11. Tätigkeitsbericht 2003/2004

Eidgenössischer
Datenschutzbeauftragter

Tätigkeitsbericht 2003/2004 des Eidgenössischen Datenschutzbeauftragten

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 2003 und 31. März 2004 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

Datenschutz in Zeiten des Umbruchs. Die weltweite Terrorangst, mit welcher die westliche Welt in Zukunft allem Anschein nach leben muss, setzt in allen Demokratien Prinzipien einer freiheitlichen Ordnung auf den Prüfstand. Dass der Geissel Terrorismus durch weltweite Zusammenarbeit und verstärkte Aufklärung begegnet werden muss, ist unbestritten. Weniger klar ist, was unter dem Titel Prävention in einer liberalen Demokratie zulässig ist. Eine präventive Massnahme muss zunächst das Ziel verfolgen, terroristische Strategien in ihrem sozialen Umfeld zu isolieren. Eine so definierte Strategie verstünde unter präventiven Massnahmen in erster Linie das Bemühen, jenem Teil der Bevölkerung, der den Terrorismus tendenziell unterstützt und trägt, alle elementaren – auch die sozialen und wirtschaftlichen – Menschenrechte zu sichern. Solange die Ausschaltung terroristischer Aktivisten nicht verhindern kann, dass diese am nächsten Tag durch neue Zellen ersetzt werden, hat die Prävention ihr Ziel nicht erreicht.

Leider zeigen die aktuellen Diskussionen, dass man unter dem Begriff Prävention in erster Linie den Versuch versteht, durch polizeiliche Mittel mögliche Täter frühzeitig zu fassen. Diskutiert werden die präventive Telefonabhörung oder Abhörmassnahmen in privaten Räumen ausserhalb eines Strafverfahrens. Bevor die verfassungsrechtliche Zulässigkeit geprüft wird, ist darauf hinzuweisen, dass die Strategie nur dann auch langfristig erfolgreich wäre, wenn auf diesem Weg das Übel Terrorismus an der Wurzel beseitigt werden könnte. Da sind Zweifel mehr als angebracht.

Eine interessante Diskussion über die grundrechtlichen Aspekte einer solchen Massnahme fand in Deutschland statt. Dort hat das Bundesverfassungsgericht im Frühjahr 2004 die Lauschangriffe massiv eingeschränkt und den Schutz von Privaträumen erheblich gestärkt. Die bisherige Abhörpraxis verletze die Menschenwürde und sei deshalb in wesentlichen Teilen verfassungswidrig. Nach dem Urteil bleibt die akustische Überwachung von Wohnungen und Telefongesprächen grundsätzlich möglich, muss aber an deutlich strengere Voraussetzungen geknüpft werden als bisher. Neben der Forderung, dass der «Kernbereich privater Lebensgestaltung» stets zu respektieren sei, verlangt das Verfassungsgericht konkret, dass solche Überwachungsmethoden nur bei besonders schweren Delikten in Betracht kommen dürfen.

Diese Grundsätze sind ohne weiteres auf die Schweiz übertragbar, da wir in Bezug auf die Ausgestaltung der Grundrechte vergleichbare Verfassungsgrundlagen haben.

Das ist von Bedeutung, da bei uns derzeit Abhörmassnahmen diskutiert werden, die ausserhalb eines Strafverfahrens eingesetzt werden können. Das ist aus verschiedenen Gründen heikel. Der entscheidende Kritikpunkt bezieht sich auf den Umstand,

dass eine solche Überwachung, die ohne die Einleitung eines Strafverfahrens angeordnet werden könnte, sich nicht im Rahmen eines rechtstaatlichen Verfahrens rechtfertigen müsste und auch nicht entweder durch die Einstellung des Strafverfahrens oder die Erhebung einer Anklage zwangsläufig beendet würde. Wenn der Überwachte selber Akteneinsicht erhält, wird er spätestens zu diesem Zeitpunkt die Rechtmässigkeit der Massnahme überprüfen können. Bei einer präventiven Überwachung ausserhalb eines Strafverfahrens fiele diese Kontrolle weg.

Vor dem Erlass neuer Gesetze ist im Übrigen darauf hinzuweisen, dass nicht nur die Frage nach der Wirksamkeit der zur Diskussion gestellten Massnahmen gestellt, sondern zuallererst die Wirksamkeit der bestehenden Gesetze überprüft werden muss. Allzu schnell reagiert nämlich der Gesetzgeber in Krisenzeiten mit der Schaffung neuer Gesetze, bevor analysiert wurde, ob es an adäquaten Gesetzen oder lediglich am Vollzug derselben mangelte.

Auch auf internationaler Ebene werden Massnahmen erörtert und beschlossen. Im März dieses Jahres verabschiedete die EU eine umfangreiche Deklaration zur Bekämpfung des Terrorismus. Zur Diskussion stehen zahlreiche Massnahmen, von denen kaum alle der Terrorismusbekämpfung dienen. Die Frage ist in jedem einzelnen Fall zu stellen, ob eine Massnahme zur Bekämpfung des Terrorismus tatsächlich auch nötig und geeignet ist, oder ob sie eher auf eine umfassende Überwachung der Bürger abzielt und potentiell zur sozialen und politischen Kontrolle benützt werden kann. Es ist evident, dass zwischen der Wahrung der Menschenrechte und der öffentlichen Sicherheit ein Spannungsverhältnis besteht. Deshalb ist eine sorgfältige Interessenabwägung erforderlich. Fraglich ist, ob diese Interessenabwägung ausreichend respektiert wird. Auch wenn eine harte Gangart gegen gewaltbereite terroristische Kräfte in Europa verständlich und nötig ist, kann in einem liberalen Rechtsstaat nicht darauf verzichtet werden, dass beim Erlass antiterroristischer Massnahmen eine sorgfältige Interessenabwägung erfolgt und sie auf ihre Notwendigkeit, Nützlichkeit und Verhältnismässigkeit hin überprüft werden.

Umfassende Überwachungsmassnahmen werden inzwischen sogar als Wachstumsmotor für die Wirtschaft entdeckt und gepriesen, wie kürzlich einem Artikel in der Sonntagspresse entnommen werden konnte. Folgerichtig ist, dass aus dieser Perspektive der Datenschutz nur noch als «Korsett» gesehen wird, das zu beseitigen ist. Man träumt davon, dass die «anstehenden Verknüpfungen über die elektronischen Überwachungsnetze» auch wirtschaftlich nutzbar gemacht werden sollten. Kaum verwunderlich, dass bei solchen marktzentrierten Denkansätzen die Tatsache, dass der Schutz der Privatsphäre eine grundrechtliche Dimension hat, vollständig ignoriert wird und nicht einmal im Rahmen einer Güterabwägung zwischen öffentlicher Sicherheit, wirtschaftlicher Effizienz und verfassungsmässig garantierten Freiheitsrechten

eine Erwähnung findet. Ausgeblendet wird zudem, dass ein effizienter Datenschutz gerade auch für das Funktionieren einer auf Konkurrenz basierten Wirtschaft von grosser Wichtigkeit ist.

Wenn der Verknüpfung elektronischer Überwachungsnetze das Wort geredet wird, ist darauf hinzuweisen, dass heute aufgrund der technischen Möglichkeiten Kontrollen Orwell'schen Ausmasses realisierbar sind. Mit der Chip-Markierung (über RFID-Etiketten) sind Güter, Personen oder ihre Dienste auf dem ganzen Territorium lokalisierbar. Die daraus gewonnen Informationen könnten problemlos mit andern Datenbanken (Telefonverbindungsdaten, Kreditkarteneinkäufe, Bankkonti, Kundenkarten usw.) verknüpft werden, was die Erstellung von sehr detaillierten Persönlichkeitsprofilen ermöglichen würde. Der gläserne Mensch ist längst keine literarische Metapher mehr, sondern eine mögliche Perspektive für die sehr nahe Zukunft.

Dass den Bewohnerinnen und Bewohner der Schweiz diese Zukunftsaussichten Sorgen bereiten, ergab eine im Frühjahr 2004s publizierte repräsentative Meinungsumfrage des neu gegründetes Rates für Persönlichkeitsschutz, «einer Lobby für Persönlichkeitsrechte im weitesten Sinne»: Obwohl eine überwältigende Mehrheit der Befragten dem Persönlichkeitsschutz sehr hohe Priorität einräumt, ist eine ebenso grosse Mehrheit der Überzeugung, dass man sich gegen die missbräuchliche Verwendung der Daten kaum schützen könne und die bestehenden Gesetze nicht genügten. Das ist eine deutliche Aufforderung an den Gesetzgeber, dem Persönlichkeitsschutz angesichts der Gefährdungen, die durch den technologischen Fortschritt noch zunehmen werden, hohe Priorität einzuräumen und die gesetzlichen Instrumente zu verbessern.

Hanspeter Thür

Abkürzungsverzeichnis

AG	Aktiengesellschaft
BGE	Bundesgerichtsentscheide
BSV	Bundesamt für Sozialversicherung
BV	Bundesverfassung
CIRCA	Communication & Information Resource Centre Administrator
DSG	Bundesgesetz über den Datenschutz
EDSB	Eidgenössischer Datenschutzbeauftragter
EDSK	Eidgenössische Datenschutzkommission
GV	Generalversammlung
IDA	Interexchange of Data between Administrations (Informationsaustausch zwischen öffentlichen Verwaltungen)
KVG	Bundesgesetz über die Krankenversicherung
RFID	Radio Frequency Identification
SUVA	Schweizerische Unfallversicherungsanstalt
UVG	Unfallversicherungsgesetz
VAG	Bundesgesetz betreffend die Aufsicht von Versicherungsunternehmen
VBS	Departement für Verteidigung, Bevölkerungsschutz und Sport
VR	Verwaltungsrat
VVG	Bundesgesetz über den Versicherungsvertrag
WPISP	Working Party for Information Security and Privacy
ZIS	Zentrales Informationssystem

1. Grundrechte

1.1 Verschiedene Themen

1.1.1 Publikationsgesetz: Risiken und Probleme bei der Veröffentlichung von Personendaten im Internet

Im Rahmen einer Ämterkonsultation zum Publikationsgesetz wurden wir gebeten, uns zu den Risiken und Problemen zu äussern, wenn ein Bundesorgan Personendaten im Internet veröffentlicht. Die so publizierten Personendaten können mittels elektronischen Suchmaschinen weltweit und vor allem zeitlich uneingeschränkt (d.h. noch jahrelang) aufgefunden werden. Bevor ein Bundesorgan Daten von Bürgerinnen und Bürgern im Internet veröffentlicht, muss es grundsätzliche Überlegungen anstellen, denn gerade den Staat trifft eine besondere Pflicht, den verfassungsrechtlich geschützten Anspruch jeder Person auf Schutz vor Missbrauch ihrer persönlichen Daten einzuhalten.

Das Publikationsgesetz regelt die Veröffentlichung der Sammlungen des Bundesrechts und des Bundesblatts. Im Bundesblatt werden u.a. auch die Namen von Personen publiziert, die von Notifikationen, Verfügungen oder Vorladungen betroffen sind.

Der Revisionsentwurf sah unter anderem vor, dass Personendaten in der elektronischen Form (also auch über Internet) grundsätzlich anonymisiert veröffentlicht werden müssen und eine Publikation der Personendaten im Internet nur ausnahmsweise erfolgen darf. Laut Revisionsentwurf muss dies in einem Spezialgesetz ausdrücklich so vorgesehen sein. Wir haben diese Lösung für die Veröffentlichung von Personendaten im Internet durch ein Bundesorgan ausdrücklich unterstützt und dies ausführlich begründet.

