegt keine gesetzliche Aufbewahrungspflicht im Zusammenhang mit Protokollierungen. Zu Beweissicherungszwecken dürfen die Protokollierungen für eine beschränkte Zeit, in der Regel nicht länger als vier Wochen, aufbewahrt werden.

Die Aufbewahrungsdauer hängt vom Zweck der Protokollierung ab. Im Rahmen von Sanktionsverfahren oder Strafverfolgungen dürfen sie bis zum Ablauf der entsprechenden Rechtsmittelfristen aufbewahrt werden.

13.2. Merkblatt über «Austritts- und Operationsberichte»

DSB-CPD.CH

Die schweizerischen Datenschutzbeauftragten

Les Commissaires suisses à la protection des données

Merkblatt über
Austritts- und Operationsberichte

Worum geht es?

Für die Beurteilung ihrer Leistungspflicht verlangt der Grossteil der Versicherer von den Spitälern und Heimen im obligatorischen Bereich die Herausgabe der vollständigen Austritts- und Operationsberichte.

Der **Austrittsbericht** fasst den Fall eines Patienten/einer Patientin im Hinblick auf einen Spital- oder Heimaufenthalt zusammen. Grundsätzlich umfasst er alle Diagnosen. Die aktiven Diagnosen werden durch andere Aktenelemente, deren Ergebnisse erwähnt sind, gestützt. Der Austrittsbericht enthält Kommentare oder wenn nötig eine Diskussion sowie die Behandlung nach der Spitalentlassung. Zudem gibt der Austrittsbericht Empfehlungen für die nachfolgende medizinische Betreuung.

Der primäre Zweck eines Austrittsberichtes liegt damit in der Information des nachbehandelnden Arztes.

Der **Operationsbericht** besteht darin, den Ablauf der Operation zu beschreiben, indem er Angaben darüber macht, wie lange eine Person anästhesiert war, wie viel Blut sie durch Transfusion erhalten musste, welche technischen Handlungen der Chirurg oder andere Personen, die in den Ablauf eingebunden waren, vornehmen mussten.

Damit enthalten sowohl Austritts- als auch Operationsberichte besonders schützenswerte Personendaten über die Patienten/Betreuten im Sinne des Datenschutzes.

An die Bearbeitung besonders schützenswerter Personendaten werden von Gesetzes wegen erhöhte Anforderungen gestellt.

Zur Bearbeitung von Personendaten gehören auch die Weitergabe von Personendaten an Dritte sowie die Beschaffung dieser Daten durch Dritte, in concreto die Weitergabe von Austritts- und Operationsberichten an Versicherer beziehungsweise die Beschaffung dieser Berichte durch die Versicherer.

Die Weitergabe darf nur unter Einhaltung der allgemeinen datenschutzrechtlichen Bearbeitungsgrundsätze wie Rechtmässigkeit, Zweckgebundenheit, Verhältnismässigkeit und Richtigkeit erfolgen.

Zweck der Datenbeschaffung durch die Versicherer

Die Beschaffung von Versichertendaten durch die Versicherer dient dem Zweck, die Leistungspflicht abzuklären und insbesondere über deren Höhe und Dauer zu entscheiden.

Verhältnismässigkeit der Datenbeschaffung durch die Versicherer

Es dürfen durch die Versicherer nur die Versichertendaten beschafft werden, die zur Erfüllung ihrer gesetzlichen Aufgabe (Zweckbindung) unentbehrlich sind.

Verhältnismässigkeit der Weitergabe von Austritts- und Operationsberichten

Sowohl Austritts- als auch Operationsberichte beinhalten viele besonders schützenswerten Daten über die Versicherten. Die Angaben über den Versicherten sind entweder direkt erkennbar (z.B. die Diagnose) oder sie können indirekt aus anderen Angaben entnommen werden (z.B. kann aus der Länge der Anästhesie darauf geschlossen werden, ob eine Person raucht). Darüber hinaus können den Austritts- und Operationsberichten zum Beispiel Aussagen über Krankheiten oder psychische Zustände entnommen werden, die nicht der Grund für die Hospitalisation oder die Betreuung in einem Heim waren.

Die Versicherer dürfen diejenigen Daten, die zum Festlegen der Leistungspflicht unentbehrlich sind, beschaffen. Die Spitäler und Heime dürfen diese Daten den Versicherern weitergeben.

Für die Festlegung der Leistungspflicht genügt in der Regel eine detaillierte Rechnung. In begründeten Einzelfällen können weitere Angaben notwendig sein.

Empfohlenes Vorgehen für die Spitäler und Heime

Das führt zu folgendem stufenweisen Vorgehen:

1. Stufe: Die Spitäler und Heime stellen eine detaillierte und verständliche Rechnung.

2. Stufe: Benötigt der Versicherer im Einzelfall zusätzliche Angaben, kann er dem Leistungserbringer schriftliche, spezifische, auf den konkreten Fall bezogene Fragen stellen. Er hat die Notwendigkeit dieser Rückfrage zu begründen. Der versicherten Person ist zur Information eine Kopie zuzustellen.

3. Stufe: Sind diese Angaben ausnahmsweise nicht ausreichend, kann der Versicherer zuhanden seines beratenden Arztes einen Austritts- oder Operationsbericht einholen. Er hat die Notwendigkeit dieses Vorgehens schriftlich zu begründen. Der versicherten Person ist zur Information eine Kopie zuzustellen.

DSB+CPD.CH / Dezember 2001

13.3. Muster-Datenschutzklausel für Staatsverträge im Bereich der Sozialen Sicherheit

Artikel X

Soweit aufgrund dieses Abkommens Personendaten übermittelt werden, gelten für die Bearbeitung und Sicherung dieser Daten, unter Berücksichtigung des in der Vertragspartei national und international geltenden Datenschutzrechts, die nachfolgenden Bestimmungen:

a. Die übermittelten Daten dürfen nur für die Durchführung dieses Abkommens und der Rechtsvorschriften, auf die es sich bezieht, an die im Empfängerstaat zuständigen Stellen übermittelt werden. Der Empfängerstaat darf sie nur zu dem angegebenen Zweck bearbeiten und nutzen. Die Bearbeitung im Empfängerstaat für andere Zwecke ist im Rahmen des Rechts des Empfängerstaats zulässig, wenn dies Zwecken der sozialen Sicherheit einschliesslich damit zusammenhängender gerichtlicher Verfahren dient. Im übrigen darf die Weiterübermittlung an andere Stellen nur mit vorheriger Zustimmung der übermittelnden Stelle erfolgen.

b. Der Empfänger unterrichtet die übermittelnde Vertragspartei auf Ersuchen über die Verwendung der übermittelten Daten und über die dadurch erzielten Ergebnisse.

c. Die übermittelnde Stelle ist verpflichtet, auf die Richtigkeit der zu übermittelnden Daten sowie auf die Verhältnismässigkeit in Bezug auf den mit der Übermittlung verfolgten Zweck zu achten. Dabei sind die nach dem jeweiligen innerstaatlichen Recht geltenden Übermittlungsverbote zu beachten. Erweist sich, dass unrichtige oder Daten, die nicht übermittelt werden durften, übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. Er ist verpflichtet, die Berichtigung oder Vernichtung vorzunehmen.

d. Die übermittelnde Stelle ist verpflichtet, die betroffenen Personen über die Übermittlung ihrer Daten in angemessener Weise zu informieren.

e. Die übermittelten Personendaten sind nur solange aufzubewahren, wie es der Zweck, zu dem sie übermittelt worden sind, erfordert und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen der Betroffenen im Bereich der sozialen Sicherheit beeinträchtigt werden.

f. Die übermittelnde und die empfangende Stelle sind verpflichtet, die Übermittlung, den Empfang und die Weiterbearbeitung von Personendaten festzuhalten.

g. Die übermittelnde und die empfangende Stelle sind verpflichtet, Personendaten, die übermittelt werden, wirksam gegen unbefugten Zugang, unbefugte Veränderung und unbefugte Bekanntgabe zu schützen.

13.4. Die Post und das Geldwäschereigesetz

Warum die Post Identitätskarten kopieren darf

Seit einiger Zeit erreichen uns immer wieder Anfragen von Inhabern von Postcheckkonten, die sich teilweise nach Jahren zum ersten Mal bei der Post ausweisen müssen. Als so genannte Finanzintermediärin wird die Post vom Geldwäschereigesetz dazu verpflichtet, die Identität der Kontoinhaber und -inhaberinnen festzustellen und den Inhalt der Identitätspapiere aufzunehmen und aufzubewahren. Die Praxis der Post, die Papiere zu kopieren, steht in Übereinstimmung mit den Bestimmungen des Datenschutzes.

Seit einiger Zeit verlangt und kopiert die Post bei allen Neueröffnungen von Postcheckkonten einen Pass oder eine Identitätskarte. Desgleichen fordert sie alle Kontoinhaber und -inhaberinnen, die ihr Konto bereits vorher eröffnet haben, per Zirkular auf, ihre Papiere bei Gelegenheit vorzulegen. Auch diese Papiere werden von der Post kopiert. Diesbezüglich gelangten viele Anfragen von Personen an uns, wie dieses Vorgehen datenschutzrechtlich zu beurteilen sei.

Eine Bearbeitung von Personendaten ist datenschutzrechtlich unter anderem nicht widerrechtlich, wenn sie durch Gesetz gerechtfertigt ist (vgl. Art. 13 Abs. 1 Datenschutzgesetz; SR 235.1). Die Post verlangt die Ausweiskopie als Massnahme gegen die Geldwäscherei gestützt auf das Geldwäschereigesetz (GwG; SR 955.0). Auch die Schweizerische Post gilt als Finanzintermediärin im Sinne des GwG und hat dessen Vorschriften zu beachten. Gemäss Art. 3 Abs. 1 GwG muss der Finanzintermediär bei der Aufnahme von Geschäftsbeziehungen die Vertragspartei aufgrund eines beweiskräftigen Dokuments identifizieren. Der amtliche Identitätsausweis (wie Identitätskarte oder Pass bei natürlichen Personen oder ein Auszug aus dem Handelsregister oder ein gleichwertiges Dokument bei juristischen Personen) ist nicht nur zu prüfen, sondern es ist auch dessen wesentlicher Inhalt aufzunehmen und aufzubewahren. Dabei handelt es sich um eine Sorgfaltspflicht, von der sämtliche Vertragsparteien resp. Kontoinhaber betroffen sind und die dem öffentlichen Interesse dient. Die von der Post gewählte Lösung, den Ausweis zu kopieren, entspricht der Praxis im Bankenbereich. Das Kopieren des Ausweises ist zudem adäquat und verhältnismässig. Datenschutzrechtlich ist das Verhalten der Post nicht zu beanstanden.

Es ist noch darauf hinzuweisen, dass die Post die Ausweiskopien nur für den im GwG vorgesehenen Zweck, d.h. die Bekämpfung der Geldwäscherei, verwenden darf. Mit anderen Worten dürfte die Post diese Ausweiskopien beispielsweise nicht für Marketingzwecke an andere Personen verkaufen.

13.5. Akkreditierungsverfahren für die Datenschutzbehörden

Siehe Seite 127 im französischen Teil des Berichtes

13.6. Empfehlungen des EDSB

13.6.1. Empfehlung in Sachen Weitergabe von Personendaten aus Kontoeröffnungsanträgen

13. Juni 2001

EMPFEHLUNG

gemäss

Art. 29 Abs. 3 des Bundesgesetzes über den

Datenschutz vom 19. Juni 1992

in Sachen

Weitergabe von Personendaten aus Kontoeröffnungsanträgen der XX Bank AG

I. Der Eidg. Datenschutzbeauftragte stellt fest:

1. Die X-Bank AG bietet ihren Kundinnen und Kunden verschiedene Möglichkeiten zur Kapitalanlage an. Die entsprechenden Kontoeröffnungsanträge enthalten u.a. eine Rubrik, die sich zur Datenbearbeitung durch die Bank äussert.

2. Der Eidg. Datenschutzbeauftragte (EDSB) hat bei der X-Bank AG wiederholt wegen der Rubrik «Datenbearbeitung» interveniert. Dabei bemängelte er insbesondere, dass der Satz «Die Einwilligung zur Datenbearbeitung kann jederzeit widerrufen werden» von zahlreichen Personen missverstanden werde und dass die Umschreibung «zu der X-Group gehörende Gesellschaften» als mögliche Datenempfänger zu unbestimmt sei.

3. Erst nach mehreren Briefwechseln erklärte sich die X-Bank AG in einem Schreiben vom 25. Oktober 1999 bereit, den Forderungen des EDSB nachzukommen und die Rubrik Datenbearbeitung folgendermassen anzupassen:

   Der Kunde ermächtigt die Bank, Kundendaten zu bearbeiten und zum Zweck der vertieften Analyse der Kundenbedürfnisse und zur Verbesserung der Leistungserbringung an zur X-Group gehörende Gesellschaften zur Bearbeitung weiterzuleiten. Der Kunde ermächtigt die Bank, den Abschlussvermittler und dessen Arbeitge-

ber, beide ebenfalls dem Bankgeheimnis unterstellt, über die Kundendaten zu informieren. Der Kunde hat das Recht, bei der Bank über die Bearbeitung der ihn betreffenden Daten die gesetzlich vorgesehenen Auskünfte sowie eine Aufstellung der zur X-Group gehörende Gesellschaften zu verlangen.

4. Am 9. März 2001 intervenierte der EDSB erneut bei der X-Bank AG, weil diese noch immer Antragsformulare mit dem ursprünglichen Text zur Datenbearbeitung benützte, und bat darum, die von der Bank vorgeschlagene Textversion zur Datenbearbeitung doch endlich anzuwenden.

5. Mit Schreiben vom 30. März 2001 bestätigte die X-Bank AG, dass künftig keine Antragsformulare mit der ursprünglichen Textversion mehr versandt würden. Gleichzeitig teilte sie dem EDSB auch mit, dass ab Mai 2001 der Halbsatz, wonach jeder Kunde das Recht habe, *«... eine Aufstellung der zur X-Group gehörenden Gesellschaften zu verlangen»*, wieder gestrichen werde, weil *«.... im übrigen lediglich die im Geschäftsbericht der X-Group und nicht generell alle Gruppengesellschaften bekannt gegeben werden können»*.