Gesetzliche Grundlagen

Die Bundesverfassung gewährt jeder Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Das DSG definiert als Personendaten jene Angaben, die sich auf eine bestimmte oder bestimmbare (natürliche oder juristische) Person beziehen. Das DSG unterscheidet also nicht zwischen positiven oder negativen Personendaten, sondern schützt diese ohne Wertung in ihrer Gesamtheit. Eine Qualifizierung sieht das DSG für besonders schützenswerte Personendaten und Persönlichkeitsprofile vor.

Ein Bundesorgan benötigt gemäss DSG für jedes Bearbeiten von Personendaten eine hinreichend bestimmte gesetzliche Grundlage. Werden besonders schützenswerte Personendaten oder Persönlichkeitsprofile in einem Abrufverfahren (wie

beispielsweise im Internet) zugänglich gemacht, muss dies in einem Gesetz im formellen Sinn ausdrücklich vorgesehen sein.

An die hinreichende Bestimmtheit der gesetzlichen Grundlage werden folgende Anforderungen gestellt:

- Definition des Bearbeitungszwecks;
- Umschreibung des Umfangs der Datenbearbeitung in groben Zügen (Nachvollziehbarkeit für die betroffenen Personen);
- Festhalten der Beteiligten an der Datenbearbeitung (Datenbearbeiter; Datenempfänger);
- Aufführen der Kategorien der bearbeiteten Daten (sofern besonders schützenswerte Personendaten oder Persönlichkeitsprofile betroffen sind).

Problematik der Veröffentlichung von Personendaten im Internet

Informationen aus dem Bundesblatt können mit Angaben aus anderen öffentlichen Registern und öffentlich zugänglichen respektive privaten Datensammlungen verknüpft werden. Dies können durchaus auch besonders schützenswerte Personendaten sein. Mit allen verfügbaren Informationen können unter Umständen sogar Persönlichkeitsprofile erstellt werden.

Es gibt zahlreiche Unternehmen, die sich auf das systematische Sammeln und Auswerten von Personendaten spezialisiert haben. Sie benützen dazu immer auch Informationen aus amtlichen Publikationen (Amtsblätter, Handelsregister, Betreibungsregister usw.) und erstellen damit Datensammlungen (beispielsweise Bonitätsdatensammlungen, Adressdateien; sogenanntes Monitoring [systematische und kontinuierliche Überwachung]).

Die Praxis zeigt, dass dabei Personendaten über Jahre hinweg (z.B. auf Archivlisten von Suchmaschinenbetreibern) gespeichert bleiben und nicht mehr auf ihre Aktualität und/oder Richtigkeit überprüft werden. Oft haben die Betroffenen keine Kenntnis von der Speicherung oder Bearbeitung ihrer Daten. Um so schwieriger gestaltet sich daher die Ausübung ihrer Rechte (Auskunfts-, Berichtigungs-, Löschungsrecht gemäss DSG). Bezeichnend für die Publikation von Personendaten im Internet ist, dass die Betroffenen die Herrschaft über die eigenen Daten vollständig verlieren.

Die Auswirkungen für die Betroffenen sind dabei nicht zu unterschätzen: Dritte können unkontrolliert gesammelte Informationen zusammentragen und verbreiten (z.B. Kreditwürdigkeit, Beurteilung des Kaufverhaltens, staatliche Verfolgungen und Sankti-

onen). Es muss davon ausgegangen werden, dass inskünftig alle Personendaten, die eine Behörde in elektronischer Form publiziert (z.B. Grundbuchdaten oder Informationen über Personen, die im Bundesblatt veröffentlicht werden), gezielt erfasst, mit andern Daten verknüpft und ausgewertet werden. Als Datenbearbeiter fallen nicht nur Privatpersonen, sondern auch in- und ausländische Behörden in Betracht.

Als eigentliche Datenverantwortliche verliert die amtliche Stelle nach der Publikation jeglichen Einfluss auf die weitere Verwendung der Personendaten durch Dritte. Die Betroffenen müssen somit hinnehmen, dass ursprünglich öffentlich zugängliche Daten durch Dritte – ohne Möglichkeit der Einflussnahme und der Kontrolle – zweckgeändert weiterverwendet werden. Gerade das Veröffentlichen von Personendaten im Internet erhöht die Missbrauchsgefahr erheblich. Angesichts der besonderen Eigenschaften des Internets kann der Datenschutz nicht sichergestellt werden (fehlende Garantie hinsichtlich Vertraulichkeit, Integrität, Authentizität der Personendaten).

Als wichtigste Risiken einer Veröffentlichung von Personendaten im Internet können folgende Punkte erwähnt werden:

- Die publizierten Informationen sind weltweit zugänglich, also auch in Staaten ohne Datenschutzbestimmungen, die den schweizerischen gleichwertig sind.
- Nach den publizierten Informationen (auch und insbesondere Namen) kann weltweit gesucht werden.
- Mit der Veröffentlichung verlieren nicht nur die Betroffenen, sondern auch der ursprünglich verantwortliche Datenbearbeiter faktisch jede Kontrolle über die Zwecke künftiger Bearbeitung.
- Informationen können völlig anders verstanden werden, als ursprünglich beabsichtigt war. Dies kann sich erstens in einem Missverständnis äussern, das sich aus den Umständen einer unvorhergesehenen Situation ergibt. Zweitens ist es möglich, dass Personen/Organisationen die Informationen zu Zwecken benutzen, an die beim Veröffentlichen nicht gedacht wurde, und damit Interessen verfolgen, die denjenigen der Betroffenen entgegenstehen.
- Die veröffentlichten Informationen können faktisch nicht mehr gelöscht werden; was einmal publiziert ist, kann man nicht mehr kontrollieren.
- Es ist nie vollständig auszuschliessen, dass Daten zufällig oder absichtlich verändert und damit falsch werden.
- Die Daten werden länger online gehalten als für den beabsichtigen Zweck notwendig.

Bewertung

Das Grundrecht auf Schutz der Privatsphäre (Art. 13 Abs. 2 BV) verpflichtet den Staat, die Daten seiner Bürgerinnen und Bürger vor Missbrauch zu schützen. Bei der Frage, ob amtliche Publikationen von Personendaten künftig auch im Internet erfolgen dürfen, muss die verantwortliche Behörde allen Risiken Rechnung tragen. Dazu gehört auch, dass die Behörde mögliche Auswirkungen einer von ihr veranlassten Datenbearbeitung im Internet gebührend berücksichtigt.

Art. 13 BV setzt den Behörden klare Grenzen hinsichtlich der elektronischen Bekanntgabe von Personendaten: Aufgrund der damit verbundenen Risiken sollte eine staatliche Einrichtung *grundsätzlich* darauf verzichten, Personendaten von Bürgerinnen und Bürgern im Internet zu veröffentlichen.

Es geht somit nicht in erster Linie um die Frage, ob die Folgen der Publikation eines Namens oder die damit verbundene Information die Persönlichkeit der betroffenen Person gefährdet respektive ob deren Inhalt von der Gesellschaft als positiv oder negativ bewertet wird. Auch der Einwand, die blosse Publikation eines Namens sei ja gar nicht so gravierend, greift demnach nicht.

Vielmehr gilt es zu beachten, *wie* diese Informationen in der Zukunft verwendet werden können. Die modernen Kommunikationsmittel erlauben heute, losgelöst vom ursprünglichen Sinn und Zweck amtlicher Publikationen, eine umfassende und nicht kontrollierbare Personendatenbearbeitung. Mit anderen Worten: Eine (amtliche) Publikation kann noch nach Jahren negative Auswirkungen für eine Person entfalten, obwohl der ursprüngliche Zweck der Veröffentlichung sinnvoll erscheinen mag respektive rechtmässig erfolgte.

Eine Behörde trägt die Verantwortung dafür, dass die Art und Weise ihres Bearbeitens von Personendaten die Betroffenen *zu keinem Zeitpunkt* in ihrer Persönlichkeit verletzt.

Das Grundrecht auf Schutz der Privatsphäre, das Verhältnismässigkeitsprinzip und die Zweckbindung sowie Art. 19 Abs. 3 DSG lassen nur eine Möglichkeit zu:

Staatliche Organe müssen in elektronischer Form publizierte Personendaten grundsätzlich anonymisieren. Ausnahmen sind nur möglich, wenn eine formellrechtliche Grundlage ausdrücklich vorsieht, dass ein bestimmter Bearbeitungszweck eine Veröffentlichung bestimmter Personendaten verlangt.

Bundesgericht

Zur Veröffentlichung von Bundesgerichtsentscheiden im Internet siehe unseren 9. Tätigkeitsbericht 2001/2002, Abschnitt 2.3.3;

http://www.edsb.ch/d/doku/jahresberichte/tb9/kap3c.htm#233.

Zur Stellung des Straftäters in der Öffentlichkeit siehe BGE 109 II 353ff.

1.1.2 Übermittlung von Personendaten durch Luftfahrtgesellschaften an US-Behörden

In Hinblick auf die Erfordernisse der Datenschutzgesetzgebung wäre ein Abkommen für die Übermittlung von Passagier-Personendaten durch schweizerische Fluggesellschaften an die US-Behörden die beste Lösung. Durch die blosse Information der Passagiere werden nicht alle Datenschutzvorschriften erfüllt, da erstens die Zustimmung der betroffenen Personen nicht als freiwillig bezeichnet werden kann und da zweitens die Daten an einen Drittstaat übermittelt werden, der keinen Datenschutz garantiert, der dem schweizerischen gleichwertig ist. Allerdings könnte die auf der Information der betroffenen Personen basierende Lösung angewandt werden, bis ein bilaterales Abkommen in Kraft tritt.

Neben den zahlreichen Sicherheitsmassnahmen verlangen die US-amerikanischen Behörden im Rahmen der Terrorismusbekämpfung von den Fluggesellschaften, welche die Vereinigten Staaten anfliegen (Ankunft, Abflug, Transit), den Zugriff auf sämtliche Passagierdaten. Im Fall der Weigerung drohen Sanktionen, die bis zum Landeverbot im amerikanischen Hoheitsgebiet reichen können. Damit die schweizerischen Fluggesellschaften als Privatpersonen den US-Behörden Personendaten übermitteln können, muss ein Rechtfertigungsgrund vorliegen: eine Gesetzesbestimmung, ein überwiegendes öffentliches oder privates Interesse oder die Zustimmung der betroffenen Personen.

Die US-Gesetze gelten in der Schweiz nicht, und es gibt gegenwärtig keinen Vertrag zwischen den Vereinigten Staaten und der Schweiz über die systematische Übermittlung der Daten von Passagieren, die in das amerikanische Hoheitsgebiet ein-, aus diesem aus- oder durch dieses hindurchreisen.

Die Massnahmen, welche die amerikanischen Behörden im Auge haben, erfüllen die Grundsätze der Verhältnismässigkeit und der Zweckbindung nicht. Ein überwiegendes öffentliches oder privates Interesse kann daher nicht geltend gemacht werden. Das Beschaffen zahlreicher Personendaten – einschliesslich besonders schützens-

werter Gesundheitsdaten oder von Daten, die Rückschlüsse auf die Religion erlauben – ist nicht verhältnismässig. Die amerikanischen Behörden geben zu unbestimmte Verwendungszwecke an, die sich zudem nicht auf die Terrorismusbekämpfung beschränken. Ausserdem ist eine übermässig lange Aufbewahrungsfrist geplant. Nichtamerikanischen Staatsbürgern fehlt jegliche konkrete Möglichkeit, um bei missbräuchlicher Nutzung ihrer Personendaten durch die amerikanischen Behörden ihre Rechte geltend zu machen.