6. Weil dem EDSB erneut Kontoeröffnungsanträge mit dem ursprünglichen Text zur Datenbearbeitung vorgelegt worden sind, wandte er sich am 3. Mai 2001 wiederum an die X-Bank AG und wies bei dieser Gelegenheit nochmals darauf hin, dass der Verzicht auf eine Aufstellung aller zur X-Group gehörenden Gesellschaften nicht mit dem datenschutzrechtlichen Transparenzprinzip vereinbar sei.

7. Die X-Bank AG führte dazu in ihrer Stellungnahme vom 21. Mai 2001 aus, dass der Halbsatz *«... bezüglich des Aspekts der Transparenz nichts beizutragen vermag. Da der Kunde überdies klar darauf hingewiesen wird, dass er die gesetzlich vorgesehenen Auskünfte jederzeit bei der Bank verlangen kann, ist der Bestimmung von Art. 8 des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) Genüge getan»*.

II. Der Eidg. Datenschutzbeauftragte zieht in Erwägung:

1. Das Bundesgesetz über den Datenschutz (DSG, SR 235.1) regelt unter anderem die Bearbeitung von Daten natürlicher und juristischer Personen durch private Personen (Art. 2 Abs. 1 DSG). Die Bekanntgabe von Daten im Zusammenhang mit Anlageanträgen stellt eine Bearbeitung von Personendaten im Sinne von Art. 3 Bst. e DSG dar. Die X-Bank AG ist eine private Person und fällt daher unter die Bestimmungen des DSG (Art. 2 Abs. 1 DSG).

2. Gemäss Art. 29 DSG klärt der EDSB im Privatbereich von sich aus oder auf Meldung Dritter den Sachverhalt näher ab, namentlich wenn die Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler, Art. 29 Abs. 1 Bst. a DSG). Die Eidgenössische Datenschutzkommis-

sion hat in ihrem Entscheid vom 21. November 1996 in S. Mietwesen (VPB 1996, 62.42B) festgestellt, «dass die Empfehlungsbefugnis des EDSB nach Art. 29 Abs. 1 Bst. a DSG weiter zu interpretieren und nicht bloss auf Fehler von Informationssystemen der EDV zu beschränken sei». Mit anderen Worten ist von einem «Systemfehler» im Sinne der genannten Bestimmung auch dann zu sprechen, «wenn die Bearbeitung von Daten inhaltlich rechtswidrig, d.h. die Bearbeitung als solche so angelegt ist, dass sie geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen». Eine Datenbeschaffung ohne Angaben über die geplanten möglichen, zukünftigen Datenempfänger ist geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen.

3. Ausgehend vom verfassungsmässig garantierten Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten (Art. 13 Abs. 2 Bundesverfassung) muss jede Person die Herrschaft über die sie betreffenden Informationen ausüben und eine Bearbeitung dieser Daten durch Dritte einschränken können (informationelles Selbstbestimmungsrecht; vgl. BUNTSCHU, in Maurer/Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Art. 1, N 14ff.).

4. Ohne genaue Kenntnis der Datenempfänger ist es der betroffenen Person nicht möglich, frei zu entscheiden, ob und wem die Personendaten zugetragen werden sollen. Durch die generelle Umschreibung, gemäss welcher die Personendaten an eine für die betroffene Person unbestimmte Anzahl von Gesellschaften der X-Group weiter gegeben werden können, wird das informationelle Selbstbestimmungsrecht tangiert.

5. Zudem verstösst diese Formulierung auch gegen den Grundsatz von Treu und Glauben und das Transparenzprinzip von Art. 4 Abs. 2 DSG. Demnach muss jede Form der Bearbeitung, also auch die Weitergabe von Personendaten nach Treu und Glauben erfolgen und für die betroffene Person erkennbar sein. Dass die X-AG nicht gewillt ist, alle in Frage kommenden Datenempfänger bekannt zu geben, zeigt sich auch daran, dass sie sich bei der Offenlegung lediglich auf die im Geschäftsbericht der X-Group aufgeführten Gesellschaften beschränkt, andere Datenempfänger jedoch offenbar bewusst nicht bekannt geben möchte (s.o. Ziffer I.5.).

6. Die X-Bank AG verkennt, dass das Transparenzprinzip als fundamentaler datenschutzrechtlicher Grundsatz nicht erst im Zeitpunkt einer allfällig verlangten Auskunftserteilung seine Wirkung zu entfalten hat, sondern bereits ab dem Moment der Aufnahme der Bearbeitung von Personendaten uneingeschränkt berücksichtigt werden muss.

III. Aufgrund dieser Erwägungen empfiehlt der Eidg. Datenschutzbeauftragte:

1. Die X-Bank AG übernimmt die unter Ziffer I.3. erwähnte Formulierung zur Datenbearbeitung für die Kontoeröffnungsanträge.

2. Die X-Bank AG teilt dem Eidg. Datenschutzbeauftragten innerhalb von 30 Tagen seit Erhalt dieser Empfehlung mit, ob sie die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung nicht befolgt oder abgelehnt, so kann der Eidg. Datenschutzbeauftragte die Angelegenheit der Eidg. Datenschutzkommission zum Entscheid vorlegen.

3. Diese Empfehlung wird der X-Bank AG mitgeteilt.

DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE

Der Beauftragte:

O. Guntern

13.6.2. Empfehlung in Sachen Anmeldeformulare für Mietwohnungen

Bern, 6. September 2001

EMPFEHLUNG

gemäss

Art. 29 Abs. 3 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992

in Sachen

Anmeldeformulare für Mietwohnungen der Société X, Genève

I. Der Eidg. Datenschutzbeauftragte stellt fest:

1. Im Zusammenhang mit der Anfrage einer Privatperson hat der Eidgenössische Datenschutzbeauftragte EDSB von der Immobiliengesellschaft Société X verlangt, ihm ein Anmeldeformular für Mietwohnungen zukommen zu lassen.

2. Eine Überprüfung ergab, dass das Anmeldeformular der X in mehreren Punkten gegen das Urteil der Eidgenössischen Datenschutzkommission vom 21. November 1996 (VPB 62.42B) in Sachen Mietwesen verstösst und dem im Anschluss an dieses Urteil neu verfassten EDSB-Merkblatt *über die Anmeldeformulare von Mietwohnungen* keine Rechnung trägt. Der EDSB informierte die X über die ungenügenden Punkte und verlangte eine Anpassung des Formulars im Sinne des Urteils und des Merkblatts.

3. Im April 2001 unterbreitete die X dem EDSB ein neu gestaltetes Anmeldeformular für Mietwohnungen, das unter anderem auch folgende Einwilligungserklärung enthielt:

   Il autorise la Société de Gérance à prendre tous renseignements utiles à son sujet en relation avec la présente demande de location.

   Der EDSB wies in seiner Antwort vom 1. Juni 2001 darauf hin, *que la X n'avait pas donné suite à ses suggestions relatives à la rédaction de son formulaire et que, par conséquent, la pratique de la X n'était toujours pas conforme à la décision de la Commission fédérale de la protection des données.* Zur Einwilligungserklärung führte der EDSB aus, *que le consentement à la collecte de données auprès de tiers devait intervenir de manière expresse*.

4. Mit einem Schreiben (undatiert, eingegangen beim EDSB am 4. Juli 2001) unterrichtete der Rechtsvertreter der X den EDSB, dass die X in den folgenden Bereichen bereit sei, die Gestaltung entsprechend dem besagten Urteil der EDSK zu ändern:

nationalité (suisse/étranger), état civil; salaire annuel (à indiquer par des tranches de CHF 10'000.— jusqu'à CHF 100'000.—).

In folgenden Punkten gab die X ihrer eigenen Auffassung den Vorzug:

voitures/moto (numéro de plaques d'immatriculation); poursuites; loyer mensuel actuellement payé; pièces jointes à la demande (livret de famille ou pièce d'identité pours les suisse, permis de séjour ou d'établissement pour les étrangers, attestation mensuelle de salaire récente, attestation de non poursuites délivrée par l'Office des poursuites).

Als Einwilligungserklärung unterbreitete die X den folgenden Vorschlag:

Le soussigné autorise expressément le bailleur, respectivement la X, d'obtenir de l'Office des poursuites, de son employeur et/ou bailleur actuels tout renseignement en rapport avec sa solvabilité, à savoir des informations sur son emploi, son salaire, ses poursuites et/ou actes de défaut de biens éventuels, le paiement de son loyer et, cas échéant, les raisons de la résiliation de son bail. Le sousigné autorise également le bailleur, respectivement la X, à obtenir lesdits renseignements par l'intermédiaire d'une agence de renseignements commerciaux.

II. Der Eidg. Datenschutzbeauftragte zieht in Erwägung:

129 1. Das Bundesgesetz über den Datenschutz (DSG, SR 235.1) regelt unter anderem die Bearbeitung von Daten natürlicher und juristischer Personen durch private Personen (art. 2 al. 1 LPD). Die Entgegennahme von ausgefüllten Anmeldeformularen für Mietwohnungen durch eine Immobiliengesellschaft stellt eine Erhebung und Bearbeitung von Personendaten im Sinne von art. 3 lit. e LPD dar. Die X ist eine private Person und fällt daher unter die Bestimmungen des LPD (art. 2 al. 1 LPD).

2. Gemäss art. 29 LPD klärt der EDSB im Privatbereich von sich aus oder auf Meldung Dritter den Sachverhalt näher ab, namentlich wenn die Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler, art. 29 al. 1 lit. a LPD). Die Eidgenössische Datenschutzkommission hat in ihrem Entscheid vom 21. November 1996 in S. Mietwesen (VPB 1996, 62.42B) festgestellt, «dass die Empfehlungsbefugnis des EDSB nach Art. 29 Abs. 1 Bst. a DSG weiter zu interpretieren und nicht bloss auf Fehler von Informationssystemen der EDV zu beschränken sei». Mit anderen Worten ist von einem «Systemfehler» im Sinne der genannten Bestimmung auch dann zu sprechen, «wenn die Bearbeitung von Daten inhaltlich rechtswidrig, d.h. die Bearbeitung als solche so angelegt ist, dass sie geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen». Eine Datenbearbeitung von allen Personen, die ein Anmeldeformular für Mietwohnungen ausfüllen und bei der Immobilienverwaltung einreichen, ist

geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen.

3. Art. 13 Abs. 1 DSG hält fest, dass eine Persönlichkeitsverletzung widerrechtlich ist, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

a) *Die X geht auch davon aus, «que pour toutes les données contenues dans le formulaire, qui est rempli par le locataire, ce dernier donne son consentement exprès à la récolte des données et que, partant, une telle récolte n'est en rien illicite».* Der von der X vorgebrachte Einwand, dass der Mietinteressent das Gesuch letztlich ja unterschreibe und damit die Daten freiwillig abgebe, verkennt die rechtliche Tragweite des Rechtfertigungsgrundes der **Einwilligung des Verletzten** von art. 13 al. 1 LPD. Eine wirksame Einwilligung des Betroffenen schliesst in aller Regel zwar die Widerrechtlichkeit der Eingriffshandlung aus (Mario M. Pedrazzini/Niklaus Oberholzer, Grundriss des Personenrechts, 3. A., Bern 1989, S. 125). Vorausgesetzt ist allerdings, dass sich die Einwilligung im konkreten Fall als Akt wirklicher Selbstbestimmung darstellt, dass sie freiwillig und in Kenntnis der sich daraus ergebenden Konsequenzen erfolgt (consentement libre et éclairé). Die betroffene Person muss einerseits die Fähigkeit besitzen, Bedeutung und Tragweite des Eingriffes zu beurteilen und darf andererseits in ihrer Entscheidungsfreiheit nicht durch ausserhalb der Sache liegende Einflüsse, insbesondere Willensmängel beeinträchtigt sein (Pedrazzini/Oberholzer, a.a.O., S. 125 f.; Steinauer, Le droit privé matériel, a.a.O., S. 101). Befindet sich der Mietinteressent in einer echten oder vermeintlichen Notlage (zum Beispiel weil sich nur sehr wenige für ihn finanziell erschwingliche Wohnungen auf dem Markt befinden oder weil er nicht dem mehrheitlich gewünschten Idealprofil des Mieters entspricht, etwa weil er nicht die «richtige» Nationalität hat oder arbeitslos ist) so dürfte die Datenbekanntgabe in der Regel keinen Akt der wirklichen Selbstbestimmung darstellen. Alsdann kann nicht davon ausgegangen werden, dass die Datenbearbeitung durch die Einwilligung der betroffenen Person gerechtfertigt ist. So kann auch nicht davon ausgegangen werden, dass der Mietinteressent in der Regel frei ist, nur gewisse Fragen zu beantworten. Vielmehr zieht die Nichtbeantwortung einzelner Fragen, die als Verletzung der Privatsphäre empfunden werden, in der Regel das Ausscheiden des Mietinteressenten als Kandidat für das betreffende Wohnobjekt nach sich.

b) Die **wirksame Einwilligung** stellt zudem nur einen Rechtfertigungsgrund dar, soweit sie die betreffende Persönlichkeitsverletzung abdeckt. Eine Datenbearbeitung, welche gegen den Grundsatz der Verhältnismässigkeit oder andere allgemeine Bearbeitungsgrundsätze verstösst, kann nur durch die Einwilligung der betroffenen Person gerechtfertigt sein, wenn diese ihre Einwilligung in Kenntnis des Verstosses gegen den Bearbeitungsgrundsatz erteilt hat. Soweit also der Vermieter

Daten erhebt, die für den Vertragsabschluss nicht unbedingt erforderlich sind, kann er nur davon ausgehen, dass der Mietinteressent mit dieser Datenbearbeitung einverstanden ist, wenn er explizit auf diesen Umstand hingewiesen hat.

c) Die von der X vorgeschlagene clause de consentement trägt diesen Ausführungen in keiner Weise Rechnung. Ausserdem wird durch die Art und Weise der Fragestellung beim Mietinteressenten der Eindruck erweckt, dass die Abgabe der Einwilligung notwendige Voraussetzung für die Wohnungsbewerbung sei und er/sie überhaupt keine andere Wahl habe, als sein Einverständnis abzugeben. Als stossend erweist sich dabei besonders die Tatsache, dass die X zwar Bereitschaft signalisiert, gewisse Rubriken auf dem Anmeldeformular entsprechend dem Urteil der EDSK anzupassen bzw. darauf zu verzichten (le salaire exact, le loyer actuel, les raisons de la résiliation de son bail), sie auf dem Umweg über diese Einwilligungserklärung, die Mietinteressenten dazu anhalten will, eben diese Informationen zu liefern. Dabei scheint die X gezielt die Tatsache auszunützen, dass es sich ein Wohnungsinteressent – will er seine Chancen auf die Wohnung wahren - nicht leisten kann, die Einwilligung zu verweigern.