Als Lösung bleibt deshalb die Information und das Einholen der Zustimmung der betroffenen Personen. Da die Vereinigten Staaten keinen Datenschutz kennen, der dem schweizerischen gleichwertig ist, muss die Frage des Schutzes der übermittelten Daten mit den amerikanischen Behörden vertraglich geregelt werden. Ein solcher Vertrag muss insbesondere den Zweck der Übermittlung, die Aufbewahrungsfrist und die Regeln über das Löschen ausweisen und festhalten, dass die Daten nicht zu anderen Zwecken verwendet werden. Ausserdem ergibt sich aus dem Zweckbindungsprinzip, dass den Behörden nur die Daten derjenigen Personen, die zum gegenwärtigen Zeitpunkt in die Vereinigten Staaten reisen möchten, bekannt gegeben werden. Auch diese Lösung lässt jedoch zu wünschen übrig. Erstens kann die Zustimmung der betroffenen Personen nicht als freiwillig bezeichnet werden. Zweitens bietet ein Vertrag, welcher die oben erwähnten Datenbearbeitungen regelt, keine absolute Garantie gegen die Verwendung der Daten im Rahmen von besonderen amerikanischen Gesetzesmassnahmen. Eine Alternative zur oben dargelegten Lösung bestünde darin, mit den amerikanischen Behörden ein Abkommen abzuschliessen, welches die fraglichen Datenübermittlungen in einen Gesetzesrahmen stellt.

Die schweizerischen Behörden haben wie ihre europäischen Pendants beschlossen, Verhandlungen mit den amerikanischen Behörden aufzunehmen. Unter der Leitung des Bundesamts für Zivilluftfahrt soll eine interdepartementale Arbeitsgruppe, in der wir auch vertreten sind, ein Abkommen ausarbeiten, das die Flugverbindungen mit den Vereinigten Staaten unter Achtung der allgemeinen Datenschutzgrundsätze garantieren soll. Um Unannehmlichkeiten für Reisende zu vermeiden und um einen Mindestschutz der Personendaten von Fluggästen zu gewährleisten, könnte bis zum Inkrafttreten des fraglichen Abkommens provisorisch eine Lösung angewandt werden, die darin besteht, die Passagiere zu informieren und ihre Zustimmung einzuholen.

Siehe auch Abschnitt 11.4.1.

1.2 E-Government

1.2.1 Arbeiten betreffend Datenschutzfragen im E-Government

Im Zusammenhang mit dem so genannten E-Government existieren in der Verwaltung mehrere Projekte, deren reine Grössenordnung es dem EDSB verunmöglicht, sie ernsthaft zu begleiten. Deshalb haben wir die Projektverantwortlichen verschiedener Vorhaben darauf hingewiesen, dass sie in der Projektorganisation auch die Verantwortung für den Datenschutz festlegen und entsprechendes Know-how beschaffen müssen.

Wie schon in den vergangenen beiden Tätigkeitsberichten ausgeführt, sind die Ziele verschiedener Vorhaben im Umfeld der elektronischen Verwaltung ausserordentlich unbestimmt formuliert. Beispielsweise ist für den Guichet Virtuel im Anhang 2 zur E-Government Strategie des Bundes (Stand April 2003) das Ziel beschrieben als «Vereinfachen der Kontaktaufnahme mit den Behörden, erhöhte Transparenz der Tätigkeiten der Behörden, Ermöglichung von Transaktionen.» Aufgrund solcher Zielformulierungen sind sinnvolle Überlegungen zu Datenschutz und Datensicherheit nicht möglich, weil klare Ziele unabdingbare Voraussetzung für solche Überlegungen sind. Hier sehen wir uns einem nicht lösbaren konzeptuellen Widerspruch gegenüber. Für uns besteht daneben das Problem, dass die Vielzahl von Vorhaben sowie die reine Grössenordnung mancher davon es uns verunmöglichen, diese auch nur einigermassen zu begleiten. Um diese beiden Probleme einer Lösung näher zu bringen, haben wir die Projektverantwortlichen auf das eigentlich Selbstverständliche hingewiesen: Weil die Auftraggeber von Projekten des E-Government für die Einhaltung des Datenschutzes in ihren Vorhaben verantwortlich sind, müssen sie auch in der Projektorganisation entsprechende Verantwortlichkeiten festlegen lassen. Die Projektverantwortlichen haben ebenfalls dafür zu sorgen, dass Datenschutz-Know-how im Rahmen der Projekte vorhanden ist.

2. Datenschutzfragen allgemein

2.1 Datenschutz und Datensicherheit

2.1.1 EDSB-Office: Geschäftsverwaltungssystem mit hoher Vertraulichkeit und Datenverfügbarkeit

Die Chiffrierung von sensiblen Daten im Rahmen einer Public Key Infrastructure gewährleistet heute ein hohes Mass an Vertraulichkeit. Zudem können wir dank der jüngsten Systemumstellung auf zwei Cluster-Server eine hohe Verfügbarkeit unserer Daten bieten. Die Redundanz der Server ermöglicht es ausserdem, die unverzichtbaren Wartungsvorgänge während der normalen Arbeitszeiten und vor allem ohne Systemunterbrechung durchzuführen.

Die Funktionen und die Datenverfügbarkeit von EDSB-Office – das Ergebnis von Bestrebungen, die hohen internen Ansprüchen an die Datenvertraulichkeit genügen sollten (vgl. unseren 8. Tätigkeitsbericht 2000/2001, Abschnitt. 7.5) – haben sich weiter entwickelt. Es sei daran erinnert, dass die Vertraulichkeit durch Chiffrierung und Dechiffrierung der sensiblen Datenbearbeitungen auf jedem Arbeitsplatzrechner, einschliesslich der Ausgabe von Daten an einen Netzdrucker, gewährleistet wird. Diese technischen Massnahmen gehen mit entsprechenden organisatorischen Massnahmen einher, um das angestrebte Vertraulichkeitsniveau flächendeckend zu erreichen. Unsere Anwendung, die auf einer klassischen relationalen Datenbank beruht, setzt den Aufbau einer Public Key Infrastructure (PKI) voraus, im vorliegenden Fall auf der Basis der Software PGP (Pretty Good Privacy). Die Generierung des Schlüsselpaars, die physische Verwaltung des durch eine «Passphrase» geschützten privaten Schlüssels und der Import der benötigten öffentlichen Schlüssel erlaubte es den Benutzern, praktische Erfahrungen mit der asymmetrischen Kryptographie zu sammeln. Diese Elemente sind vollständig in die Anwendung integriert, damit der Benutzer sich in einem standardmässigen Büroautomatikumfeld auf seine Alltagsarbeit – Dokumenten- und Dossierverwaltung, Terminplanung – konzentrieren kann. Verschiedene Chiffrierungsgruppen gewährleisten einen differenzierten Zugriff auf die Dokumente. Damit wird der Grundsatz der Verhältnismässigkeit beachtet. Das setzt ebenfalls voraus, dass den Administratoren der Applikation nicht alle Entschlüsselungsrechte erteilt werden. Damit ist die wirtschaftliche und operationelle Machbarkeit der gesicherten Speicherung von sensiblen Daten in chiffrierter Form erwiesen. Die Reaktionszeiten für das Abspeichern und Öffnen von Dokumenten sind in einer üblichen Hardwareumgebung völlig zufriedenstellend.

Unter den Funktionalitäten ist zunächst die Volltextsuche zu erwähnen. Damit lassen sich beliebige gespeicherte Dokumente nach inhaltlich signifikanten Stichwörtern wieder finden. Ferner ist die bidirektionale Schnittstelle mit dem E-Mail-Programm Outlook zu nennen, welche als wesentlichen Vorteil eine perfekte Integration des Maileingangs und -ausgangs in das Geschäftsverwaltungssystem bietet. Damit wird die Klippe der parallelen Archivierung des E-mail Verkehrs, der ständig an Bedeutung gewinnt, umschifft.

Schliesslich ist festzustellen, dass die Verfügbarkeit der Daten im Jahr 2003 dank der Inbetriebnahme von Cluster-Servern stark erhöht wurde. Die Dateien-, Datenbank- und Druckdienste sind in weniger als einer Minute nach einem Serverausfall vollständig verfügbar. Diese Fähigkeit lässt sich im Übrigen nutzen, um die unverzichtbaren technischen Wartungsvorgänge während der üblichen Arbeitszeiten ohne Systemunterbrechung durchzuführen. Der Rechner im Ruhestand wird aktualisiert, während der andere Rechner im Betriebszustand läuft; auf dem zweiten kann nach der integralen Betriebsaufnahme des ersten die gleiche Aktualisierung vorgenommen werden. Dank der hohen Datenintegrität, welche die aktuelle Soft- und Hardware bieten, darf EDSB-Office als Anwendung mit integraler Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) der Daten bezeichnet werden.

2.1.2 Standards im Bereich Informationssicherheit und -schutz

Es gibt eine Fülle von Standards betreffend die Informationssicherheit. Wir befassten uns mit dem internationalen Standard ISO 17799, der als sehr vollständiger einschlägiger Referenzstandard gilt. Das letzte Kapitel behandelt die Gesetzeskonformität und besonders die Datenschutzaspekte. Der Standard BS7799-2 ermöglicht einen nahtlosen Übergang zum Audit-Bereich, welcher im Übrigen im Rahmen der Revision unseres Datenschutzgesetzes als Gegenstand eines neuen Artikels vorgeschlagen wird.

Die Informationssicherheit umfasst technologische und juristische Aspekte der Datensicherheit und des Datenschutzes. In diesem Bereich sind heute de facto mehrere nationale und internationale Standards anzutreffen: ISF/SoGP, OIT/ISG, BS 15000 (ITIL), BS 7799, ISO 17799, ISO 13335 usw. Wir haben uns mit dem internationalen Standard ISO 17799:2000 (Code of Practice for Information Security Management) sowie mit dem britischen Pendant BS 7799-2:2002 (Information Security Management Systems) beschäftigt. Der erste Standard bildet ein sehr vollständiges Referenzsystem (CoP: Code of Practice), mit welchem sich die technischen und organisatorischen Informationssicherungsmassnahmen je nach den vom Inhaber der Datensammlung (Unternehmen) als vertretbar eingestuften Risiken festlegen lassen. ISO 17799 umfasst zehn

Sicherheitsziele, die formell von drei bis zwölf nummeriert sind; das erste bildet die absolute Grundlage des Standards:

- *Sicherheitspolitik*
- Organisation der Sicherheitspolitik (Infrastruktur, Zugriff durch Dritte, Externalisierung …)
- Einstufung und Kontrolle der Werte (Etikettierung, Handhabung …)
- Personelle Sicherheit (Verantwortung, Ausbildung, Sanktionen bei Missbrauch …)
- Physische Sicherheit (Räumlichkeiten, Ausrüstungen, Allgemeines)
- Management Kommunikation und Betrieb (Verfahren, Kapazität, Malware, Routinevorgänge, Netz, Wartung der Datenträger, Informationsaustausch)
- Zugangskontrolle (Bedürfnisse, Benutzer, Passwörter, Netzdienste, Betriebssysteme, Applikationen, Überwachung, tragbare Geräte, Telearbeit)
- Systementwicklung und -wartung (Applikationen, Kryptographie, Upgrades, Korrekturprogramme, Testdaten …)
- Management Geschäftsbetrieb (Plan, Test, Wartung)
- Einhaltung der Verpflichtungen (gesetzliche und technische Anforderungen, die der Informationssicherheitspolitik folgen; Protokollierung)

Das erste Ziel – die Politik der Informationssicherheit – entspricht dem zentralen Dokument mit einer Reihe strategischer und konzeptueller Ziele über die globale Informationssicherheit einer Organisation. Die meisten durch die neuen Informations- und Kommunikationstechnologien verursachten Probleme werden unter den Zwischenzielen berücksichtigt.