4. Im Schreiben vom Juli 2001 vertritt die Meinung der X widergegeben, wonach qu'il est inexact de prétendre que ce formulaire [=Anmeldeformulare für Mietwohnungen] s'adresse à un nombre indéterminé de personnes. Weiter wird aufgeführt, dass ein unterzeichnetes Anmeldeformular «constitue selon son texte même une offre ferme de location d'un appartement donné et entre ainsi dans le cadre de la conclusion d'un contrat de bail déterminé». Die X sieht sich daher aufgrund dieser Argumentation berechtigt, sich bereits für die Anmeldeformulare auf den Rechtfertigungsgrund des **überwiegenden privaten Interesses** von Art. 13 Abs. 2 Bst. a DSG zu berufen. Der Wortlaut der besagten Bestimmung lässt indessen keinen Zweifel darüber offen, dass eine Berufung auf diesen Rechtfertigungsgrund nur dann möglich ist, wenn die Datenbearbeitung in unmittelbaren Zusammenhang mit dem Abschluss des Vertrages erfolgt. Dabei genügt es nicht, dass auf dem Anmeldeformular der Vermerk aufgeführt wird, wonach das Formular bereits une offre ferme de location d'appartement darstelle. Jede im Vorfeld eines möglichen Vertragsabschlusses vorgenommene Tätigkeit reicht nicht aus, um als unmittelbares Element für den späteren Abschluss bezeichnet werden zu können. Tatsache ist vielmehr, dass eine Immobiliengesellschaft ein Mietobjekt gerade deshalb auf dem freien Markt anbietet, um eine möglichst grosse Anzahl von Wohnungssuchenden erreichen zu können. Demzufolge muss davon ausgegangen werden, dass sich die Mietofferten der X in den überwiegenden Fällen an eine unbestimmte Anzahl von Mietinteressenten richten. Eine allgemeine Berufung auf den Rechtfertigungsgrund von art. 13 al. 2 lit. a LPD für eine Datenbearbeitung zu einem Zeitpunkt, zu

dem es noch zu keinen konkreten Verhandlungen zwischen den Vertragspartnern gekommen ist, ist nicht statthaft. Je zahlreicher die Personen sind, über die im Vorfeld eines Vertragsabschlusses Daten erhoben werden, desto mehr Zurückhaltung ist bei der Erhebung und Bearbeitung von Daten über diese Personen angebracht, da das Vorhandensein eines unmittelbaren Zusammenhangs mit dem Vertragsabschluss bei den Mietinteressenten nicht gegeben ist.

5. Zu den weiterhin noch offenen Rubriken auf dem Anmeldeformulare der X hält der EDSB Folgendes fest:

a) Wohnsituation

Zur aktuellen Wohnsituation stellt die X folgende Fragen:

- Namen und Adresse des gegenwärtigen Vermieters,
- Seit wann der Mieter in der gegenwärtigen Wohnung wohnt,
- Gegenwärtiger Mietzins inklusiv Nebenkosten.

Die X versucht, sich durch Fragen nach der bisherigen Wohnsituation einen Einblick in das Verhalten des zukünftigen Mieters zu verschaffen. Diese Fragen sind grundsätzlich unzulässig. Die X darf sich nur erkundigen, ob die Kündigung vom bisherigen Vermieter ausgegangen ist und wenn ja, aus welchem Grund die Wohnung gekündigt wurde. Beim bisherigen Vermieter, beziehungsweise beim Hausmeister darf sie nur Angaben über den Mietinteressenten einholen, wenn dieser ihn als Referenz angegeben hat. Aber auch dann darf die X keine Erkundigungen nach der Grösse der Wohnung und nach der Höhe des Mietzinses einziehen, sondern sich nur nach Schwierigkeiten hinsichtlich der Zahlung der Miete und des Verhaltens des Mieters erkundigen. Hinsichlich le loyer mensuel actuellement payé gilt festzuhalten, *que ce montant ne permet pas à la X de juger correctement sa situation financière et ne vous est pas nécessaire pour examiner la demande. Le seul critère décisif pour le bailleur réside dans le fait de s'assurer que le locataire puisse payer à l'avenir son loyer.* Dies ergibt sich in ausreichendem Masse aus der Lohnbekanntgabe des Interessenten.

b) Permis de séjour, pieces de légitimation

Es verstösst gegen den Grundsatz der Verhältnismässigkeit, wenn all jene, die ein Mietgesuchsformular ausfüllen und bei der X einreichen, bereits die Kategorie des Aufenthaltstitels angeben sowie eine Kopie eines Ausweispapiers (unabhängig welcher Art) einreichen müssen. Die Massnahme ist, sofern eine gesetzliche Bestimmung dies verlangt, frühestens dann angebracht, wenn die Immobiliengesellschaft sich für einen Mietinteressenten definitiv entschieden hat und nur noch der Mietvertrag unterzeichnet werden muss.

c) Voitures/motos

Das Verhältnismässigkeitsprinzip von art. 4 al. 2 LPD verlangt, dass nur jene Daten bearbeitet werden, die für die Erreichung des angestrebten Zwecks unabdingbar sind. Gemäss eigenen Aussagen de X ces informations (numéro de plaques d'immatriculation) sont demandées , «par souci de simplification». Diese Datenbearbeitung verstösst damit eindeutig gegen das Verhältnismässigkeitsprinzip und das LPD. Der EDSB ist zudem der Ansicht, dass jegliche Fragen wie Anzahl sowie allenfalls Autokennzeichen nur dann zu stellen sind, wenn die Mietpartei einen Garagen- oder Parkplatz mieten möchte.

d) Poursuites

Mit Blick auf das Verhältnismässigkeitsprinzip darf auf dem Mietgesuchsformular nur Auskunft über hängige Betreibungen der letzten zwei Jahre verlangt werden. Zeigt die Immobiliengesellschaft ein weitergehendes Interesse in dieser Sache, so kann sie wie jede Person, die ein Interesse glaubhaft macht, die Protokolle und Register der Betreibungs-und der Konkursämter einsehen und sich Auszüge daraus geben lassen (art. 8a al. 1 de la loi fédérale sur la poursuite pour dettes et la faillite; LP; RS 281.1).

e) Pièces jointes à la demande

133 Von den Mietinteressenten dürfen Schriftstücke nur einverlangt werden, wenn dies entsprechend dem Verhältnismässigkeitsprinzip ein notwendiges Mittel zur Zielerreichung darstellt oder ein Gesetz dies ausdrücklich vorsieht. Die X hatte bis anhin keine stichhaltigen Argumente vorbringen, warum beispielsweise le livret de famille ou une pièce d'identité pour les suisse oder andere Dokumente dem Anmeldeformular beizulegen sind. Ausserdem steht das Einverlangen d'une attestation mensuelle de salaire récente der angeblichen Bereitschaft der X entgegen, que le salaire soit indiqué sous forme d'échelle par tranche de CHF 10'000.—.

III. Aufgrund dieser Erwägungen empfiehlt der Eidg. Datenschutzbeauftragte:

1. Die Société X setzt umgehend Anmeldeformulare für Mietwohungen ein, die sich uneingeschränkt an das EDSB-Merkblatt über die Anmeldeformulare für Mietwohnungen halten und das Urteil der EDSK umsetzen. Dies bedeutet hinsichtlich der noch offenen Punkte insbesondere:

1.1 Zur aktuellen Wohnsituation darf einzig die Frage gestellt werden, ob die bisherige Wohnung durch den Vermieter gekündigt wurde und wenn ja, aus welchem Grund.

1.2 Auf permis de séjour und d'autres pièces de légitimation ist zum Zeitpunkt derGesucheinreichung zu verzichten und kann – sofern eine gesetzliche Bestimmung dies verlangt – frühestens einverlangt werden, wenn sich die X definitiv für einen Mieter entschieden hat.

1.3 Die Frage nach hängigen Betreibungen ist auf die letzten zwei Jahre zu beschränken.

1.4 Auf die von der Société X im Juli 2001 vorgeschlagene Einwilligungserklärung ist zu verzichten.

1.5 Für die Einholung von Informationen bei Dritten (z.B. Inkassobüros, gegenwärtiger Vermieter, Arbeitgeber etc.) muss die Société X dem Mietinteressenten vorgängig informieren und ihm die Gelegenheit geben, die Zustimmung dazu zu verweigern, indem auf dem Anmeldeformular die entsprechende Rubrik mit dem Vermerk fakultativ gekennzeichnet wird.

1.6 Zusätzliche Dokumente dürfen nur dann verlangt werden, wenn sie für den Abschluss eines Mietvertrages unabdingbar sind oder eine gesetzliche Verpflichtung besteht. In jedem Fall dürfen diese Dokumente aber erst zum Zeitpunkt des unmittelbaren Vertragsabschlusses vom definitiv ausgewählten Mieter einverlangt werden. Dokumente, die nicht in einem direkten Zusammenhang mit dem Abschluss des Mietvertrages stehen, dürfen nur dann einverlangt werden, wenn eine klare und eindeutige Zustimmung des Betroffenen vorliegt, indem die Beibringung der Dokumente auf dem Anmeldeformular klar als fakultativ bezeichnet werden.

2. Die Société X teilt dem Eidg. Datenschutzbeauftragten innerhalb von 30 Tagen seit Erhalt dieser Empfehlung mit, ob sie die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung nicht befolgt oder abgelehnt, so kann der Eidg. Datenschutzbeauftragte die Angelegenheit der Eidg. Datenschutzkommission zum Entscheid vorlegen.

3. Diese Empfehlung wird der Société X mitgeteilt.

DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE

Hanspeter Thür

13.6.3. Weiterzug der Empfehlung in Sachen Drogentests in der Lehre an die EDSK

Auszug aus der

Weiterziehung des EDSB

in der Sache

Empfehlung des Eidgenössischen Datenschutzbeauftragten (EDSB) vom 22. Februar 2001 betreffend

Drogentests in der Lehre

Begehren

Folgendem Begehren sei stattzugeben:

Es sei die Firma x aufzufordern, die Drogentests bei Lehrlingen und die damit zusammenhängenden Datenbearbeitungen einzustellen.

Der EDSB zieht in Erwägung

Der Bericht der Arbeitsgruppe «Drogentests in der Lehre» ist dort, wo die vorliegende Weiterziehung schweigt, integrierender Bestandteil der Argumentation. Dies gilt insb. für Themen wie die Zuverlässigkeit von Drogentests und die Drogenprävention.

1. Der Persönlichkeitsschutz

Gegenstand dieser Weiterziehung ist eine Empfehlung des EDSB zum Schutz der Persönlichkeit von Lehrlingen der Firma x. Der Eingriff in die Persönlichkeit entsteht durch die Abgabe und Analyse von Urin zur Feststellung von Drogenkonsum und durch die entsprechende detaillierte Bearbeitung von Daten aus dem Privat- und Gesundheitsbereich des Lehrlings.

Der Arbeitgeber hat im Arbeitsverhältnis die Persönlichkeit des Arbeitnehmers zu achten und zu schützen, auf dessen Gesundheit gebührend Rücksicht zu nehmen und für die Wahrung der Sittlichkeit zu sorgen (Art. 328 Abs. 1 des Schweiz. Obligationenrechts, OR, SR 220). In Art. 328 Abs. 1 ist eine Spezialnorm zu Art. 28ff ZGB über den Persönlichkeitsschutz bezogen auf den Arbeitnehmer und dessen Stellung im Arbeitsverhältnis zu sehen. Danach hat der Arbeitgeber im Rahmen des Arbeitsvertrages dem Arbeitnehmer Schutz und Fürsorge zu gewähren und alles zu unterlassen, was den berechtigten Interessen des Arbeitnehmers widerspricht. Es geht beim Persönlichkeitsschutz um die Achtung vor der Individualität des Arbeitnehmers in seelischer, geistiger und körperlicher Hinsicht durch Vorgesetzte, Mitarbeiter und Dritte am Arbeitsplatz. Zu

den geschützten Gütern gehören u.a. Stellung und Ansehen im Betrieb, die private Geheimsphäre, wozu auch ein positiver Aids-Test gehört (vgl. Jürg Brühwiler in «Kommentar zum Einzelarbeitsvertrag», Zentralverband schweiz. Arbeitgeber-Organisationen [Hrsg.], Bern, Stuttgart, Wien, 1996, S. 189ff, 191).

Gemäss Brunner, Bühler, Waeber in «Commentaire du contrat de travail» (Schweiz. Gewerkschaftsbund, Lausanne 1996, S. 96ff) *«les principes de protection de la personnalité revêtent une importance particulière dans les rapports de travail en raison des liens étroits qui caractérisent la relation de travail et de la dépendance du travailleur à l'égard de l'employeur. La protection de la personnalité s'exerce en ce sens que le travailleur a le droit à ne pas subir d'atteinte dans sa sphère personnelle. Si une telle atteinte se produit néanmoins, elle constitue une violation de l'obligation de l'employeur de respecter la personnalité du travailleur, au sens de l'article 328 CO. […] Il [l'employeur] a en effet non seulement l'obligation de s'abstenir directement de toute atteinte aux droits de la personnalité, mais il a également l'obligation d'entreprendre tout ce qui est nécessaire pour empêcher que le travailleur ne subisse une telle atteinte. Ces obligations régissent de manière impérative tous les comportements et tous les événements liés directement ou indirectement aux rapports de travail. […]. Les valeurs protégées par les droits de la personnalité sont entre autre la sphère privée qui englobe la vie intime, c'est-à-dire les faits et gestes que chacun veut garder pour soi-même ainsi que la vie privée, c'est-à-dire les événements que chacun choisit de partager avec un cercle plus ou moins étroit de personnes, qu'ils soient ou non en relation avec la vie professionnelle, l'honneur, la dignité, la considération sociale, etc. […] L'employeur doit également veiller à ce que les rapports hiérarchiques dans l'entreprise ne soient pas entachés d'attitudes discriminatoires. […] Les mesures prises à titre de contrôle doivent être objectivement justifiées et servir un intérêt légitime prépondérant de l'employeur qui ne peut être préservé par une mesure moins stricte. Ces conditions ne sont en tout cas remplies si l'employeur fait procéder p.ex. à des fouilles corporelles"*.