Das letzte Ziel ist für uns von grösstem Interesse, da es die Aspekte der Konformität mit den Gesetzesauflagen – besonders denjenigen des Datenschutzes – umfasst. Ein besonderer Akzent kann auf die wesentlichen Grundsätze Rechtmässigkeit, Transparenz, Verhältnismässigkeit und Zweckmässigkeit der Bearbeitung, Datenrichtigkeit, Auskunftsrecht und Anmeldepflicht von Datensammlungen gelegt werden. Die Protokollierungen, die Informationen über bestimmte oder bestimmbare Personen enthalten, sollten unbedingt gemäss obigen Grundsätzen behandelt werden. So erlaubt dieser internationale Standard, die Datenschutz- und Datensicherheitsmassnahmen je nach Anwendungskontext zu gewichten. Auf dieser Basis wird anschliessend der britische Standard BS 7799-2 eingesetzt, um ein Informationssicherheits-Managementsystem einzuführen. In einem Audit dieses Systems lässt sich ermitteln, ob die Informationsbearbeitung den gestellten Anforderungen entspricht. Vor diesem Hinter-

grund ist der im Rahmen der aktuellen DSG-Revision vorgeschlagene neue Artikel 11 zu sehen, welcher das Zertifizierungsverfahren (Organisationen oder Produkte) im Datenschutzbereich betrifft.

2.1.3 Elektronische Spuren am Arbeitsplatz

Am Computer durchgeführte Tätigkeiten hinterlassen elektronische Spuren, welche teilweise Personendaten enthalten. Das Beschaffen und Bearbeiten dieser Daten unterliegt dem DSG.

Die meisten Aufgaben im Beruf und im Privatleben werden heute mit Hilfe eines Computers erledigt. Alle diese Tätigkeiten hinterlassen elektronische Spuren, mit denen sich theoretisch das Vorgehen des Benutzers (wer, was, wann) rekonstruieren lässt. Das Potenzial eines Eindringens in die Privatsphäre ist erheblich.

Das DSG gilt für Personendaten, welche in den folgenden Kategorien von elektronischen Spuren enthalten sind:

- Logfiles;
- Temporäre Dateien: *.TMP, Index.dat und Cookies;
- Registryeinträge und Konfigurationsdateien (*.INI);
- Verläufe: Betriebssystem, Browser, Anwendungen usw.;
- Zwischenablagen (Clipboards);
- Papierkörbe;
- persönliche Archive (*.PST);
- Sicherheitskopien (Backups).

Daneben stellt sich die Frage des logischen oder physischen Löschens. Auf einem elektronischen Datenträger logisch gelöschte Daten lassen sich leicht wiederherstellen. Deswegen wird empfohlen, physische Löschprogramme zu benutzen, welche die Daten durch mehrmaliges Überschreiben vernichten.

Ein Unternehmen darf elektronische Spuren bearbeiten, um die Einhaltung der Richtlinien über die Nutzung der Informatikressourcen und die Effizienz der Sicherheitsmassnahmen zu überprüfen. In der Regel erzeugt Software elektronische Spuren. Deswegen ist es erforderlich, die Datenschutznormen festzulegen, die auf solche Fälle anwendbar sind. Gemäss dem DSG müssen die folgenden Vorschriften befolgt werden:

- der Inhaber der Datensammlung muss den Bearbeitungszweck klar definieren;
- es existieren keine alternativen Lösungen, die gleich effizient sind, aber die Privatsphäre in geringerem Masse beeinträchtigen;
- die Transparenz gegenüber den betroffenen Personen ist gewährleistet;
- es werden nur die für den Bearbeitungszweck erforderlichen Daten gesammelt;
- die vorgesehene Aufbewahrungsfrist wird eingehalten;
- die Auswertungen erfolgen nach vordefinierten und überprüfbaren Verfahren;
- alle bearbeiteten Daten werden gesichert;
- ein Mechanismus für die Ausübung des Auskunftsrechts wird im Vorfeld definiert.

Die Auswertungen der Logfiles müssen klar geregelt werden. Wegen des hohen Risikos von unerlaubten Zugriffen auf Personendaten handelt es sich dabei um die grösste Schwachstelle. Zur Vermeidung von Missbräuchen sollten die Auswertungen von einer kleinen Personengruppe (grundsätzlich von den Administratoren) durchgeführt werden. Die Administratoren, die diese Aufgabe übernehmen, werden von einer unabhängigen Vertrauensperson (beispielsweise vom Datenschutzberater) kontrolliert.

Für Software, die Logfiles generiert, verlangt der Transparenzgrundsatz, dass die betroffenen Personen unmissverständlich auf die Existenz der Logfiles hingewiesen werden. Zur Beachtung des Verhältnismässigkeitsgrundsatzes sollte die Erzeugung solcher Logfiles eine Option der Software darstellen, die standardmässig deaktiviert ist. Die Software muss in jedem Fall die Löschung der protokollierten Daten ermöglichen.

Für weitere Einzelheiten siehe die Veröffentlichung des Eidgenössischen Datenschutzbeauftragten, «Elektronische Spuren und Datenschutz» (http://www.edsb.ch/d/themen/sicherheit/technik/elektronische_spuren_d.pdf) .

2.1.4 Schutz des eigenen Computers

Der Einsatz des Computers für elektronische Post, E-Commerce und E-Banking oder für die Informationssuche ist heute aus dem Alltag nicht mehr wegzudenken. Die meisten Benutzer, die sich ins Internet begeben, sind sich jedoch nicht bewusst, dass dieser Vorgang die Sicherheit ihrer Installation und ihrer Daten gefährden kann. Das Risikopotenzial zu erkennen bedeutet den ersten Schritt hin zum Selbstschutz, der im Regelfall mit Gratis-Softwareprogrammen gewährleistet werden kann.

Die erste Risikokategorie besteht aus den *elektronischen Spuren***.** Auf dem Computer durchgeführte Tätigkeiten hinterlassen Spuren. Wenn sie richtig analysiert werden, lässt sich damit das Handeln des Benutzers rekonstruieren. So können besuchte Internetseiten, Mailausgang, Maileingang sowie eine Vielzahl von Personendaten enthüllt werden, aus denen sich unter Umständen sogar Persönlichkeitsprofile erstellen lassen. Der Angriff auf diese Daten setzt nicht zwangsläufig den physischen Zugriff auf den Computer voraus, da die Spuren auch über Internet gesammelt werden können.

Die zweite Risikokategorie betrifft die *Eingriffe in die Sicherheit*. Ziel solcher Angriffe ist der Diebstahl, das Einschleusen, Ändern oder Zerstören von Daten sowie die Lähmung des Computers. Der typische Fall ist der eines Virus oder einer Internetseite, die Dutzende von Werbefenstern öffnet. Zu dieser Kategorie gehören auch unaufgefordert erhaltene E-Mails (Spam), mit denen der elektronische Briefkasten so überlastet wird, dass er manchmal unbenutzbar ist.

Schliesslich gibt es die Kategorie der *wirtschaftlichen Risiken*. Dazu gehört beispielsweise so genannte Malware (Hijacker), welche die Nummer des gewohnten Internetproviders ohne Wissen des Betroffenen durch eine teurere Mehrwertnummer (090x) ersetzt.

Zur Minimierung der Risiken kann man sich oft kostenlose Schutzprogramme beschaffen:

- *Antivirus*: Die Wahrscheinlichkeit einer Infektion mit einem Virus ist hoch, insbesondere beim Herunterladen von Programmen. Eine gute und regelmässig aktualisierte Antiviren-Software stellt einen unabdingbaren Schutz dar.
- *Trace Eraser*: Nach der Benutzung eines Computers bleiben gewisse elektronische Spuren zurück. Die Beseitigung dieser Spuren ist manchmal sehr kompliziert, weshalb die Verwendung von Ad-hoc-Programmen empfehlenswert ist.

- *Cookie-Manager*: Cookies sind Spuren, die nützlich sein können, jedoch auch für den Datendiebstahl missbraucht werden können. Ein guter Cookie-Manager ermöglicht dem Benutzer eine wirksame Cookie-Verwaltung.
- *Antispyware*: Eine Spyware ist ein Programm, das ohne Wissen des Betroffenen persönliche Daten für einen Dritten sammelt. Mit einer regelmässig aktualisierten Antispyware können solche Angriffe abgewehrt werden.
- *File Wiper*: Anstelle des logischen Löschens können die persönlichen Daten mithilfe eines physischen Löschprogramms (File Wiper) vernichtet werden.
- *Persönliche Firewall*: Während einer Internetverbindung kann ein Angreifer versuchen, in Ihren Computer einzudringen. Ausserdem können ohne Ihr Wissen unkontrollierbare aktive Elemente einer Internetseite (Java, Javascript, ActiveX etc.) ausgeführt werden. Eine persönliche Firewall schränkt solche Angriffe ein.
- *Antispam*: Unaufgeforderte E-Mails (Spam) verstopfen den elektronischen Briefkasten mit Werbung. Mit den Antispam-Programmen kann diese Belästigung dank «intelligenter» Filterung der eingehenden Nachrichten grösstenteils verhindert werden.
- *Antidialer*: Ein solches Programm verhindert die unerwünschte Ersetzung der Nummer des gewohnten Internetanbieters durch die Nummer eines kostspieligeren Mehrwertdienstes. Der Entscheid des Bundesamtes für Kommunikation, die Verwendung der PC-Dialer im Zusammenhang mit den 090x-Nummern zu verbieten, stellt ein gutes Mittel gegen diese Probleme dar. Trotzdem kann es zum Beispiel im Zusammenhang mit Satellitennummern noch PC-Dialer geben, weshalb ein Antidialer-Progamm immer empfehlenswert ist.
- *Antibanner*: Gewisse Internetseiten öffnen Dutzende von Werbefenstern, welche die Benutzer erheblich stören. Ein Antibanner-Programm verringert diese Unannehmlichkeiten.

2.1.5 Die Notwendigkeit der Chiffrierung der Daten auf den Festplatten (bzw. Datenträgern) insbesondere im sensitiven Umfeld

Wenn Ärzte oder andere Berufsgruppen, die sensitive Personendaten bearbeiten, ihren Computer mit den Kundendaten beispielsweise zur Reparatur geben müssen, so ist der Computertechniker in der Lage diese Daten einzusehen bzw. zu bear-beiten. Sind die Daten in chiffrierter Form gespeichert, so wird es für den Compu-tertechniker praktisch unmöglich sein, auf diese Daten zuzugreifen.