Zum Abhängigkeitsverhältnis des Arbeitnehmers gegenüber dem Arbeitgeber äussert sich Bernhard Frei in «Der Persönlichkeitsschutz des Arbeitnehmers nach OR Art. 328 Abs. 1 unter besonderer Berücksichtigung des Personaldatenschutzes», Zürich 1982, S. 30ff wie folgt: *«Die wirtschaftliche verbunden mit der persönlichen Abhängigkeit des Arbeitnehmers zieht die Persönlichkeit des arbeitenden Menschen in noch stärkerem Masse in Mitleidenschaft, […] als dies ohnehin, aufgrund des Arbeitstatbestandes, bereits schon der Fall ist. Die realen Gegebenheiten von wirtschaftlichem Druck, Subordination und Fremdbestimmtheit unterhöhlen zusehends die vorgängig entwickelten Ansätze eines Menschenbildes, das auch dem Arbeitnehmer Autonomie, Partizipation und persönliche Entfaltung zubilligt. Im Lichte des Persönlichkeitsschutzes des*

Arbeitnehmers, der Wahrung seiner Würde, erhalten Postulate wie Mitbestimmung auf betrieblicher wie unternehmerischer Ebene, Humanisierung der Arbeitsbedingungen und Kündigungsschutz besondere Aktualität».

Art. 328*b* OR präzisiert Art. 328 OR insofern, als er besagt, dass der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten darf, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Gemäss Brunner, Bühler, Waeber (a. a. O., S. 108ff) *«l'article 328b CO protège l'ensemble de la vie privée et professionnelle du travailleur. Il limite de manière précise le droit de l'employeur à ne réunir des renseignements personnels sur chaque travailleur que dans la mesure où ils sont indispensables à la conclusion et à l'exécution du contrat de travail. […] Le traitement de données par l'employeur est soumis entr'autre au principe de la proportionnalité, ce qui signifie que l'employeur ne doit collecter et traiter que les renseignements qui sont vraiment indispensables à la conclusion et à l'exécution du contrat de travail, en s'efforçant de préserver au maximum les droits de la personnalité du travailleur. […] Selon les termes mêmes de l'article 328b al. 1 CO, il est interdit à l'employeur de réunir et traiter des données qui n'ont aucun lien avec les aptitudes du travailleur concerné à remplir son emploi ou qui ne se justifient pas dans le cadre de la conclusion ou l'exécution du contrat de travail. Ainsi en est-il de tout ce qui a trait à la sphère privée et n'interfère pas sur la relation de travail (p. ex. séropositivité).* Nach M. Rehbinder, in «Berner Kommentar», IV/2, 2. Teilband, S. 420, *«steht dem Arbeitgeber grundsätzlich wie jedem anderen das Recht zu, sich über den Arbeitnehmer ein Bild zu machen und zu diesem Zwecke Angaben zur Person sowie Unterlagen über seine Fähigkeiten und Leistungen zu sammeln. Die Beschaffung und Weitergabe der Informationen ist jedoch nur dann frei, wenn das Interesse des Informationsempfängers das Interesse des Betroffenen an der Geheimhaltung überwiegt (BGE 97 II 97ff) und wenn die Mittel der Informationsbeschaffung nicht persönlichkeitsverletzend sind».*

Daten über die Gesundheit stellen besonders schützenswerte Personendaten (Art. 3 lit. c, Ziff. 2 Datenschutzgesetz, DSG, SR 235.1) dar, deren Bearbeitung eines speziellen Schutzes bedarf. Gesundheitsdaten definieren sich als *«Informationen, die direkt oder indirekt Rückschlüsse über den physischen und psychischen Gesundheitszustand einer Person zulassen, Daten also, die im weitesten Sinn einen medizinischen Befund darstellen. Es muss sich daher nicht um eine den Ansprüchen der Medizin gerecht werdende Diagnose handeln»* (U. Belser, in Maurer/Vogt [Hrsg.] «Kommentar zum Schweizerischen Datenschutzgesetz,, Art. 3, N 13). Der Begriff «Gesundheitsdaten» betrifft Daten, die einen offensichtlichen und engen Zusammenhang mit der Gesundheit aufweisen (**Empfehlung N° R (97) 5 des Europarates vom 13. Februar 1997)**. Die Tragweite des Begriffs wird von der Botschaft zum DSG vom 23. März 1988 (BBl

1988 II 413) insofern eingeengt, als darunter nur medizinische Befunde fallen sollen, welche sich für die Betroffenen negativ auswirken können. Das mit dem Bearbeiten solcher Informationen verbundene Gefährdungspotential für die Persönlichkeit ist sehr unterschiedlich (Kommentar zum DSG, a. a. O., Art. 3, N 9).

Kurzsichtigkeit und der positive Befund eines Urintests sind zwar beides medizinische Befunde und als solche besonders schützenswerte Personendaten gemäss DSG, sie sind aber offensichtlich nicht gleichermassen schützenswert. Der Kommentar führt weiter aus, dass *«die Persönlichkeitsbeeinträchtigung oft auch nicht von der Datenart, sondern vielmehr vom Bearbeitungskontext, vom Zweck, von der Verbreitung der Information und von vielen anderen Elementen abhängt. Aus diesem Grund ist bei der Beurteilung, ob eine Datenbearbeitung die Persönlichkeit der betroffenen Person verletzt, nicht allein darauf abzustellen, ob besonders schützenswerte Daten i. S. des Datenschutzgesetzes bearbeitet werden, sondern auch auf die tatsächliche Sensitivität der Daten [...]».*

Die Schwere des Eingriffs in die Persönlichkeit der Lehrlinge ist im vorliegenden Fall einleuchtend: Neben den regelmässigen Drogenscreenings mit entsprechenden Befunden bearbeitet die Firma x einen beeindruckenden und mit den Bedürfnissen des Lehrverhältnisses kaum zu rechtfertigenden Gesundheitsdatenkatalog. Die Auswertung solcher Informationen ergibt ein vollständiges und detailliertes Bild nicht nur in wesentlichen Gesundheitsaspekten, sondern auch in bestimmten privaten Verhaltensweisen der betroffenen Person (z.B. Besuchen von Schulturnen, Sportaktivität, Drogenkonsum, Alkoholkonsum, Vereinsmitgliedschaft). Die Tatsache, dass das Formular nicht von der Firma x konzipiert wurde, vermag dessen Unverhältnismässigkeit nicht zu heilen.

Demgegenüber werden seitens der Firma x u.a. Interessen wie Sicherheit, Gesundheitsschutz sowie Fürsorgepflicht geltend gemacht. Die Firma x pflegt zu unterstreichen, dass auch der EDSB gegen das Ziel, die Sicherheit und die Gesundheit am Arbeitsplatz zu gewährleisten, grundsätzlich nichts einzuwenden hat. Dies trifft zu. Die Meinungen gehen jedoch bei der Umsetzung dieses Zieles diametral auseinander. Der EDSB, wie auch die Mitglieder der Arbeitsgruppe «Drogentests in der Lehre», sind der Überzeugung, dass zur Erreichung des genannten Ziels nicht jedes Mittel gerechtfertigt ist. Im Gefahrenkontext der Firma x stellen Drogentests einen unzulässigen Eingriff in die Persönlichkeit der Lehrlinge dar. Dies werden wir im Folgenden darlegen.

2. Die Sicherheit

Vor Abklärung der Sicherheitsaspekte bei der Firma x und vor der Abwägung zwischen Sicherheits- und Persönlichkeitsschutzinteressen sollen die nachfolgenden Erläute-

rungen einen Überblick über die Entstehung der entsprechenden Argumentation verschaffen.

Bei der Beantwortung der Fragen des EDSB vom 22. Dezember 1999, insbesondere im Zusammenhang mit dem Zweck der Drogentests, hat die Firma x die Drogentests bzw. den Einsatz einer entsprechenden internen Fachgruppe mit *«akzentuierten Problemen wie Dealen im Lehrlingsheim, vorzeitige Lehrabbrüche infolge Drogenkonsums, Ermahnungen von Elternseite an die Firma zur Wahrnehmung ihrer Sorgfaltspflicht»* begründet.

Die Förderung der Sicherheit wird nur allgemein erwähnt und auf der Interessenskala dem Gesundheitsschutz und der Vermittlung einer soliden, drogenfreien und ganzheitlichen Ausbildung gleichgestellt. Die Empfehlung des EDSB vom 30. März 2000 hat die Bedeutung überwiegender Sicherheitsinteressen als Rechtfertigung für Drogentests betont. In der Reaktion auf die Empfehlung beschränkt sich die Firma x auf die Wiederholung ihrer Argumentation, begründet aber die Drogentests neu auch mit den Persönlichkeitsschutzinteressen der Lehrlinge und der Drogenprävention. Die Arbeitsgruppe «Drogentests in der Lehre» hat in der Folge den Bericht über Drogentests in der Lehre publiziert.

Aus dem Bericht ist zu entnehmen, dass «Drogen, je nach Art und/oder Menge des Konsums, die Sicherheit im Unternehmen in einem das tolerierbare Grenzrisiko übersteigenden Mass gefährden können. Die Toleranzgrenze hängt hauptsächlich von den geschützten Rechtsgütern ab. So sind Drogentests grundsätzlich dann zulässig, wenn die geschützten Sicherheitsgüter gegenüber dem Persönlichkeitsschutz der betroffenen Person überwiegen. Dies ist z.B. dann der Fall, wenn die Verletzung einer Sicherheitsnorm zur Gefährdung des Lebens des Arbeitnehmers oder von Dritten führen kann. Die Übertretung von Sicherheitsnormen z.B. im Bereich des Luft- und Zugsverkehrs kann zur Gefährdung des Lebens der Passagiere führen. Zu denken ist auch an Arbeiten auf dem Bau – wie Gerüstbau, Arbeiten auf Dächern oder bei Kranführern – und an den Umgang mit gefährlichen Stoffen. In solchen Fällen können Drogentests – sofern sie nur stichprobenartig und im Rahmen eines bestimmten, im Arbeitsvertrag umschriebenen Sicherheitsmassnahmenpakets vorgenommen werden – vom Arbeitgeber präventiv angeordnet werden. Flächendeckende Tests wären unverhältnismässig». Auch anlässlich des Hearings vom 11. Dezember 2000 hat die Firma x ihre Argumentation auf die bereits bekannten Elemente beschränkt, ohne auf die überwiegende Natur ihrer Sicherheitsinteressen einzugehen trotz mehrmaligem Hinweis vom EDSB. Die Empfehlung des EDSB vom 22. Februar 2001 kommt nochmals auf die Voraussetzung eines überwiegenden Sicherheitsinteresses zu sprechen und betont, dass die Firma x ein solches bis zu diesem Zeitpunkt nicht belegt hat. Die Empfehlung unter-

streicht den Umstand, dass andere Sicherheitsvorkehren (z.B. ISO-Normen für die Gewährleistung der Produktqualität, Vorschriften der Arbeitssicherheit, effiziente Überwachungsmassnahmen) die Sicherheit ohne Eingriff in die besonders schützenswerte Gesundheitssphäre des Lehrlings gewährleisten können (Verhältnismässigkeits- und Zweckmässigkeitsprinzip). Erst danach liefert die Firma x – nach zwei Empfehlungen, einem Bericht der Arbeitsgruppe und einem Hearing – eine Aufstellung der zu den verschiedenen Lehrkategorien gehörenden, sicherheitsrelevanten Tätigkeiten, welche die Vornahme von Drogentests bei drei Lehrkategorien (Biologie- und Chemielaboranten sowie Chemikanten) begründen soll. Aufgrund dieser neuen Dokumentation hat der EDSB beschlossen, am 14. August 2001 einen Augenschein bei der Firma x vorzunehmen. Auch anlässlich des Augenscheins hat die Firma x nochmals unterstrichen, dass die Sicherheit nur ein Teilaspekt der Begründung für die Drogentests sei. Auf die anderen Elemente der Begründung (Druck der Eltern, Fürsorgepflicht, Gesundheitsschutz, usw.) wird nicht eingegangen, da sie nicht Gegenstand der Besprechung sind. Die Firma x vertritt die Auffassung, dass die Störfallverordnung (StFV, SR 814.012) die gesetzliche Grundlage für die Drogentests darstellt. Sie ermöglicht ihrer Meinung nach das Treffen nicht nur technischer und räumlicher, sondern auch personeller Massnahmen. Die Firma x führt anlässlich des Augenscheins weiter aus, Drogentests würden als risikomindernde, das Sicherheitsbewusstsein fördernde Massnahmen eingesetzt und aus Gleichbehandlungs- und Solidaritätsgründen auch bei Lehrkategorien vorgenommen, welche überhaupt keine Sicherheitsrelevanz aufweisen.

Zu den einzelnen Elementen der Begründung:

a. Die Anwendbarkeit der Störfallverordnung

Es ist unbestritten, dass die Firma x der Störfallverordnung untersteht. Die Störfallverordnung bezweckt die Schaffung technischer und räumlicher Massnahmen zum Schutz von Umwelt und Bevölkerung (Art. 1 Abs. 1 StFV). Dies geht auch aus der gesetzlichen Grundlage der Verordnung hervor: Art. 10 des Bundesgesetzes über den Umweltschutz (SR 814.01) spricht von Massnahmen wie «Geeignete Wahl der Standorte, Einhaltung von Sicherheitsabstände, Treffen von technischen Sicherheitsvorkehren, Überwachung des Betriebs, Gewährleistung der Alarmorganisation».