Immer wieder erreichen uns Anfragen, wie vorzugehen sei, wenn Personalcomputer oder Festplatten repariert werden müssen, damit die Daten nicht von anderen Personen, wie beispielsweise von Computertechnikern, eingesehen werden können. Insbesondere Ärzte, Notare oder Anwälte haben sehr sensitive Kundendaten. Aber auch private Personalcomputerbenutzer haben auf ihren eigenen Systemen Informationen gespeichert, die einen Service- oder Computertechniker oder andere Drittpersonen nichts angehen. Denken wir beispielsweise an Daten der Steuererklärung oder andere persönliche Notierungen. Sensitive Personendaten wie besonders schützenswerte Personendaten oder Persönlichkeitsprofile dürfen gemäss den gesetzlichen Vorgaben nur bearbeitet werden, wenn bei den Sicherheitsmassnahmen der Stand der Technik umgesetzt ist. Dies bedeutet unter anderem, dass solche Daten auf den Festplatten nur in chiffrierter Form gespeichert werden dürfen. Insbesondere im Umfeld von kleineren EDV-Systemen ist der Einsatz von Verschlüsselungsverfahren problemlos möglich. Muss man eine Festplatte reparieren lassen oder wird das Gerät gestohlen, so werden Unbefugte, die nicht im Besitz des Passwortes oder Passphrase und/oder der Chipkarte sind, welche eine Entschlüsselung der gespeicherten Daten ermöglichen würden, nicht in der Lage sein, auf diese Daten zuzugreifen.

In vielen Fällen ist es auch so, dass EDV-Systeme oder Teile davon nach einer gewissen Zeitdauer verkauft werden. In einem solchen Fall muss man die gespeicherten Daten löschen, so dass diese nicht mehr rekonstruiert werden können. In vielen Fällen bieten die standardmässigen Löschprogramme nur eine logische Datenlöschung an, so dass die Daten, sofern diese nicht überschrieben wurden, ohne grössere Mühe rekonstruiert werden können. Sofern die sensitiven Daten in chiffrierter Form gespeichert wurden und man diese physisch gelöscht hat, ist es nicht mehr zwingend notwendig, die gelöschten Daten durch mehrere Bitmuster mehrfach zu überschreiben, weil ja neben der Löschung auch noch die Chiffrierung der Daten eine Rekonstruktion der Informationen erschwert. Ganz sicher kann man aber erst sein, wenn man die Festplatte bzw. den Datenspeicher oder Datenträger physikalisch so zerstört, dass eine Rekonstruktion der Daten nicht mehr möglich ist.

2.1.6 Protokollierung der Aktivitäten in produktiven Systemen

Protokollierungen sind in denjenigen Bereichen vorzunehmen, in denen man den Datenschutz oder die Datensicherheit nicht durch präventive Massnahmen gewährleisten kann. Ein solcher Bereich ist beispielsweise der Zugriff auf EDV-Systeme durch interne oder externe Mitarbeiter, die hohe Systemprivilegien besitzen, wie beispielsweise Systemverantwortliche, Datenbankadministratoren, Superuser, usw.

Protokollierungen sind insbesondere in den Bereichen einzusetzen, in denen mit präventiven Massnahmen (beispielsweise durch den Einsatz von Chiffrierverfahren) die notwendigen Si-cherheitsvorkehrungen nicht umgesetzt werden können. Mit Hilfe der Protokollierung kann man allerdings nur festhalten, was bereits geschehen ist. Eine mögliche Datenschutzverletzung wäre, sofern man diese aufgrund des Protokolleintrags feststellt, bereits eingetreten. Protokollierungen haben aber dennoch eine präventive Wirkung, weil die Systembenutzer oder -betreiber wissen, dass gewisse Aktivitäten protokolliert werden. Allen Betroffenen ist möglichst transparent mitzuteilen, was warum protokolliert wird. Je nach System können verschiedenen Protokollierungen notwendig sein. Ein wichtiger Grundsatz ist aber der, dass nur das Notwendige protokolliert werden soll, so dass nicht riesige Mengen von Protokolldaten anfallen, die man gar nicht mehr auswerten kann. Im Weiteren ist es sinnvoll, dass man die Protokolle so gestaltet bzw. festhält, dass diese möglichst nur in anonymisierter oder pseudonymisierter Form vorliegen. Im Normalfall muss bei einer Protokollauswertung nicht auf den einzelnen Benutzer geschlossen werden können. Die Auswertung soll möglichst anonym erfolgen, so dass nur auf Organisationseinheiten, wie beispielsweise Ämter, Abteilungen, Sektionen geschlossen werden kann. Grundsätzlich ist es wichtig, dass man bei der Systemplanung bzw. -entwicklung mit Hilfe von präventiven Massnahmen das System so zu gestalten versucht, dass für den jeweiligen Benutzer nur ein datenschutzkonformes Arbeiten möglich ist, so dass nur noch einige wenige «offene» Bereiche durch Protokollierungsmassnah-men abgedeckt werden müssen. Ein solch «offener» Bereich ist der Zugriff auf produktive EDV-Systeme durch eigene oder externe Mitarbeiter, die hohe Systemprivilegien besitzen, wie beispielsweise Systemverantwortliche, Datenbankadministratoren, Superuser, usw., sofern für diese die Daten frei zugänglich, also nicht logisch oder physisch abgeschottet sind. In diesem Umfeld besteht ein erhöhtes Risiko, weil auf alle gespeicherten Daten zugegriffen werden kann. Die Protokolldaten sind revisionssicher festzuhalten. Dies bedeutet insbesondere, dass diese Dateien so zu gestalten sind, dass sie nachträglich weder manipuliert noch unkontrolliert gelöscht werden können. Im Weiteren gilt es zu beachten, dass die Protokolldaten nur eine gewisse Zeit lang aufbewahrt werden dürfen.

2.2 Weitere Themen

2.2.1 Medizinisch-psychologischer Fragebogen bei der Rekrutierung von Stellungspflichtigen

Die Stellungspflichtigen müssen bei ihrer Rekrutierung einen medizinisch-psychologischen Fragebogen ausfüllen, der dazu dient, ihre Diensttauglichkeit festzustellen. Viel zu reden gaben dabei vor allem die Fragen zur Sexualität. Nicht nur diese, sondern auch die meisten übrigen Fragen greifen in die Privat- und Intimsphäre der Stellungspflichtigen ein. Die Antworten sind daher besonders schützenswerte Personendaten oder stellen Persönlichkeitsprofile dar. Eine Bearbeitung von derart sensiblen Personendaten durch eine Behörde ist nur unter Einhaltung bestimmter Voraussetzungen zulässig. Den Grundsatzentscheid, ob solche Eignungstests überhaupt eingesetzt werden dürfen, muss das Parlament fällen.

Seit kurzem müssen die Stellungspflichtigen bei den Rekrutierungen einen umfangreichen Fragebogen ausfüllen. Laut einer Stellungnahme des VBS im Internet soll der Fragebogen dazu dienen, neben der medizinischen auch die psychische Diensttauglichkeit der Stellungspflichtigen zu beurteilen. Der Fragebogen enthielt gemäss VBS «rund 400 Fragen». Darunter auch sechs Fragen zur Sexualität, «weil diese ein Grundverhalten des Menschen darstellt und auch Verhaltensweisen umfasst, welche Auswirkungen auf die psychische Gesundheit haben können». Die Stellungspflichtigen mussten alle Fragen zwingend beantworten.

Insbesondere die Fragen zur Sexualität wurden oft und kritisch in den Medien diskutiert. Bei uns sind sehr viele Anfragen von besorgten und verunsicherten Betroffenen und deren Angehörigen eingegangen. Wir haben umgehend mit den verantwortlichen Stellen im VBS Kontakt aufgenommen und zusätzliche Informationen verlangt.

Aufgrund der Medienberichte und Aussagen von Stellungspflichtigen, die sich direkt an uns gewandt haben, haben wir Folgendes festgestellt:

Antworten zu den die Sexualität betreffenden Fragen stellen besonders schützenswerte Personendaten dar.

Auch zahlreiche der übrigen «rund» 394 Fragen betreffen besonders schützenswerte Personendaten (z.B. Fragen zur Gesundheit, zu Massnahmen der sozialen Hilfe, zu administrativen oder strafrechtlichen Verfolgungen und Sanktionen). (Diesem Umstand ist in der öffentlichen Diskussion erstaunlicherweise wenig Beachtung geschenkt worden.)

Die Antworten erlauben es, wesentliche Aspekte der Persönlichkeit der Stellungspflichtigen zu beurteilen. Damit liegt ein Persönlichkeitsprofil im Sinne des DSG vor.

Aufgrund ihres sensiblen Gehalts reichen bereits wenige Antworten aus, um ein Persönlichkeitsprofil zu erstellen.

Bedenklich ist die Tatsache, dass die oder der Stellungspflichtige Fragen zu Drittpersonen wie Eltern, Grosseltern und Geschwistern beantworten muss. Dies ist grundsätzlich nur zulässig, wenn die Einwilligung der Betroffenen vorliegt.

An einer Sitzung mit den zuständigen Stellen des VBS nahmen wir die Gelegenheit wahr, die Haltung des Datenschutzbeauftragten in dieser Angelegenheit ausführlich und klar darzulegen:

Ein von einer staatlichen Behörde angeordneter, medizinisch-psychologischer Eignungstest greift in die Privat- und Intimsphäre des einzelnen Bürgers ein.

Dem Entscheid, ob eine Behörde derartige Eignungstests einsetzen darf, muss stets ein gesellschaftlicher und politischer Diskurs vorausgehen. Einzig das Parlament ist legitimiert, im ordentlichen Gesetzgebungsverfahren über die Notwendigkeit und die Zweckmässigkeit solcher Eignungstests zu entscheiden.

Die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen muss ausdrücklich in einem Bundesgesetz vorgesehen sein.

Die Grundzüge der Datenbearbeitung müssen im Bundesgesetz aufgeführt sein. Es sind dies:

- die Definition des Bearbeitungszwecks;
- die Umschreibung des Umfangs der Datenbearbeitung in groben Zügen (muss für die betroffenen Personen nachvollziehbar sein);
- das Festhalten der Beteiligten an der Datenbearbeitung (Datenbearbeiter; Datenempfänger);
- das Aufführen der Kategorien der bearbeiteten Daten (sofern besonders schützenswerte Personendaten oder Persönlichkeitsprofile betroffen sind).

Erst nach Vorliegen der genügenden gesetzlichen Grundlagen kann eine Verwaltungsbehörde solche Eignungstests ausarbeiten und zum Einsatz bringen.

Wie bei jeder Datenbearbeitung müssen auch hier in jeder Phase die allgemeinen Datenschutzgrundsätze strikte eingehalten werden (Verhältnismässigkeit der Fragestellung, Transparenz bei der Datenbearbeitung, Zweckbindung usw.).

In Anbetracht der sensiblen Personendaten ist vor allem dem Transparenzprinzip besondere Beachtung zu schenken. Die Stellungspflichtigen müssen genau darüber informiert werden, welche Zwecke mit dem Fragebogen verfolgt werden, wer auf die Antworten Zugriff hat, wie lange die Daten aufbewahrt werden, ob die Antworten an Dritte weitergegeben werden usw.

2.2.2 Veröffentlichung von Fotos und Namen bei elektronischen Zugangssystemen

Elektronische Zugangs- und Kontrollsysteme, wie sie etwa in Skigebieten oder sonstigen Sportanlagen eingesetzt werden, dürfen keine Daten wie Name oder Geburtsdatum auf einem allgemein ersichtlichen Monitor anzeigen. Wenn keine andere Kontrollmöglichkeit besteht, darf ausnahmsweise zur Überprüfung das Foto des rechtmässigen Inhabers eines Tickets angezeigt werden, allerdings nur in unmittelbarer Nähe des Kontrollpunktes.

Skifahrerinnen und Skifahrer sehen sich vermehrt mit modernen Ticketing- und Zutrittskontrollsystemen konfrontiert, bei denen auch Personendaten bearbeitet werden. Beim Kauf von (vor allem länger gültigen) Tickets wird neben den üblichen persönlichen Daten das Foto des Kunden digital gespeichert. Der Zweck ist, kontrollieren zu können, ob die persönlichen Tickets tatsächlich nur vom Inhaber und nicht von einer andern Person benutzt werden.

In verschiedenen Skigebieten sind die Personendaten auch für das Publikum im Bereich des Zutrittskontrollsystems sichtbar. Wenn der Kunde das Drehkreuz passiert, erscheint auf einem grossen Monitor sein Bild beziehungsweise das Bild des rechtmässigen Karteninhabers. Zusätzlich können weitere Daten wie Name, Vorname oder Geburtsdatum eingeblendet sein. Beabsichtigt wird dadurch, dass der Missbrauch abnimmt, insbesondere dass persönliche Karten nicht von andern Personen verwendet werden. Das System ermöglicht somit eine Art gegenseitige Kontrolle unter den Skifahrern. Uns wurde von Fällen berichtet, bei denen die Anzeige während einer Zeit von mehreren Minuten erfolgte.

Beim Einsatz derartiger Systeme ist immer der Verhältnismässigkeitsgrundsatz zu berücksichtigen. Der Eingriff in die Persönlichkeit der betroffenen Personen darf nur so tief sein, wie es nötig ist, um den Missbrauch einzudämmen. Andere Kontrollverfahren, die eine zurückhaltendere Datenbearbeitung beinhalten, insbesondere weniger Daten Dritten zugänglich machen, sind vorzuziehen. Dabei ist etwa an das stichprobenweise Überprüfen der Tickets durch das Personal zu denken. Wird ein System mit abgelegten Bildern der Kunden verwendet, ist eine Lösung zu finden, bei der der Kontrollmonitor in einem Raum vom Personal überprüft wird und nicht von Dritten einsehbar ist.

Wenn die konkreten Umstände keine andere Kontrollmöglichkeit erlauben, ist das kurzzeitige (wenige Sekunden) Aufschalten des Bildes und allenfalls einer nichtsprechenden Ticketnummer des rechtmässigen Inhabers des Tickets im öffentlichen Zutrittsbereich akzeptabel. Allerdings darf der Monitor nur in unmittelbarer Nähe des Kontrollpunktes und nicht für eine ganze Warteschlange einsehbar sein. Das zusätzliche öffentlich ersichtliche Einblenden von Name, Vorname und Geburtsdatum oder weiteren Daten ist jedoch unverhältnismässig.

In jedem Fall sind die Kunden bei der Erhebung der Personendaten unmissverständlich über die Datenbearbeitung und deren Zweck aufzuklären.

3. Justiz/Polizei/Sicherheit

3.1 Polizeiwesen

3.1.1 Gesichtserkennung in Stadien

Der Einsatz eines Gesichtserkennungssystems stellt eine Bearbeitung von Personendaten dar. Werden die Daten durch private Personen bearbeitet, brauchen diese dafür einen Rechtfertigungsgrund und müssen die allgemeinen datenschutzrechtlichen Grundsätze beachten. In allen Fällen drängt sich eine klare Information der betroffenen Personen auf, um diese auf das Gesichtserkennungssystem sowie auf die Möglichkeit der Ausübung des Auskunftsrechts hinzuweisen. Zudem stellt sich das Problem der Koordination sowie der Kompetenz- und Aufgabenteilung zwischen privaten Organen einerseits, die für bestimmte Sicherheitsmassnahmen zuständig sind, sowie Polizeiorganen andererseits, die für die Wahrung der öffentlichen Sicherheit zuständig sind. Vor dem Einsatz eines Gesichtserkennungssystems sind alle weiteren Details klar zu regeln.

Wir wurden angefragt, ob es sinnvoll wäre, in Stadien ein Gesichtserkennungssystem einzusetzen. Da noch keine konkreten Angaben vorlagen, konnten wir uns zu dieser Frage datenschutzrechtlich nur sehr allgemein äussern.

Zunächst ist diesbezüglich auf unser Merkblatt über die Videoüberwachung durch private Personen (vgl. unseren 8. Tätigkeitsbericht, Abschnitt 3.1 und Anhang 3) hinzuweisen. Allerdings stellen sich beim Einsatz eines Gesichterkennungssystems weitergehendere Fragen. Zudem darf nicht vergessen werden, dass das Gesichtserkennungssystem zur Zeit immer noch eine hohe Fehlerquote aufweist. Dies würde dazu führen, dass das System zum Teil auch völlig unbehelligte (d.h. nicht in der Datenbank aufgeführte) Zuschauer irrtümlicherweise als registrierte gewalttätige Personen identifizieren würde. Für die betroffenen Personen würde dies einen unzulässigen Eingriff in ihre Persönlichkeit bedeuten, zudem wäre damit der Grundsatz der Richtigkeit der Personendaten verletzt. Diese Aspekte dürfen vor der Einführung eines Gesichtserkennungssystems sicher nicht vernachlässigt werden.

Das Gesichtserkennungssystem stellt, gleich wie die Videoüberwachung von Zuschauern, eine Bearbeitung von Personendaten dar. Folglich ist dabei das DSG zu beachten. Auf Bundesebene gibt es das DSG, das anwendbar ist, wenn Bundesorgane und/oder private Personen Daten bearbeiten. Bearbeiten Bundesorgane Personendaten, braucht es dafür zudem eine Rechtsgrundlage. Desgleichen braucht es gemäss

den kantonalen Datenschutzgesetzen eine gesetzliche Grundlage, wenn kantonale Organe Daten bearbeiten.

Bei der vorliegenden Anfrage war davon auszugehen, dass die Daten von privaten Personen (worunter auch Vereine fallen) bearbeitet werden sollten. Damit private Personen Personendaten bearbeiten dürfen, brauchen sie dafür einen Rechtfertigungsgrund, nämlich die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder ein Gesetz. Zudem müssen die allgemeinen Grundsätze des DSG (insbesondere Rechtmässigkeitsprinzip, Prinzip von Treu und Glauben, Verhältnismässigkeitsprinzip, Zweckbindungsprinzip, Richtigkeit der Daten, Prinzip der Datensicherheit sowie Auskunftsrecht) eingehalten werden. So dürfen die Daten nur rechtmässig beschafft werden, und gemäss dem Prinzip der Verhältnismässigkeit dürfen nur diejenigen Daten bearbeitet werden, die für den verfolgten Zweck auch nötig und geeignet sind. Ob diese Voraussetzungen gegeben sind, ist jeweils im Einzelfall zu prüfen.

Betreffend die Rechtfertigungsgründe kommen insbesondere das überwiegende öffentliche Interesse im Rahmen von Sicherheitsmassnahmen sowie die Einwilligung der betroffenen Personen in Frage. In allen Fällen drängt sich eine klare Information – sei es auf der Eintrittskarte oder anderswo – der betroffenen Personen auf, um diese auf den Einsatz eines Gesichtserkennungssystems sowie auf die Möglichkeit der Ausübung des Auskunftsrechts hinzuweisen.

Zudem stellt sich das Problem der Koordination sowie der Kompetenz- und Aufgabenteilung zwischen privaten Organen (der Heimclubs und/oder allenfalls der FIFA) einerseits, die für bestimmte Sicherheitsmassnahmen zuständig sind, sowie Polizeiorganen andererseits, die für die Wahrung der öffentlichen Sicherheit zuständig sind. Je nach gewählter Variante müssten allenfalls noch gesetzliche Grundlagen geschaffen werden. Zum Ganzen ist darauf hinzuweisen, dass zur Zeit auf Bundesebene der Entwurf zu einem Bundesgesetz über Massnahmen gegen Rassismus und Hooliganismus besteht (das erwähnte Bundesgesetz soll in das bereits bestehende Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit integriert werden). Dieser Gesetzesentwurf sieht zwar keinen Einsatz eines Gesichtserkennungssystems vor, dafür aber die Einführung einer «Hooliganismusdatenbank».

Schliesslich müssten vor Einsatz eines Gesichtserkennungssystems die weiteren Details klar festgelegt werden. Insbesondere müsste geregelt werden, unter welchen Voraussetzungen eine Person in die Datenbank aufgenommen wird, welche Daten unter welchen Bedingungen an wen (Polizeibehörde, andere Fussballclubs, usw.) bekannt gegeben werden, wo und wie lange die Daten aufbewahrt werden, resp. wann sie gelöscht werden, wer Zugriff auf diese Personendaten hat, wer für die Behandlung

von Auskunftsgesuchen zuständig ist, wie die betroffenen Personen (insbesondere die Zuschauer) über den Einsatz eines solchen Systems informiert werden, usw. Bei der Festlegung dieser Bedingungen sind die oben erwähnten allgemeinen Grundsätze des DSG zu beachten, darunter auch das Verhältnismässigkeitsprinzip. Am besten wäre es, diese Einzelheiten in einem Bearbeitungsreglement festzuhalten (resp. in einem Gesetz, falls die Daten von einem Bundes- oder kantonalen Organ) bearbeitet werden.

3.2 Weitere Themen

3.2.1 Videoüberwachungsverordnung SBB

Die Verordnung über die Videoüberwachung durch die Schweizerischen Bundesbahnen (SBB) vom 5. Dezember 2003 ist am 1. Januar 2004 in Kraft getreten. Die Verordnung bildet die vom DSG verlangte gesetzliche Grundlage für Bearbeitungen von Personendaten im Rahmen der Videoüberwachungstätigkeiten in den Bahnhofanlagen und Zügen der SBB. Unsere Bemerkungen zum Schutz der Privatsphäre – besonders diejenigen zur Information der betroffenen Personen, zum Zugriff auf die Daten und zur Aufbewahrungsfrist – sind bei der Ausarbeitung der Verordnung berücksichtigt worden. Wir hatten bereits bei der versuchsweisen Installation von Videoüberwachungssystemen in Nahverkehrszügen (siehe unseren 8. Tätigkeitsbericht 2000/2001, Abschnitt II.3.2) sowie nach unseren Kontrollen der Videoüberwachungstätigkeiten der SBB im Hauptbahnhof Zürich (siehe unseren 9. Tätigkeitsbericht 2001/2002, Abschnitt 3.2.2 und unseren 10. Tätigkeitsbericht 2002/2003, Abschnitt 3.2.3) gefordert, dass eine entsprechende Vorschrift ausgearbeitet werden solle.

3.2.2 Zivilprozessordnung und Datenschutzgesetz

Im Rahmen der Ämterkonsultation zum Expertenentwurf für eine einheitliche schweizerische Zivilprozessordnung nahmen wir insbesondere zu den geplanten Änderungen von Art. 15 DSG betreffend die Rechtsansprüche Stellung. Dabei geht es uns unter anderem darum, dass im DSG selbst weiterhin auf bestimmte Rechte verwiesen wird.

Im Rahmen der Ämterkonsultation konnten wir zum Expertenentwurf für eine einheitliche schweizerische Zivilprozessordnung (CH-ZPO) Stellung nehmen. Der Expertenentwurf der CH-ZPO sieht unter anderem eine Änderung von Art. 15 DSG, der die Rechtsansprüche regelt, vor. Wir wiesen in unserer Stellungnahme zunächst darauf hin, dass sich das DSG zur Zeit in Revision befindet, wobei auch Art. 15 DSG von einer

kleinen Änderung betroffen sei. Daher sei sicherzustellen, dass beim Expertenentwurf CH-ZPO vom Revisionsentwurf des DSG ausgegangen würde.