Auch in Art. 26 des Bundesgesetzes über den Schutz der Gewässer (SR 814.20) ist von technischen und räumlichen Massnahmen die Rede («Standortwahl, Konstruktionsmaterial, technische Ausgestaltung und Revision der Anlagen»). Somit sind die in Art. 3 Abs. 1 der Störfallverordnung genannten Massnahmen konsequenterweise technischer und räumlicher Natur. Auch der Begriff «betriebliche Ursachen» (vgl. Art. 3 Abs. 2 StFV) betrifft nur Anlagen und nicht das Personal. Dies ergibt sich aus Art. 2 Abs. 1 StFV, wonach unter dem Begriff «Betrieb» Anlagen zu verstehen sind. Drogentests können

auch nicht als Verhaltensregeln zur Verhinderung, Begrenzung und Bewältigung von Störfällen oder als Ausbildung gemäss Anhang 2.1 lit. *l* und *m* und Anhang 2.2 lit. *d* der Störfallverordnung bezeichnet werden, da sie eben keine Regel oder Ausbildung, sondern eine ärztliche Massnahme darstellen. Somit stellt die Störfallverordnung die Grundlage für technische und räumliche, nicht aber für personelle Massnahmen wie Drogentests dar.

b. Das Gefährdungspotential für die Sicherheit

Aus der Aufstellung der sicherheitsrelevanten Tätigkeiten, aus dem Augenschein vor Ort sowie aus den Augenscheinunterlagen lassen sich für die Lehrkategorien Chemie- und Biologielaboranten sowie Chemikanten folgende Hauptkategorien von Gefahren festhalten: Verätzungs-, Explosions-, Vergiftungs-, Missbildungs-, Erkrankungs-, Verbrennungs- und Verletzungsgefahr.

Die Firma x hat in diesem Zusammenhang zugesichert, dass die technischen Installationen Sicherungen besitzen und somit eine Fehlertoleranz aufweisen und die Lehrlinge vom Ausbildner in der Ausführung ihrer Tätigkeiten ständig im Auge behalten werden. Erst im dritten Lehrjahr arbeiten die Lehrlinge mehr oder weniger selbständig. Ausserdem besteht eine ständige, gegenseitige visuelle Kontrolle unter Angestellten. Im Übrigen bestehen Messstellen an jeder Maschine, welche eine ständige Kontrolle der chemischen Vorgänge erlauben. Regelmässige Bewusstseinsförderung in Bezug auf die Sicherheit, Standortanweisungen und Vorsichtsschilder gehören auch zu den bestehenden Sicherheitsmassnahmen. Umweltschutzdienst, Feuerwehrdienst, computergesteuerte Qualitätssicherungsverfahren, ständige Analyse der Schmelzvorgänge, Bestreben nach Reduktion des Einsatzes von gefährlichen Lösungsmitteln, obligatorische Brillen zum Schutz der Augen, Durchführung der chemischen Experimente hinter Glasscheibe («Kapelle»), Produktionsbetrieb nur unter der Regie von diplomierten Chemikanten sowie allgemeine Qualitätssicherungsmassnahmen und spezifische Arbeitsvorschriften stellen weitere Sicherheitsmassnahmen im Bereich Chemielaborant dar. Im Chemikantenbereich ist eine Überwachung der Vorgänge und der Lehrlingen ein Muss. In bestimmten Firmen arbeiten Chemikanten immer zu zweit. Bei der Firma x arbeiten die Lehrlinge nie alleine, sondern immer in Gruppen zusammen mit einem Ausbildner. Auch die Kontrolle der chemischen Vorgänge erfolgt nicht alleine. Mischungen chemischer Substanzen in den Reaktoren erfolgen immer nach Besprechung mit dem Ausbildner. Nach acht Wochen Einführungskurs im Labor und acht Wochen Lehrbetrieb kommen die Lehrlinge in die Produktion. Dort werden sie von einem Meister betreut. Auch die Arbeit am Computer erfolgt mit dem Ausbildner. Die Chemikanten kontrollieren, ob alle nach der Produktionsvorschrift arbeiten. Auch Biologielaborant/innen müssen sich je nach Arbeit mit Sicherheitsmassnahmen wie

Handschuhen, Brille, Gesichtsschutz oder Gesichtsmaske schützen**.** Die besondere Partnerschaft zwischen Auszubildendem und Ausbildner wird auch in der Broschüre «Grünes Licht für eine Berufslehre bei der Firma x» unterstrichen.

Ohne solche technische und organisatorische Sicherheitsmassnahmen wäre es seitens einer Firma geradezu grobfahrlässig, Lehrlinge mit sicherheitsrelevanten Aufgaben (z.B. dem Mischen chemischer Substanzen mit entsprechender Explosionsgefahr) zu beauftragen. Gemäss Berner Kommentar (a. a. O., S. 425ff) *«hat er [der Arbeitgeber] den Arbeitnehmer auf Gefahren hinzuweisen, ihn zu instruieren und für geeignete Überwachung bezüglich der Einhaltung der Sicherheitsvorkehrungen zu sorgen (BGE 102 II 18ff). […]. So müssen beispielsweise bei Heizanlagen angesichts ihrer Explosionsgefahr immer genügend Sicherungen gegen gelegentliche Fehlbedienungen eingebaut sein, die das Schlimmste verhüten können […]. Die Anforderungen an Auswahl, Instruktion und Überwachung erhöhen sich, wenn es sich um besonders schutzbedürftige Arbeitnehmer handelt (BGE 95 II 141) wie Jugendliche, insbesondere Lehrlinge und unerfahrene Arbeitnehmer, z.B. Aushilfen oder Behinderte. Selbst wenn den Arbeitnehmer ein erhebliches Selbstverschulden an seiner Schädigung trifft, so ändert dies nichts am Mitverschulden des Arbeitgebers und dessen damit eintretender Haftung».*

Wie die «Commission canadienne des droits de la personne» 1999 in einem Bericht über die Drogentests festgehalten hat, *«les tests de dépistage de drogues préalables à l'emploi ou effectués au hasard peuvent être permis pour les postes où la sécurité revêt une importance fondamentale, à condition que l'employeur puisse démontrer qu'il n'y a pas d'autre moyen de s'assurer que les employés ne sont pas frappés d'incapaciter de travail […]»* dennoch weiter, dass *«en temps normal, les tests de dépistage de drogues ne sont pas justifiables dans le cas de postes non critiques pour la sécurité parce que ces tests ne mesurent pas le niveau d'altération des facultés découlant de l'usage de drogues, et, par conséquent, ils ne peuvent pas être utilisés pour évaluer la capacité d'une personne d'exécuter un travail».* Die Behörde hält weiter fest, dass *«l'employeur doit établir que la politique ou la pratique [de dépistage de drogues] a un lien rationnel avec le poste et qu'elle est proportionnelle, en ce sens qu'il n'existe pas d'autre solution de rechange moins discriminatoire».* Weiter fügt sie hinzu, dass *«les tests de dépistage pourraient ne pas être acceptables si la personne occupant le poste est régulièrement en contact avec des collègues ou un superviseur dans l'exercice de ses fonctions même si ce contact n'est pas continu".*

Die kanadische Ärztegesellschaft hält in einem 2001 publizierten Bericht fest, dass *«les tests de dépistage de drogues au hasard chez les employés ont un rôle limité, s'il en est, en milieu de travail. De tels tests devraient être restreints aux employés qui occupent des postes critiques pour la sécurité, et on ne devrait les effectuer qu'en*

l'absence de mesures efficaces du rendement et de l'observation efficace par les pairs ou les superviseurs".

Der Rechtsprechung der kanadischen Gerichtsbehörden ist zu entnehmen, dass *«Il [der Richter] reconnait que de tels tests ne doivent être ordonnés que lorsque l'employeur a des motifs raisonnables de croire qu'un employé a des facultés affaiblies" […] «Ces politiques [de dépistage systématique de drogue] ont été déclarées déraisonnables parce qu'aucune preuve n'a établi que les companies ont subi des préjudices suite à l'abus de drogue ou d'alcool, de leurs salaries".* In einem Urteil gegen die Firma ESSO Kanada hat das Gericht entschieden, *«qu'il existe d'autres moyens moins invasifs pour s'assurer de la capacité des salariés à remplir leurs fonctions sans danger».* In einem anderen Urteil gegen die Bank Toronto Dominion ist das Gericht zum Schluss gekommen, dass *«cette méthode – c'est-à-dire l'analyse d'urine obligatoire – a un caractère attentatoire. Cette politique générale représente une étape importante dans l'invasion de la vie privée de nombreux individus dans le domaine de l'emploi.*

Cette méthode ne pourrait être jugée raisonnable qu'en présence d'une preuve de fond indiquant l'existence d'une menace grave pour les autres employés de la Banque et pour le public, ses clients". Bestimmte Unternehmen machen die Zulässigkeit von Drogentests von den nationalen und lokalen Gesetzen abhängig. Die Arbeitsgruppe «Drogentests in der Lehre» ist in ihrem Bericht zu den gleichen Schlussfolgerungen gekommen.

Die Sicherheitsmassnahmen, die bei der Firma x bestehen, reduzieren das Risiko für die Sicherheit in einem zweifellos vertretbaren Rahmen. Das konkrete Gefährdungspotential für die Sicherheit scheint im Endeffekt durchaus tragbar zu sein. Erwähnenswert in diesem Zusammenhang ist auch die Aussage der Firma x, wonach «Versetzungen an nicht sicherheitsrelevante Arbeitsplätze vorzunehmen sind, wenn der auf Urintests positiv resultierende Lehrling die angebotenen Hilfemassnahmen [Suchttherapie] nicht akzeptiert». *E contrario*, wenn der Lehrling die Hilfsmassnahme akzeptiert, darf er weiter an seinem «sicherheitsrelevanten» Arbeitsplatz arbeiten.

Unter diesen Umständen vermögen Drogentests den Eingriff in die besonders schützenswerte Gesundheitssphäre der Lehrlinge nicht zu rechtfertigen. Drogentests stellen ausserdem eine unverhältnismässige Massnahme dar (Art. 328b OR und Art. 4 Abs. 2 DSG), da sie im konkreten Fall zur Gewährleistung der Sicherheit weder nötig noch geeignet sind.

Auffallend ist auch, dass Drogentests «nur» zweimal jährlich durchgeführt werden. Unter der Annahme, dass die Sicherheit gegenüber dem Persönlichkeitsschutz überwiegen würde, müssten effiziente Drogentests jedoch öfters als nur zweimal pro Jahr durchgeführt werden. Flächendeckende Tests wären jedoch unverhältnismässig.

Erwähnenswert in diesem Zusammenhang ist weiter, dass sich die Firma x in Deutschland –bei gleicher Sicherheitsgefährdung– deutlich und öffentlich von der Drogenpolitik von der Firma x in der Schweiz distanziert hat. Auch intern – insb. von Seiten der Arbeitnehmervertretung– herrscht keine Einstimmigkeit in Bezug auf die Sicherheitsproblematik. Drogentests werden auch nicht bei Chemie- oder Biologiestudenten vorgenommen, welche, abgesehen vielleicht von den Stoffmengen, den gleichen Sicherheitsgefahren ausgesetzt sind wie bei Chemikanten.

Befremdend sind die Drogentests bei der Firma x vor allem deswegen, weil sie nur bei Lehrlingen, aber nicht bei den übrigen, diplomierten Mitabeitern, vorgenommen werden. Wenn die Sicherheit eine so zentrale Rolle spielt, wie die Firma x glauben machen will, dann wäre es zumindest logisch, ja sogar notwendig, dass die Drogentests auf die ganze Belegschaft der Chemie- und Biologielaboranten sowie Chemikanten ausgeweitet würden. Sicherheitsprobleme stellen sich auch bei diplomierten Mitarbeitern, da sie vermehrt mit sicherheitsgefährdenden Tätigkeiten und Überwachungsfunktionen konfrontiert sind als Lehrlinge. Gemäss Berner Kommentar (a. a. O., S. 426) sind Überwachungspflichten des Arbeitgebers gegenüber berufserfahrenen und fachkundigen Arbeitnehmern nicht auszuschliessen.

Die mehrmals wiederholte Aussage der Firma x, wonach das Gefährdungspotential bei Lehrlingen höher ist als bei diplomierten Mitarbeitern, vermag diese Ungleichbehandlung (oder Diskriminierung?) nicht zu rechtfertigen, da ein Drogenkonsum bei diplomierten Mitarbeitern nicht *a priori* ausgeschlossen werden kann.

Immer unter der Annahme, dass die Sicherheit ein gegenüber dem Persönlichkeitsschutz überwiegendes Interesse darstellt, würde die dadurch entstehende, markante Sicherheitslücke nicht zu rechtfertigen sein. Die Firma x steht dieser Frage gegenüber in einem offensichtlichen Begründungsnotstand. Die Sicherheitsargumentation der Firma x ist auch deswegen unglaubwürdig, weil Alkoholkonsum – mindestens so gefährlich, jedoch gesellschaftlich und moralisch besser akzeptiert als Drogenkonsum – nicht getestet wird.

Auch «legale» Drogen wie Aufputsch- oder Beruhigungsmittel, Epilepsiemedikamente usw., können die Aufnahmefähigkeit bzw. die Konzentration der Arbeitnehmer erheblich beeinträchtigen. In diesem Zusammenhang ist zu unterstreichen, dass die Arbeitnehmer bereits aufgrund der Treuepflicht (Art. 321a OR) gehalten sind, in einem den Arbeitsanforderungen angemessenen Zustand zu erscheinen.

Zusammenfassend lässt sich sagen, dass die Sicherheitsmassnahmen der Firma x entweder ungenügend sind, oder aber – und dies ist unsere Überzeugung – die Sicherheitsproblematik die Drogentests nicht rechtfertigt. Die hohen Anforderungen, die an die Rechtfertigungsgründe für Drogentests gestellt werden, sind begründet: Die in die-

ser Weiterziehung dargelegte Schwere des Eingriffes in die Persönlichkeit stellt das durch die Interessen der Firma x zu übertreffende Mass dar. Dass dieses Mass ohnehin auch durch die – inexistente oder kaum existente – Sicherheitsrelevanz bei den übrigen Lehrkategorien (kaufmännische Angestellte, medizinische Praxisassistentinnen, Anlage- und Apparatebauer, Automatiker, Elektroniker, Informatiker, Konstrukteure, Lageristen und Polimechaniker) nicht übertroffen werden kann, bedarf keiner näheren Ausführung. Im Namen der Gruppendynamik, der Gleichbehandlung bzw. der Solidarität praktiziert jedoch die Firma x Drogentests auch bei diesen Lehrkategorien.

3. Die Einwilligung

Die Firma x vertritt die Auffassung, dass die Einwilligung des Verletzten (Art. 13 Abs. 1 DSG) ein gültiger, alternativer Rechtfertigungsgrund für die Vornahme von Drogentests sei. Die Arbeitsgruppe «Drogentests in der Lehre» ist hingegen der Meinung, dass dies im Arbeitsrecht nur dann zutrifft, wenn die Drogentests zugunsten des Lehrlings erfolgen. Zum gleichen Schluss kommen auch die kanadischen Gerichtsbehörden, wonach *«la renonciation à un droit fondamental doit comporter des avantages compensatoires pour les employés». […]. «Leur négation [des droits] dans la personne d'un individu, fût-il consentant, menace leur intégrité pour l'ensemble de la collectivité dans la mesure où c'est toute la collectivité qui a intérêt à ce qu'ils soient appliqués». «Il peut ne pas être permis de renoncer au bénéfice de dispositions législatives qui présentent un intérêt important pour la société»* (zu dieser Thematik vgl. auch unsere Empfehlung vom 30. März 2000, Erw. 7, wo wir sinngemäss auf das Bedürfnis einer gesetzlichen Grundlage für Drogentests hingewiesen haben).

Mit anderen Worten soll im Arbeitsverhältnis nicht jede Persönlichkeitsverletzung durch die Einwilligung der betroffenen Person gerechtfertigt werden können. Tatsächlich wird die Bedeutung der Einwilligung durch die arbeitsrechtliche Bestimmung von Art. 362 OR insofern eingeschränkt, als der Arbeitnehmer nur in für ihn «günstigen» Persönlichkeitsverletzungen einwilligen darf (vgl. Art. 328 und 328*b* OR). Gemäss Brunner, Bühler, Waeber (a. a. O., S. 330ff) «*le contrat de travail, à l'instar de tous les autres contrats, est soumis au principe de la liberté contractuelle. Le législateur reste toutefois libre d'indiquer dans quelle mesure il entend lui-même déroger à ce principe, en établissant des normes qui s'appliquent impérativement aux parties au contrat.*

Dans le droit du contrat de travail, le législateur a fixé depuis toujours des règles tendant à la protection des travailleurs, auxquelles les employeurs ne peuvent déroger en défaveur des travailleurs. La codification du droit du contrat de travail n'a donc pas pour but seulement de réglementer les aspects contractuels que les parties n'ont pas précisés elles-mêmes mais aussi de limiter la liberté contractuelle pour tenir compte de la relation de dépendance du travailleur à l'égard de l'employeur. […] L'utilisation

[dans le texte legal] des verbes à la forme injonctive manifeste la volonté du législateur que les parties respectent l'obligation [...]. Si une disposition revêt un caractère relativement impératif (art. 362 CO) cela signifie qu'il ne peut y être dérogé qu'en faveur du travailleur, que ce soit par accord entre les parties au contrat de travail ou par convention collective de travail. Il n'est pas aisé de déterminer dans tous les cas si une dérogation déploie des effets en faveur ou au détriment du travailleur. […] Si les parties se mettent d'accord oralement ou par écrit sur un point quelconque de leurs rapports de travail en dérogation à une règle impérative de la loi, leur accord n'a pas d'effet.

De telles dérogations sont illicites et, par conséquent, nulles: elles sont automatiquement remplacées par le contenu des normes légales correspondantes". Auch nach Brühwiler (a. a. O., S. 190) «können die sich aus Art. 328 OR ergebenden privatrechtlichen Schutzpflichten des Arbeitgebers nicht durch Vertrag eingeschränkt, sondern nur [...] zugunsten des Arbeitnehmers [...] erweitert werden».

Die Frage, die sich im Zusammenhang mit Drogentests stellt, ist demnach nicht, ob die Einwilligung die Drogentests rechtfertigt, sondern ob die Drogentests und die entsprechende Einwilligung zugunsten des Arbeitnehmers erfolgen.

Dies ist nach Meinung der Arbeitsgruppe nur ausnahmsweise der Fall. Wie wir bereits in dieser Weiterziehung dargelegt haben, stellen Drogentests im Gefahrenkontext der Firma x einen unzulässigen Eingriff in die Persönlichkeit der Lehrlinge dar. Nicht zugunsten des Lehrlings sind Drogentests auch deswegen, weil sie, wie wir hiernach darlegen werden, ohne freie Einwilligung erfolgen, ein Misstrauenszeichen sowie eine Benachteiligung der Lehrlinge darstellen und keine weitere Rechtfertigung besitzen.

Aus dem Bericht der Arbeitsgruppe über Drogentests in der Lehre entnehmen wir folgende Passagen: «Die Einwilligung zu einem Eingriff in die Persönlichkeit gehört zu den höchstpersönlichen Rechten einer Person. Die Einwilligung muss frei, spezifisch und ausdrücklich sein. [...] Unter freier Einwilligung versteht man, dass die betroffene Person nicht unter einem äusseren Druck steht. Der Lehrling befindet sich in einer hierarchisch schwächeren Position gegenüber dem Vertragspartner, welche dazu führt, dass er aus Angst vor Repressionen durch die Eltern bzw. eventuell vor Verlust der Lehrstelle aufgrund der Beschäftigungslage den Drogentest akzeptiert. Während des Lehrverhältnisses kann das Verweigern der Einwilligung überdies zu Diskussionen zwischen Arbeitgeber und Lehrling sowie zwischen Arbeitgeber und Eltern führen, um den Grund der Verweigerung herauszufinden (dabei wird oft übersehen, dass der Grund der Verweigerung häufig im Schutz der eigenen Persönlichkeit am Arbeitsplatz besteht). Unter diesen Umständen kann nicht von freier Einwilligung gesprochen werden. Von freier Einwilligung ist dann die Rede, wenn deren Verweigerung keine Folgen für den Lehrling hat. Die Verweigerung der Einwilligung darf nur dann Konsequenzen

für den Lehrling haben, wenn auch die Sicherheit in einem nicht vertretbaren Rahmen darunter leiden könnte».

Die Vornahme von Drogentests bei der Firma x wird im Lehrvertrag festgehalten und ist unabdingbare Voraussetzung für die Annahme der Kandidatur des Lehrlings. Die Verweigerung der entsprechenden Vertragsklausel bleibt nicht ohne Konsequenzen: Ohne Akzeptierung der Drogentests kommt der Lehrvertrag nicht zustande.

Unter diesen Umständen kann nicht einmal die Annahme der Vertragsvoraussetzungen als freiwillig bezeichnet werden, geschweige denn die Vornahme der Drogentests selber; wenn einmal die Vertragsbedingungen akzeptiert sind, sind die Drogentests Pflicht. Daran vermag auch die wiederholte Abgabe des Einwilligungsformulars vor jedem einzelnen Drogentest nichts zu ändern.

Unter diesen Umständen kann nicht von freier Einwilligung für die Vornahme von Drogentests gesprochen werden. Es geht vielmehr um ein Akzeptieren oder, besser gesagt, um ein Hinnehmen bzw. ein «Sich unabdingbarer Vorgaben unterwerfen». Daran vermag auch die Tatsache nichts zu ändern, dass die Lehrlinge und ihre Eltern über die Drogentests vorgängig informiert werden und nicht verpflichtet sind, bei der Firma x eine Lehre anzufangen. Die Firma x verwechselt offensichtlich den Begriff «freie Wahl des Arbeitsplatzes» mit «freier Einwilligung zu den Drogentests». Dies bekräftigt und anerkennt sie in ihrem Schreiben vom 31. Mai 2000.

4. Der Gesundheitsschutz

Die Firma x stützt die Drogentests auch auf das Argument des Gesundheitsschutzes. Dem erwidert die Arbeitsgruppe «Drogentests in der Lehre» mit dem Argument, dass gemäss Arbeitsgesetzgebung «Massnahmen des Gesundheitsschutzes arbeitsbedingt sind und Änderungen im Arbeitsumfeld bewirken». Der Berner Kommentar (a. a. O., S. 425ff) präzisiert, dass *«er* [der Arbeitgeber] *muss für eine einwandfreie Beschaffenheit der Arbeitsräume und anderer vom Arbeitnehmer zu benutzender Räume sorgen, geeignete Maschinen und Geräte zur Verfügung stellen und mit den erforderlichen Schutzvorrichtungen versehen lassen sowie den Arbeitsablauf möglichst gefahrlos gestalten (BGE 60 II 118)».* Brühwiler (a. a. O., S. 193) erläutert die Rücksichtnahme auf die Gesundheit des Arbeitnehmers dadurch, dass *«der Arbeitgeber den Arbeitnehmer nicht überfordern oder überanstrengen, ihn nicht mit Arbeit so belasten darf, dass seine Gesundheit geschädigt oder gefährdet werden könnte».* In jedem Fall werden Massnahmen des Gesundheitsschutzes nicht als Eingriffe in die Gesundheitssphäre verstanden. Drogentests stellen jedoch gemäss Bericht über Drogentests in der Lehre einen Eingriff in die Gesundheitssphäre dar.

«Drogentests sind nicht Massnahmen des Gesundheitsschutzes, weshalb sie nicht mit

der Pflicht des Arbeitgebers, die Gesundheit des Arbeitnehmers zu schützen, begründet werden können». Der Bericht schliesst nicht aus, dass der Arbeitgeber sich für das Wohlergehen seiner Angestellten einsetzt. Die getroffenen Lösungen und Massnahmen dürfen jedoch nicht die Grenzen der Legalität überschreiten. In diesem Zusammenhang fällt die Aussage der Firma x auf, wonach *«was bei der Beurteilung einer Drogenprävention zähle, die Resultate sind»*. Wir möchten an dieser Stelle korrigierend hinzufügen, dass das Ziel bekanntlich nicht jedes Mittel heiligt.

5. Die erweiterte Fürsorgepflicht

Ein weiteres Argument, das die Firma x immer wieder für die Begründung ihrer Drogentests benutzt, ist die erweiterte Fürsorgepflicht des Arbeitgebers gegenüber Lehrlingen. Auch diesbezüglich hat sich die Arbeitsgruppe in ihrem Bericht klar geäussert: «Die erweiterte Fürsorgepflicht muss den Persönlichkeitsschutz des Lehrlings berücksichtigen und die Drogenproblematik ganzheitlich betrachten. Dies setzt voraus, dass der Arbeitgeber seine Aufmerksamkeit nicht auf die Drogentests fokussiert, sondern konstruktive Hilfsmassnahmen anbietet und Drogenprävention betreibt.

Drogentests sind Fahndungs- und Personalbewirtschaftungsinstrumente, welche zur erweiterten Fürsorgepflicht des Arbeitgebers gegenüber Lehrlingen nicht passen». Die Firma x behauptet, Drogentests stellen nicht Fahndungs- und Personalbewirtschaftungsinstrumente, sondern wissenschaftlich empfohlene sekundärpräventive Massnahmen dar. Ausserdem behauptet sie einerseits, Drogentests würden dazu beitragen, bestmögliche Arbeitsbedingungen zu schaffen und einen wertvollen Beitrag zum Persönlichkeitsschutz leisten, weil dieser nicht nur mit Datenschutz gewährleistet werden könne, andererseits gibt sie im gleichen Schreiben zu, dass Drogentests «einen geringfügigen Eingriff in die Persönlichkeitssphäre darstellen». Der Widerspruch ist offensichtlich. Es entzieht sich unserem Verständnis, wie das Recht auf Leben, auf körperliche Integrität, auf Bewegungsfreiheit und sexuelle Freiheit, auf affektive Persönlichkeit, auf Namen, auf Bild und Stimme, auf Privatsphäre, auf Ehre, auf Entscheidungsfreiheit und Information, auf Vergessen usw. mit Drogentests gewährleistet werden kann. Der Arbeitgeber hat zum Schutz von Leben, Gesundheit und persönlicher Integrität der Arbeitnehmerinnen und Arbeitnehmer die Massnahmen zu treffen, die nach der Erfahrung notwendig, nach dem Stand der Technik anwendbar und den Verhältnissen des Betriebes oder Haushaltes angemessen sind, soweit es mit Rücksicht auf das einzelne Arbeitsverhältnis und die Natur der Arbeitsleistung ihm billigerweise zugemutet werden kann (Art. 328 OR). Dass Drogentests nicht zu solchen Massnahmen gehören, geht u. a. aus dem Bericht über Drogentests in der Lehre sowie aus § 1 dieser Weiterziehung hervor. Danach stellen Drogentests einen Eingriff in die Privatsphäre dar.

6. Die Drogenprävention

In ihren Stellungnahmen begründet die Firma x die Drogentests auch damit, dass Drogentests Bestandteil der Drogenprävention sind und dass der EDSB gegen Drogenprävention nichts einzuwenden hat. Es trifft zu, dass der EDSB nichts gegen die Drogenprävention einwendet. Das Problem ist, dass sowohl der EDSB als auch die anderen Mitglieder der Arbeitsgruppe «Drogentests in der Lehre» eine andere Definition von Drogenprävention haben als die Firma x. Was der EDSB und die Arbeitsgruppe unter Drogenprävention verstehen, geht aus dem Bericht über Drogentests in der Lehre sowie aus der Broschüre «Jugend, Drogen, Lehrbetrieb» der Schweizerischen Fachstelle für Alkohol- und andere Drogenprobleme hervor. Danach haben Drogentests in der Drogenprävention keinen Platz. Die Firma x integriert in ihrer Definition von Drogenprävention auch die Drogentests. Drogentests sollen ihrer Meinung nach eine Früherkennung einer sich anbahnenden Drogenproblematik ermöglichen sowie einen Druck erzeugen, keine Drogen zu nehmen.