Wir regten an, auf die im Expertenentwurf CH-ZPO geplanten Änderungen betreffend Art. 15 Abs. 1 DSG zu verzichten. So solle weiterhin auf das Recht auf Gegendarstellung (Art. 28 – 28l ZGB), das ein wichtiges Instrument des Persönlichkeitsrechts darstelle, verwiesen werden. Zudem sei es wichtig, wie bis anhin, im DSG selbst ausdrücklich auf das Recht, die Sperrung, Berichtigung und Vernichtung von Daten zu verlangen, hinzuweisen. Desgleichen sei im DSG selbst (Art. 15 Abs. 4 DSG) weiterhin explizit festzuhalten, dass für Klagen zur Durchsetzung des Auskunftsrechts ein einfaches und rasches Verfahren gelte. Damit bleibe das DSG für den Laien leserlich und verständlich.

Weiter verlangten wir, in Art. 15 Abs. 3 DSG ausdrücklich auf die Möglichkeit, die Sperre der Bekanntgabe von Daten an Dritte verlangen zu können, hinzuweisen, wie dies der Revisionsentwurf des DSG vorsehe.

4. IT und Telekommunikation

4.1 Webcams datenschutzkonform betreiben

Webcams im Internet existieren seit Jahren und führen immer wieder zur Frage, ob sie datenschutzkonform sind. Kurz zusammengefasst gibt es zwei Möglichkeiten des legalen Einsatzes: Entweder sind die Kameras so positioniert bzw. konfiguriert, dass keine Personen erkennbar sind, oder die betroffenen Personen willigen ein, aufgenommen zu werden.

Die Webcam-Bilder sind weltweit per Internet abrufbar und können unkontrolliert weiterverarbeitet (speichern, ausdrucken, weitergeben etc.) werden. Sie sind je nach System von unterschiedlicher Qualität: einige Kameras sind fest montiert und erlauben es dem Betrachter nicht einen eigenen Bildausschnitt zu wählen. Andere Kameras bieten dem Benutzer die Möglichkeit, in verschiedene Positionen gebracht zu werden und/oder einen Bildausschnitt vergrössert darzustellen. Je nach Technik und Positionierung des Kamerasystems ist es möglich, Personen auf den Kamerabildern zu erkennen. Die Kameras werden von den erfassten Personen oft nicht wahrgenommen. Diese haben somit keine Kenntnis davon, dass – und zu welchem Zweck – ihr Bild im Internet weltweit abrufbar ist. Enthalten die abrufbaren Bilder keine Angaben über bestimmte oder bestimmbare Personen, sind keinerlei datenschutzrechtliche Bedenken einzuwenden. Falls es jedoch möglich ist, Personen zu bestimmen, liegt ein Bearbeiten von Personendaten im Sinne des DSG vor. Bestimmbar ist eine Person auch dann, wenn sie zwar durch ihre Daten nicht eindeutig identifiziert wird, aus den Umständen, das heisst aus dem Kontext einer Information (z.B. Gegenstände, Kleidung, Fahrzeuge etc.) aber auf sie geschlossen werden kann.

Wer Personendaten bearbeitet, hat namentlich folgende Bearbeitungsgrundsätze des DSG zu beachten: Personendaten dürfen nur rechtmässig beschafft werden. Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein Datenschutz fehlt, der dem schweizerischen gleichwertig ist.

Private Personen, die Personendaten bearbeiten, dürfen die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzten. Eine Persönlichkeitsverletzung bei der Bearbeitung durch private Personen ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch ein Gesetz gerechtfertigt ist. Die Betreiber von Webcams können kein

überwiegendes privates Interesse geltend machen. Auch ein öffentliches Interesse oder eine gesetzliche Rechtfertigung zum Betrieb von Webcams existiert nicht. Somit können Personendaten via Webcams nur nach Einwilligung der betroffenen Personen bekannt gegeben werden. Die Einwilligung muss frei und in Kenntnis aller Umstände erfolgen. Hat die betroffene Person irgendwelche Nachteile zu gewärtigen, wenn sie sich nicht von der Kamera erfassen lassen will, ist die Einwilligung nicht gültig. Eine Einwilligung ist oftmals (z.B. Webcams auf öffentlichen Strassen) nicht praktikabel. In diesen Fällen ist mit technischen und organisatorischen Massnahmen sicherzustellen, dass die erfassten Personen nicht bestimmbar sind.

Daraus ergeben sich folgende Möglichkeiten für den datenschutzkonformen Einsatz von Webcams in öffentlich zugänglichen Bereichen:

- Die Webcam ist so konfiguriert, dass keine Personen (bzw. Gegenstände, durch welche Personen bestimmt werden können) erkannt werden.
- Falls eine Bestimmbarkeit möglich ist, muss die Person, die von der Kamera aufgenommen werden soll, zustimmen. Der Wille, nicht gefilmt zu werden, muss jederzeit respektiert werden können. Zudem muss eine Einwilligung frei von irgendwelchen Bedingungen verbunden mit einer verständlichen Information erfolgen, bevor der Aufnahmebereich der Kamera betreten wird.

Wir haben mehrere Betreiber von Webcam-Systemen in der Schweiz aufgefordert, die Datenschutzkonformität zu überprüfen und wo nötig anzupassen. Aus Kapazitätsgründen ist es uns nicht möglich, die Webcams systematisch zu kontrollieren. Die betroffenen Personen können im Falle einer Persönlichkeitsverletzung Zivilklage einreichen.

5. Gesundheit

5.1 Videoaufnahmen von Patientinnen und Patienten zu Supervisions- und Weiterbildungszwecken

Die Bearbeitung von Personendaten durch Privatkliniken untersteht dem DSG. Videoaufnahmen von Patientinnen und Patienten beinhalten besonders schützenswerte Personendaten und sind als Persönlichkeitsprofil zu betrachten. Die Bearbeitung solcher Daten für Supervisions- und Schulungszwecke lässt sich nur schwer rechtfertigen. Wird sie zugelassen, so muss das Vorgehen verbindlich geregelt werden. Der Patient muss seine Einwilligung zur Aufnahme und Verwendung der Videobänder schriftlich erteilen. Die Verantwortung für den Datenschutz trägt die Klinik, welche die Videobänder herstellt und einsetzt.

Eine psychiatrische Privatklinik möchte Videoaufnahmen von Patienten zu Supervisions- und Weiterbildungszwecken verwenden. Die Aufnahme, Verwendung, Aufbewahrung und Weitergabe solcher Aufnahmen regelt sie in einem entsprechenden Reglement. Als Orientierungshilfe für die Erstellung des Reglements haben wir der Klinik die nachfolgenden Erwägungen zukommen lassen.

Die Bearbeitung von Personendaten durch Privatkliniken untersteht dem DSG. Videoaufnahmen von Patienten stellen eine Datenbearbeitung im Sinne des DSG dar. Sie beinhalten einerseits besonders schützenswerte Personendaten (Gesundheitsdaten) und stellen anderseits ein Persönlichkeitsprofil dar, d.h. sie ermöglichen die Beurteilung wesentlicher Aspekte der Persönlichkeit. Die Klinik muss, wie bei jeder Datenbearbeitung, die allgemeinen Grundsätze des DSG einhalten und einen Rechtfertigungsgrund (Einwilligung, überwiegendes Interesse oder Gesetz) nachweisen können.

Die Verantwortung für die Umsetzung der Datenbearbeitungsgrundsätze des DSG trägt immer der Datenbearbeiter, im vorliegenden Fall also die Klinik. Sie muss alle Risiken der vorgesehenen Datenbearbeitung abschätzen und die notwendigen Interessenabwägungen vornehmen.

Zentrale Grundsätze des DSG sind das Verhältnismässigkeitsprinzip und das Zweckbindungsprinzip. Sie müssen bei jeder Datenbearbeitung eingehalten werden. Die Verhältnismässigkeit ist dann gegeben, wenn die Bearbeitung für den vorgesehenen Zweck geeignet und erforderlich ist und der verfolgte Zweck nicht durch eine andere, weniger in das Persönlichkeitsrecht des Betroffenen eingreifende Datenbearbeitung erreicht werden kann. Die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen greift stark in das Persönlichkeitsrecht des Betroffenen ein. Für Supervisions- und Schulungszwecke lässt sich ein solcher Eingriff kaum

rechtfertigen. Er darf daher, wenn überhaupt, nur in begrenztem Rahmen und unter klar festgelegten Bedingungen zugelassen werden. Zu bedenken ist, dass die Patienten zu einem ganz anderen Zweck in der Klinik weilen, nämlich zur Wiedererlangung ihrer Gesundheit. Supervision und Schulung verfolgen hingegen andere Ziele, nämlich die individuelle Beratung im konkreten beruflichen Kontext einer Berufsperson (z.B. Therapeut) bzw. die berufliche Aus- und Weiterbildung.

Es ist Aufgabe der Klinik, die Verhältnismässigkeit beim Einsatz von Videoaufnahmen zu beurteilen. Dabei ist für jeden vorgesehenen Zweck eine separate Beurteilung erforderlich.

Das Verhältnismässigkeitsprinzip verlangt, dass überall dort, wo ein Personenbezug nicht unbedingt notwendig ist, eine konsequente Anonymisierung oder mindestens eine Pseudonymisierung der Personendaten vorgenommen wird. Anonyme Daten verlieren den Charakter von Personendaten und ihre Bearbeitung unterliegt nicht mehr dem DSG. Eine vollständige Anonymisierung ist allerdings erst gegeben, wenn jeder Bezug zur betroffenen Person ausgeschlossen, diese also überhaupt nicht mehr erkennbar ist. In der Praxis wird oft ein «Balken über den Augen» zur Unkenntlichmachung einer Person verwendet. Damit wird aber nur in den wenigsten Fällen eine genügende Anonymisierung erreicht. Bei Videoaufnahmen muss z.B. darauf geachtet werden, dass die Umgebung neutral ist, die Stimmen verzerrt werden und weder Gesichter noch andere identifizierende Merkmale sichtbar sind. Auch hier fällt die Beurteilung unter Berücksichtigung des Zwecks unterschiedlich aus. Während für die Supervision keine oder nur eine geringe Verschleierung der Identität des Betroffenen allenfalls noch verhältnismässig sein kann, ist bei Aufnahmen, die für Schulungszwecke verwendet werden, ein viel höherer Anonymisierungsgrad notwendig. Fraglich ist jedoch, ob bei Videoaufnahmen im Bereich der Psychiatrie überhaupt eine vollständige Anonymisierung erreicht werden kann. In den aufgenommenen Sitzungsgesprächen werden vermutlich oft Umstände und Vorgänge geschildert, die für den jeweiligen Fall so spezifisch und wichtig sind, dass man sie nicht einfach herausfiltern kann, ohne den Inhalt zu sehr zu entleeren oder zu verzerren.

Ein weiterer Aspekt der Verhältnismässigkeit ist die zeitliche Limite für die Verwendung der Videoaufnahmen. Eine Verwendung auf unbestimmte Zeit ist mit dem Verhältnismässigkeitsprinzip nicht zu vereinbaren, und zwar auch dann nicht, wenn der Patient in eine solche einwilligen sollte. Die Einwilligung in eine unverhältnismässige Datenbearbeitung ist nicht möglich und daher auch nicht rechtsgültig. Wenn der Zweck erfüllt ist (z.B. nach Beendigung der Supervision) ist eine weitere Verwendung oder Aufbewahrung der Bänder nicht mehr gerechtfertigt. Auch die Verwendung zu Schulungszwecken muss zeitlich limitiert sein. Da es um besonders schützenswerte Personendaten und Persönlichkeitsprofile geht, kann es sich dabei nur um einen Zeitraum von wenigen Monaten handeln.