7. Die Vertragsfreiheit

In ihrem Schreiben vom 2. April 2001 beruft sich die Firma x auf die Vertragsfreiheit, um ihre Drogentests vom Vorwurf der Illegalität zu befreien. Dabei scheint sie nicht wahrnehmen zu wollen, dass die Vertragsfreiheit nicht uneingeschränkt ist. Sie findet dort ihre Grenzen, wo andere Rechte tangiert werden können. Dass dies bei der Vornahme von Drogentests der Fall ist, haben wir in dieser Weiterziehung belegt.

8. Gesamtheitliches Drogenschutzkonzept

Die Firma x bezeichnet ihr Drogenschutzkonzept als gesamtheitlich, d. h. nicht nur auf Drogentests und Repression basierend, sondern auf aktive Hilfe und Schutz durch präventive Früherkennung von Suchtgefährdungen und durch Intensivbetreuung für suchtgefährdete Lehrlinge.

Dies geht aus mehreren Unterlagen der Firma x heraus. Misstrauisch gegenüber der Gefasstheit der Firma x gegenüber drogenkonsumierende Lehrlinge wird man bei der Lektüre der Lehrlingsheim-Unterlagen: Gemäss § 8 der Hausordnung des Lehrlingshauses und dem Mietvertrag hat der Konsum und das Aufbewahren von Drogen im Heim die sofortige Kündigung zur Folge. Wie dies mit dem Gedanken von Hilfe und Schutz vereinbart werden soll, ist nicht verständlich. Offensichtlich ist, dass bei drogenpositiven Befunden der betroffene Lehrling – zumindest in Bezug auf die Wohnung – kurzerhand auf die Strasse gestellt wird.

9. Weitere Argumente der Firma x

Erstklassige und ganzheitliche Berufsausbildung, Wahrnehmung der sozialen Verantwortung, Schutz vor gesundheitlicher und sittlicher Gefährdung, drogenfreie Lehrzeit, Schaffung bestmöglicher Arbeitsbedingungen, Reduktion der Lehrabbrüche und Umweltschutz sind nur einige der Lockworte, mit denen die Firma x ihre Drogentests anpreist. Nach unserem Dafürhalten liegen hinter den Drogentests in erster Linie das Dealen im Lehrlingsheim und die damit verbundenen Polizeieinsätze, der konsequenterweise entstehende Druck der Eltern und demzufolge das Bedürfnis der Firma am Schutz des eigenen Rufes. Nicht erwiesen, aber nicht gänzlich auszuschliessen ist auch eine Null-Toleranz-Politik gegenüber unkonventionellen Praktiken. Dass hinter den Drogentests eine bestimmte Haltung stecken könnte, geht auch aus der Broschüre «Probleme in der Lehre - was nun?» hervor. Dort werden u a. die Ausbildungsverantwortlichen aufgefordert, veränderte Verhaltensweisen wie hinsichtlich Kleidung, Körperpflege, Frisur, Freundes- und Bekanntenkreis usw., zu bemerken und auszuforschen.

Eigenartig ist auch die Ableitung der Drogentests aus Art. 345 OR sowie Art. 10 des Berufsbildungsgesetzes (SR 412.10), wie auch die pauschale Definition der Lehrzeit als «labile Phase der Entwicklung eines jungen Menschen».

11. Das Vertrauensverhältnis

Nicht zu vergessen ist, dass der Arbeitsvertrag auf gegenseitiges Vertrauen beruht. Letzteres kann u.a. dadurch tangiert werden, dass der Arbeitgeber ohne jeglichen konkreten Verdacht präventiv nach Drogenkonsum fahndet, indem er besonders schützenswerte Gesundheitsdaten über sämtliche Lehrlinge (auch diejenigen, die in der Tat keine Drogen konsumieren) systematisch vor und während der Lehre mit Fragebögen und Urintests bearbeitet.

Damit ist das eingangs gestellte Begehren begründet und es wird um Folgegebung ersucht.

EIDGENÖSSISCHER
DATENSCHUTZBEAUFTRAGTER

Hanspeter Thür

13.6.4. Empfehlung in Sachen CD-ROM Black Book

Bern, 28. November 2001

EMPFEHLUNG

gemäss

Artikel 29 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz

in Sachen

CD-ROM Black Book

I. Der Eidgenössische Datenschutzbeauftragte stellt fest:

1. Im Laufe des Jahres 2000 wurde die CD-ROM Black Book in der Schweiz auf den Markt gebracht. Sie wurde hergestellt und importiert durch das Unternehmen X (im Folgenden X genannt), eingetragen im Bundesstaat Nevada.

2. F.G. vertritt von der Schweiz aus das Unternehmen X in Europa (vgl. dazu den Briefkopf eines dem Eidgenössischen Datenschutzbeauftragten (EDSB) vorliegenden Begleitbriefes zu einer Lieferung sowie das Schreiben vom 26. Juni 2001 von F.G. an den EDSB). Gemäss einem Schreiben, das dem EDSB vorliegt und das von F.G. unterschrieben ist, liefert er die CD-ROM der Kundschaft in der Schweiz und bietet seine Unterstützung bei der Installation an. Er verwaltet beispielsweise die Passwörter und aktualisiert die Daten auf der CD-ROM. Er zeichnet mit dem Vermerk «X, Germansupport».

3. Die CD-ROM enthält Personendaten (Namen, Strasse, Wohnort, Beruf, Telefonnummer, E-Mail-Adressen, Internetadresse usw.) von 450'000 Personen in der Schweiz (450'000 E-Mail-Adressen von Geschäften, 150'000 Kontaktadressen und 160'000 Homepages; siehe Beschreibung der CD-ROM, Seite 1).

4. Anfang 2001 erschien ein Internetdokument mit dem Titel *Database Analysis Black Book 2000, Autor: Adrian Wiesmann, Datum: 25.04.2001, Copyright 2001 by Verein zur Gründung der «SwordLord-Foundation for new technology ethics».* Das Dokument analysiert die auf der CD-ROM enthaltene Datenbank und will Folgendes aufzeigen: die schlechte Qualität der darauf gespeicherten Daten, die Unrechtmässigkeit der Datenbeschaffung im Sinne des Datenschutzgesetzes (DSG, SR 235.1) und inwiefern diese Datenbank für unbestellte elektronische Massenwerbesendungen (sogenannte Spams) verwendet werden. Die CD-ROM enthält namentlich Software, die das Spamming ermöglicht («Bulk.Mail 2.0»).

5. Gleichzeitig machte Y das oben erwähnte Dokument auf seinem Internetsite «http://bbook.trash.net» zugänglich.

6. Mit Schreiben vom 3. Mai 2001 an Y kündete F.G. eine Zivilklage gegen Y an. Er forderte, dass die Verbreitung des oben erwähnten Dokuments gestoppt wird. Er werde dadurch in seiner Persönlichkeit verletzt, da seine eigene Internetsite («www.carfashop.com») und sein eigener Name darin erwähnt werden.

7. Am 17. Mai 2001 wurde am Zürcher Bezirksgericht mittels einer vorsorglichen Massnahme vereinbart, dass der Inhalt der Einstiegsseite des Sites «http://bbook.trash.net» gesperrt wird, bis ein Entscheid zur Sache gefällt ist. Während der Verhandlung bestätigte F.G., dass er die CD-ROM im Auftrag der X in der Schweiz vertreibt, dass die Personendaten ohne ausdrückliches Einverständnis der betroffenen Personen gesammelt worden sind und dass die CD-ROM Daten enthält, die zum Teil aus der Domain-Namen-Datenbank der Registrierungsstelle Switch beschafft worden sind. Er räumte ebenfalls ein, dass gewisse Daten vollkommen falsch sind. Weiter machte er geltend, dass jemand, der E-Mail-Adressen auf einem Website veröffentlicht, automatisch damit einverstanden sei, jede Art von elektronischer Post zu erhalten. Wie es auf der CD-ROM selbst vermerkt sei, diene diese im Übrigen der Verwaltung der Adressen von Newsletter-Kundinnen und Kunden und nicht dem Versenden von Spams.

8. Ebenfalls am 17. Mai 2001 beschlossen verschiedene Internetbenutzer-Organisationen (trash.net, SIUG, Swordlord, Linux User Group Switzerland sowie das Community-Projekt Symlink.ch) und einige Einzelpersonen, einen Fonds zu schaffen, der die Wahrung der Interessen von Internetbenutzerinnen und -benutzern im vorliegenden und in zukünftigen Fällen ermöglichen soll. In der Folge haben zwei von den oben erwähnten Kreisen beauftragte Anwaltskanzleien mit dem Eidgenössischen Datenschutzbeauftragten (EDSB) Kontakt aufgenommen und ihn um eine Stellungnahme gebeten.

9. Zur gleichen Zeit teilten mehrere Personen, die immer mehr unerwünschte Werbung erhielten, dem EDSB mit, sie hätten gegenüber F.G. ihren Anspruch auf Auskunft geltend gemacht. Sie wollten erfahren, über welche Personendaten er verfügt und ihm die Verwendung der Daten auf der CD-ROM verbieten. F.G. kam ihrer Forderung nicht nach. Immer mehr Werbung erhielt auch D.•R., der auf seinem Website «www.rosenthal.ch» ausdrücklich vermerkt, dass er keine Werbung wünscht.

10. Mit den Schreiben vom 29. Mai und 1. Juni 2001 eröffnete der EDSB gegen F.G. eine Untersuchung im Sinne von Artikel 29 des Bundesgesetzes über den Datenschutz (DSG; SR 235.1). Zu diesem Zweck forderte er ein Exemplar der CD-ROM an. Vorsorglich wurde F.G. ausserdem aufgefordert, seine CD-ROM nach Erhalt des zweiten Schreibens des EDSB und bis zur Klärung der Angelegenheit nicht mehr in Verkehr zu bringen.

11. In den Schreiben vom 26. Juni und 24. August 2001 nahm F.G. Stellung. Einige Beispiele auf Papier der CD-ROM wurden dem EDSB übergeben. F.G. erklärte, er habe die Forderung des EDSB, die Vermarktung der CD-ROM in der Schweiz einzustellen, der X weitergeleitet. Er selbst sei zu einer solchen Massnahme nicht befähigt. Seiner Ansicht nach hat die X die Massnahme durchgeführt.

12. Mit Schreiben vom 2. Oktober 2001 forderte der EDSB nochmals die Zustellung der CD-ROM.

13. Mit Schreiben vom 5. Oktober 2001 übermittelte F.G. dem EDSB ein Exemplar der besagten CD-ROM. Deren Überprüfung ergab Folgendes: Die verschiedenen Vorwahltabellen können miteinander verknüpft werden; wenn man z.B. einen Beruf eingibt, kann man die entsprechenden E-Mail-Adressen erhalten. – Viele E-Mail-Adressen sind nicht brauchbar. – Der Benutzer oder die Benutzerin hat ebenfalls Zugriff auf Postadressen. – Neben den Suchresultaten erscheint der Vermerk «opt-in», was vermuten lässt, dass alle Personendaten auf der CD-ROM mit ausdrücklicher Zustimmung der betroffenen Personen beschafft worden sind. Im Übrigen bestreitet F.G. in seinem Begleitbrief nicht, dass Daten auf der Basis der Domain-Namen-Datenbank der Switch beschafft worden sind.

14. Mit Schreiben vom 10. Oktober 2001 bestätigte Y dem EDSB, er habe auf sein Ersuchen nach Auskunft zu den über ihn in der Datensammlung vorhandenen Daten von F.G. keine Antwort erhalten.

II. Der Eidgenössische Datenschutzbeauftragte zieht in Erwägung:

1. Das Bundesgesetz über den Datenschutz (DSG, SR 235.1) regelt unter anderem die Bearbeitung von Daten natürlicher und juristischer Personen durch private Personen (Art. 2 Abs. 1 DSG). Zum einen stellt die Vermarktung der von der X hergestellten und in der Schweiz über F.G. vertriebenen CD-ROM eine **Bearbeitung** von Personendaten im Sinne von Artikel 3 Buchstabe e DSG dar. Zum andern ist F.G. eine **private Person**. Seine Tätigkeit fällt daher unter die Bestimmungen des DSG (Art. 2 Abs. 1 DSG).

2. Gemäss Artikel 29 DSG klärt der EDSB im Privatbereich von sich aus oder auf Meldung Dritter den Sachverhalt näher ab, namentlich wenn die Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler) [Art. 29 Abs. 1 Bst. a DSG]. Die Eidgenössische Datenschutzkommission hat in ihrem Entscheid vom 21. November 1996 in Sachen Mietwesen (VPB 1998, 62.42B) festgestellt, «dass die Empfehlungsbefugnis des EDSB nach Artikel 29 Absatz 1 Buchstabe a DSG weiter zu interpretieren und nicht bloss auf Fehler von Informationssystemen der EDV zu beschränken sei». Mit anderen Wor-

ten ist von einem «Systemfehler» im Sinne der genannten Bestimmung auch dann zu sprechen, «wenn die Bearbeitung von Daten inhaltlich rechtswidrig, d.h. die Bearbeitung als solche so angelegt ist, dass sie geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen». Die fragliche CD-ROM enthält Personendaten von rund 500'000 Personen in der Schweiz. Es handelt sich dabei um eine Bearbeitung von Personendaten, die **geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen**. Deshalb kann der EDSB dazu eine Empfehlung im Sinne von Artikel 29 Absatz 2 DSG abgeben.

3. Mit Schreiben vom 26. Juni 2001 bestreitet F.G., dass die fragliche Datenbearbeitung unter das DSG fällt. Er begründet seine Haltung damit, dass er nur an folgenden Tätigkeiten beteiligt war:

- an der Programmierung der Indexierungssuchmaschine X mit dem Ziel, die Sites von Schweizer und europäischen Unternehmen durch Auflistung zu indexieren und zu klassifizieren;
- im Rahmen eines Freelance-Vertrags an der Speicherung, Erstellung und Programmierung der deutschen Version des Sites «www.carfashop.com» der X;
- an der Lieferung der CD-ROMs, die Schweizer Kundinnen und Kunden bei der X bestellt hatten und an der dazu gehörigen technischen Wartung.

4. Er weist eine Beteiligung an der Beschaffung der Personendaten, am Datenexport, am Betrieb der Suchmaschine sowie an der Werbung für dieses Produkt auf seinem Internetsite zurück. Diese Tätigkeiten seien ausschliesslich durch die X ausgeführt worden. F.G. schliesst daraus, dass er nicht als Inhaber oder als Besitzer der Datensammlung bezeichnet werden könne. Die Verantwortung für alle Massnahmen – auch den Stopp des Vertriebs der CD-ROM – liege ausschliesslich bei der X, der er im Übrigen alle Schreiben des EDSB weitergeleitet habe.

5. Die Frage, ob F.G. an der Beschaffung der betroffenen Daten beteiligt war, ob er «Inhaber der Datensammlung» im Sinne von Artikel 8 DSG ist oder ob er als «Besitzer der Datensammlung» – ein Begriff, der übrigens im DSG nicht verwendet wird – bezeichnet werden soll, kann offen bleiben. Mit dem Import einer CD-ROM, die Personendaten enthält und mit der Aufbewahrung dieser CD-ROM im Hinblick auf ihre Vermarktung, bearbeitet F.G. Personendaten einer beträchtlichen Anzahl von Personen in der Schweiz. In Artikel 12 Absatz 1 DSG steht klar: «Wer Personendaten bearbeitet, darf dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen». Namentlich auf Grund dieser Bestimmung ist F.G. dem DSG unterstellt.

6. F.G. legt ebenfalls dar, die CD-ROM enthalte Adressen von Internet-Homepages zu

spezifischen Berufssparten sowie Beschreibungen der jeweiligen beruflichen Tätigkeiten, so wie sie im Internet stehen. Zudem finden sich dort die E-Mail-Adressen, die auf den betreffenden Homepages veröffentlicht sind, Namen und Adressen der Betreiber sowie gegebenenfalls die Telefon- und Faxnummern. Nach F.G. ist mit der CD-ROM kein Zugang zu den Daten allein vom Namen und vom Vornamen einer Person aus möglich. Die CD-ROM enthalte also keine Personendaten, da diese sich weder auf bestimmte noch auf bestimmbare Personen beziehen.

7. Die CD-ROM enthält ganz klar **Personendaten** im Sinne von Artikel 3 Buchstabe a DSG, da darauf Name, Adresse, Wohnort, Beruf, Telefonnummer und E-Mail-Adresse vermerkt sind. Diese beziehen sich auf klar bestimmte oder zumindest bestimmbare natürliche oder juristische Personen. Es können zudem Persönlichkeitsprofile erstellt werden, da die Daten mit Hilfe der ebenfalls vorhandenen Tabellen miteinander verknüpft werden können.

8. Mit Schreiben vom 26. Juni 2001 gibt F.G. zu, mit der CD-ROM sei der Zugriff auf Daten wie Name, Vorname, Strasse, Postleitzahl, Ort, Beruf möglich, dies aber nur für Daten, die sowieso auf dem Internet veröffentlicht sind. Er erklärt, dass die Daten auf der CD-ROM mit Hilfe von Suchmaschinen beschafft worden seien, und zwar mit «www.sear.ch», «www.infoseek.com» unter Berücksichtigung der Robot Matatgs «Robot-exclusion – Norm des W3C-Consortiums»; letzterer schliesst Daten von Personen aus, die nicht wollen, dass die Daten, die sie betreffen, von den Suchmaschinen angezeigt werden. Dieser in der Internetgemeinschaft allgemein bekannte Roboter entspreche den international anerkannten Standards (namentlich in Bezug auf das Erkennen der Sprache und der Metatags). Bezüglich D.R. führt F.G. aus, dieser habe zwar auf seinen Internetsites «www.insider.ch» und «www.ipd.ch» vermerkt, dass er keine Verwendung seiner E-Mail-Adresse zu Werbezwecken wolle. Er habe aber keine Metatags verwendet, die den Suchmaschinen eine solche Benutzungsbeschränkung anzeigt. Ausserdem stellt F.G. fest, die E-Mail-Adresse von D.R. tauche auf einem anderen Site «www.bigfoot.com» auf. Damit sei die Adresse öffentlich zugänglich, namentlich über das Suchwort «E-Mail». Im Übrigen seien viele Post- und E-Mail-Adressen sowie Telefonnummern auf dem Internet über spezielle Suchmaschinen für Adressen zugänglich. Das Projekt Blackbook unterscheide sich von diesen lediglich dadurch, dass die Daten auf einer CD-ROM vereint seien. F.G. präzisiert, die Daten stammten in keinem Fall von einem E-Mail-Server eines Unternehmens, von der Benutzerliste eines Internetanbieters (wie Bluewindow) oder von der Liste der Teilnehmerinnen und Teilnehmer einer Newsgroup. Die gesammelten Daten seien für Unternehmen bestimmt, die ihre Kontakte ausdehnen wollen. Die Verantwortlichen seien sich bewusst, dass die Daten gebraucht, nachverfolgt und indexiert werden.

Wer «Robot-exclusion – Norm des W3C-Consortiums» nicht verwendet, will bewusst die Verwendung seiner Daten nicht einschränken. F.G. unterstreicht weiter, dass es auf dem Markt bereits eine Reihe von Produkten gebe, die Name, Vorname, Adresse, Telefonnummer und E-Mail-Adresse auflisten, namentlich elektronische Verzeichnisse wie das elektronische Telefonbuch, TwixTel oder Outlook-Express. Verzeichnisse dieser Art seien zudem sehr leicht zu erstellen. Mit anderen Worten glaubt F.G., es handle sich beim vorliegenden Fall nicht um eine Verletzung der Persönlichkeit, da die betroffenen Personen **die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt** haben (Art. 12 Abs. 3 DSG).

9. Es ist unbestritten, dass die Daten aus dem Internet beschafft worden sind, einem Medium, das allen zugänglich ist, die wie F.G. über einen Netzzugang verfügen. Dies bedeutet aber noch nicht, dass über diese Daten uneingeschränkt verfügt werden kann. Die Anhörung vor dem Bezirksgericht Zürich vom 17. Mai 2001 hat ergeben, dass die Daten auf der CD-ROM mit Hilfe der Switch Domain-Namen-Datenbank beschafft worden sind. Dies geht auch aus den Briefen von F.G. hervor. Auf dem Site von Switch verbietet jedoch ein Hinweis ausdrücklich, die Datenbank für den Adressenhandel, für Werbung oder für elektronische Massenversände zu verwenden. Indem er sich an der an der Vermarktung der betroffenen Daten beteiligt hat, hat F.G. die formelle Ablehnung der Sitebetreiber gegenüber solchen Verwendungszwecken nicht respektiert. Das Beschaffen der auf der CD-ROM enthaltenen Daten ist deshalb rechtswidrig und deren Bearbeitung erfüllt den Grundsatz der Zweckbindungsprinzip nicht (Art. 4 Abs.1 und 3 DSG).

10. Zudem werden auf der CD-ROM D.R. Personendaten veröffentlicht, ohne darauf hinzuweisen, dass letzterer eine Verwendung der Daten zu Werbezwecken ablehnt. Die Angabe auf der Etikette der CD-ROM, das Programm nicht für das Spamming oder ähnliche Zwecke zu verwenden, reicht nicht aus. Der Vermerk muss bei jeder Person erscheinen, die die Verwendung der Daten zu Werbezwecken ausdrücklich ablehnt. Es kommt auch nicht darauf an, dass das System «Robot-exclusion – Norm des W3C-Consortiums» von D.R. nicht verwendet wurde: Dies ist nach schweizerischem Recht nicht zwingend. Im Übrigen ist ein solcher Roboter nicht hundertprozentig wirksam, auch wenn er programmiert worden ist. Ein automatischer Filter funktioniert momentan noch nicht immer; man muss einen manuellen Filter einbauen, um sicherzustellen, dass alle Daten rechtmässig beschafft werden. Weiter ist es unwichtig, ob die Daten auch auf einem anderen Site («infoseek.org») veröffentlicht sind oder nicht. Es liegt an der Person, die Personendaten bearbeitet, selbst die Rechtmässigkeit der Bearbeitung zu überprüfen. Schliesslich verletzt eine solche Bearbeitung den Grundsatz von Treu und Glauben sowie den Grundsatz der Zweckbindungsprinzip (Art. 4 Abs. 2 und 3 DSG).

11. In beiden Fällen (Switch und D.R.) kann kein Rechtfertigungsgrund (Art. 12 Abs. 2 und Art. 13 DSG) vorgebracht werden. Weder die Firma Switch – beziehungsweise die betroffenen in der Schweiz registrierten Personen – noch D.R. haben in die Bearbeitung der Daten eingewilligt. Ebensowenig gibt es ein Gesetz oder ein überwiegendes öffentliches Interesse, die eine Bearbeitung rechtfertigen würden (Art. 12 Abs. 2 und Art. 13 DSG). Schliesslich kann auch kein überwiegendes privates Interesse geltend gemacht werden; F.G. kann sich insbesondere auf keine Vertragsverhandlungen (Art. 13 Abs. 2 Bst. a DSG) mit Switch oder D.R. und auf keinen gegenwärtigen oder zukünftigen wirtschaftlichen Wettbewerb mit ihnen (Art. 13 Abs. 2 Bst. b DSG) berufen.

12. Der Vergleich mit anderen Produkten wie dem elektronischen Telefonbuch oder TwixTel ist zudem nicht stichhaltig. Diese Datenbanken wurden auf Grund von schon bestehenden Verträgen erstellt (Kundinnen und Kunden von Swisscom) und halten sich an die Bestimmungen der Telekommunikationsgesetzgebung; sie respektieren insbesondere den Wunsch von Personen, die keine Werbung erhalten möchten (mittels Kennzeichnung mit einem Stern), und die nicht wollen, dass ihre Daten veröffentlicht werden (via schwarze, rote, grüne und weisse Listen). Das Beschaffen von Daten im Internet, deren Verwendung nicht wie in den beiden oben erwähnten Fällen (Switch und D.R.) eingeschränkt ist, ist im Übrigen rechtmässig (Art. 12 Abs. 3).

13. Das Argument, wonach die Daten auf Grund des Prinzips «opt-in» beschafft worden sind, ist auch nicht stichhaltig. Bei der Beschaffung der Daten wurde nämlich von einem stillschweigenden Einverständnis ausgegangen. Dieses Vorgehen **widerspricht sowohl dem Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG) als auch dem Grundsatz der Richtigkeit der Daten (Art. 5 Abs. 1 DSG)**, wonach sich alle, die Personendaten bearbeiten, über deren Richtigkeit vergewissern müssen. Zudem stellt das von der «SwordLord-Foundation for new technology ethics» in Auftrag gegebene Dokument «Database Analysis Black Book 2000» auf Seite 10 schwere Mängel bei der Datenrichtigkeit fest (85 Prozent der E-Mail-Adressen seien unbrauchbar), was ebenfalls einer Verletzung von Artikel 5 DSG ist.

14. Die Personen schliesslich, die sich nachträglich gegen eine Veröffentlichung und Weiterleitung ihrer Daten durch Verkauf der CD-ROM wehren, verfügen über mehrere Rechte. So haben sie ein **Auskunftsrecht** (Art. 8 DSG). Artikel 8 Absatz 4 DSG sieht vor, dass eine Drittperson auskunftspflichtig ist, wenn sie den Inhaber der Datensammlung nicht bekannt gibt oder dieser nicht Wohnsitz in der Schweiz hat. Im vorliegenden Fall ist F.G. also **auskunftspflichtig**. Die betroffenen Personen ihrerseits können verlangen, dass unrichtige **Daten berichtigt** werden (Art. 5 Abs. 2 DSG) und dass die Bearbeitung eingestellt wird (Art. 15 DSG bzw. Art. 28-28l ZGB).

III. Auf Grund dieser Erwägungen empfiehlt der Eidg. Datenschutzbeauftragte:

1. Die Version 2000 der CD-ROM und alle eventuellen anderen Versionen, auf die der Sachverhalt zutrifft werden nach Erhalt dieses Schreibens nicht mehr vertrieben.
2. Die mit Hilfe der Switch Domain-Namen-Datenbank gesammelten Personendaten werden in der nächsten Version der CD-ROM nicht mehr enthalten sein.
3. Die Personendaten von Personen, die ausdrücklich schriftlich oder mündlich darauf hingewiesen haben, dass sie keine Werbung wünschen, werden in der nächsten bereinigten Version mit dem Vermerk «Wünscht keine Werbung» versehen. Dies gilt namentlich für die Daten von Personen, die sich mit einem Schreiben direkt an F.G. gewendet haben, die sich in eine Robinson-Liste eingetragen haben, die bei der Swisscom die Verwendung eines Sternchens vor ihrem Namen beantragt haben oder die mit einem klaren Hinweis auf ihrer Internetsite erklärt haben, dass sie keine Werbung wünschen.
4. Die Personendaten von Personen, die deren Veröffentlichung ablehnen, erscheinen in der nächsten Version der CD-ROM nicht mehr.
5. F.G. kommt seiner Auskunftspflicht nach und teilt den betroffenen Personen die Personendaten, die er bearbeitet, und deren Quellen mit.
6. Die unrichtigen Daten werden berichtigt; insbesondere wird der Vermerk «opt-in» nur verwendet, wenn eine explizite Einwilligung der betroffenen Person vorliegt.
7. Die vorliegende Empfehlung wird F.G. eingeschrieben zugestellt.
8. F.G. teilt dem Eidg. Datenschutzbeauftragten innerhalb von 30 Tagen nach Erhalt dieses Schreibens mit, ob er die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung abgelehnt oder nicht befolgt, so kann der Eidg. Datenschutzbeauftragte die Angelegenheit der Eidg. Datenschutzkommission zum Entscheid vorlegen.

EIDGENÖSSISCHER
DATENSCHUTZBEAUFTRAGTER

Hanspeter Thür