Das Verhältnismässigkeitsprinzip verlangt weiter, dass der Kreis der Personen, die von besonders schützenswerten Personendaten und/oder Persönlichkeitsprofilen Kenntnis erhalten, so klein wie möglich gehalten wird. Bei Videoaufnahmen, die für die Schulung bestimmt sind, kann diese Bedingung notgedrungen nicht erfüllt werden.

Nach Abwägung der Interessenlage muss die Klinik entscheiden, in welchem Rahmen und mit welchen Auflagen sie Videoaufnahmen zulassen will. Angesichts der Sensibilität solcher Aufnahmen, ist ein detailliertes Reglement unerlässlich. Die Klinik trägt als datenbearbeitende Stelle die Verantwortung für den Datenschutz, und sie muss sicherstellen, dass die Aufnahmen verhältnismässig und zweckmässig eingesetzt werden (z.B. nur für fachspezifische Ausbildungen und nur wenn die Aufnahmen für die Ausbildung auch tatsächlich einen zusätzlichen Nutzen bringen).

Als Rechtfertigungsgrund für Videoaufnahmen zu Supervisions- und Schulungszwecken kommt nur die Einwilligung des betroffenen Patienten in Frage. Geht es um die Bearbeitung von besonders schützenswerten Personendaten und/oder Persönlichkeitsprofilen, werden besonders hohe Anforderungen an die Einwilligung gestellt. Je heikler die zu bearbeitenden Daten sind, um so umfassender muss die Information an die betroffene Person sein und um so klarer muss die Einwilligung erfolgen (vgl. unseren 7. Tätigkeitsbericht 1999/2000, Abschnitt 3.1).

Die einwilligende Person muss den Umfang und die Tragweite ihrer Einwilligung abschätzen können. Sie muss in Bezug auf die Aufnahme und die Verwendung solcher Videobänder urteilsfähig sein. Die Einwilligung einer urteilsunfähigen Person ist nicht rechtsgültig. An ihrer Stelle kann jedoch der gesetzliche Vertreter einwilligen.

Aus Gründen der Beweisbarkeit und wegen der Sensibilität der bearbeiteten Daten muss die Einwilligung schriftlich erteilt werden. Für die Rechtsgültigkeit der Einwilligung ist ausschlaggebend, dass die betroffene Person über ihre Rechte und die vorgesehenen Datenbearbeitungen aufgeklärt worden ist. Daher ist es unumgänglich, dem Patienten ein ausführliches Informationsblatt abzugeben, welches die Verwendung vom Zeitpunkt der Aufnahme bis zur Löschung der Bänder detailliert und nachvollziehbar umschreibt.

In der Information an den Patienten muss der Zweck der Videoaufnahme präzis festgehalten sein. Werden mehrere Zwecke verfolgt, so müssen diese einzeln aufgeführt werden. Der Patient muss auch darüber informiert werden, ob und wie die Aufnahmen für die jeweiligen Zwecke anonymisiert werden. Diese Information ist wichtig für den Entscheid des Patienten, ob er in alle oder nur in einzelne der vorgesehenen Zwecke einwilligen will. Sind mehrere Zwecke vorgesehen, muss der Patient eine Wahlmöglichkeit haben. Es ist denkbar, dass jemand einverstanden ist, Aufnahmen für die Supervision zu machen, aber nicht möchte, dass die Aufnahmen auch für Schulungszwecke verwendet werden.

Solange die Aufnahmen im Besitz von Medizinalpersonen verbleiben, sind sie durch das Berufsgeheimnis weitgehend geschützt. Kommen die Aufnahmen aber in den Besitz von anderen Personen, was gestützt auf die entsprechende Einwilligung des Patienten an sich zulässig wäre, stehen sie nicht mehr unter dem Schutz des Berufsgeheimnisses. Darauf muss im Informationsblatt hingewiesen werden. Auch die Vorkehren, welche die Klinik trifft, um die Videobänder und deren Inhalt unter dem Schutz des ärztlichen Berufsgeheimnisses zu behalten, sollten erwähnt sein.

Gemäss DSG kann der Patient jederzeit Auskunft darüber verlangen, welche Daten über ihn bearbeitet werden. Das Auskunftsrecht setzt den Berechtigten in die Lage, weitere ihm zustehende Datenschutzrechte (Berichtigung, Anonymisierung oder Vernichtung von nicht mehr benötigten Daten, im vorliegenden Fall vor allem die Löschung des Videobandes) geltend zu machen. Ein Hinweis auf diese Rechte gehört ebenfalls ins Informationsblatt. Zudem muss der Patient auch darüber informiert werden, an wen er das Auskunftsgesuch richten muss.

Wichtig ist auch ein ausdrücklicher Hinweis auf die Freiwilligkeit der Videoaufnahmen und die Tatsache, dass eine Verweigerung der Einwilligung keine nachteiligen Folgen für den Patienten hat. Eine einmal erteilte Einwilligung kann jederzeit und ohne Angabe von Gründen widerrufen werden. Sollte der Patient seine Einwilligung widerrufen, dürfen die Aufnahmen ab diesem Zeitpunkt nicht mehr verwendet werden. Die Klinik muss die Kontrolle darüber behalten, wo welche Bänder im Einsatz sind, damit sie diese gegebenenfalls zurückrufen und die Löschung veranlassen kann. Der Patient kann eine Bestätigung der Löschung verlangen. Eine Herausgabe des Videobandes an den Patienten anstelle einer Löschung ist für Einzelaufnahmen denkbar.

Für Gruppenaufnahmen muss die Einwilligung jedes einzelnen Beteiligten vorliegen. Auch in solchen Fällen muss die Einwilligung frei sein, d.h. es sollte kein faktischer Zwang (Gruppenzwang) entstehen. Widerruft auch nur einer der Beteiligten seine Einwilligung, so muss das Videoband gelöscht werden. Mit der Herausgabe an einen oder mehrere Patienten (Videokopien) müssten alle Beteiligten einverstanden sein.

Auch bezüglich der Eigentumsverhältnisse stellen sich in der Praxis immer wieder Fragen. Daher sollte diese Frage im Reglement geregelt werden. Dabei geht es um das Eigentum an der Kassette. Die darauf aufgezeichneten Personendaten «gehören» aber in jedem Fall den Betroffenen. Sie können ihre diesbezüglichen Rechte unabhängig vom Eigentum an der Kassette geltend machen. Ebenso muss geregelt werden, was mit den Aufnahmen geschieht, wenn der Patient und/oder der behandelnde Arzt die Klinik verlässt. Es kann ein Grundsatz (z.B. Löschen der Aufnahme) im Reglement festgehalten werden, von dem im Einzelfall mit entsprechender schriftlicher Vereinbarung mit allen Beteiligten auch abgewichen werden kann. Die Regelungen können für die

Aufnahmen zu Supervisionszwecken und für die Aufnahmen zu Schulungszwecken unterschiedlich sein.

Für andere, neben den Patienten ebenfalls betroffene Personen (Therapeuten) gelten die gemachten Ausführungen analog. Für Videoaufnahmen zu Überwachungszwecken gilt das entsprechende Merkblatt des EDSB.

5.2 Berufsgeheimnis und externes Inkasso der Honorarrechnungen bzw. Betreibung des Patienten

Das Berufsgeheimnis verbietet Ärzten, Patientendaten an Dritte bekannt zu geben. Will ein Arzt eine Ärztekasse mit dem Inkasso seiner Honorarrechnungen beauftragen oder sieht er sich gezwungen, gegen einen säumigen Patienten die Betreibung einzuleiten, so benötigt er dazu die Einwilligung des Patienten. Im Falle der Betreibung wird der Patient sein Einverständnis wohl eher selten erteilen. Für Fälle, in denen der Betroffene die Einwilligung nicht erteilt, der Arzt aber aus persönlichem Interesse auf eine Befreiung von der Schweigepflicht angewiesen ist, sieht das Gesetz die Möglichkeit der Befreiung vom Berufsgeheimnis durch die vorgesetzte Behörde oder die Aufsichtsbehörde vor. Auf eine konkludente Einwilligung des Patienten kann sich der Arzt nicht berufen.

Es ist heute üblich, für administrative Arbeiten professionelle Institutionen beizuziehen. Das DSG erlaubt eine Datenbearbeitung durch Dritte, sofern der Auftraggeber dafür sorgt, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

Der Beauftragung von Dritten durch Ärzte, also z.B. Ärztekassen und Inkassobüros, steht eine gesetzliche Geheimhaltungspflicht entgegen, nämlich das im Strafgesetzbuch geregelte Berufsgeheimnis (Arzt-/Patientengeheimnis). Die Offenlegung von Patientendaten gegenüber Dritten ist demnach nur erlaubt, wenn die Einwilligung des betroffenen Patienten vorliegt, ein Gesetz es vorsieht oder die vorgesetzte Behörde oder Aufsichtsbehörde dem Arzt eine entsprechende Bewilligung erteilt hat. Die Formulierung im Strafgesetzbuch ist diesbezüglich klar und deutlich. Unbestritten ist heute, dass die Tatsache des Arztbesuches an sich bereits unter das Patientengeheimnis fällt. Bei den für das Inkasso bzw. die Betreibung notwendigen Daten handelt es sich somit immer um besonders schützenswerte Personendaten.

Will ein Arzt also eine Ärztekasse mit dem Inkasso seiner Honorarrechnungen beauftragen, benötigt er dazu die Einwilligung seines Patienten. In der Praxis wird die Einwilligung des Patienten in der Regel vor Beginn der Behandlung mittels eines Formu-

lars eingeholt, auf dem der Patient eine vorformulierte Einwilligungserklärung unterzeichnet. Allerdings haben wir festgestellt, dass die benutzten Einwilligungserklärungen oft zu wenig präzis verfasst sind.

Wie steht es nun im Falle, wo ein säumiger Patient betrieben werden muss? Da auch hier besonders schützenswerte Personendaten an das beauftragte Inkassobüro bzw. an das Betreibungsamt weitergegeben werden, ist eine Befreiung des Arztes vom Berufsgeheimnis erforderlich. In Frage kommt gemäss Gesetz nur die Einwilligung des Patienten oder die Befreiung durch die vorgesetzte Behörde oder Aufsichtsbehörde. Die Einwilligung kann zwar vorsorglicherweise schon zu Beginn der Behandlung auf dem schon erwähnten Formular eingeholt werden. Ein solches Vorgehen ist aber psychologisch nicht sehr geschickt – wird sich doch der Patient von Anfang an als potentieller Nichtzahler abgestempelt fühlen – und so wird in der Praxis diese Einwilligung entweder gar nicht verlangt oder vom Patienten nicht erteilt. Dass der Patient später, wenn die Betreibung notwendig wird, noch einwilligt, ist eher unrealistisch.

Immer wieder wird uns daher die Frage gestellt, ob im Falle einer notwendigen Betreibung anstelle der Befreiung vom Arztgeheimnis durch die vorgesetzte Behörde nicht aus Praktikabilitätsgründen auf eine konkludente Einwilligung geschlossen werden dürfe, sofern der Patient auf die schriftliche, ausdrückliche Androhung der Einleitung der Betreibung nicht reagiere.

Da die Einwilligung an keine Formvorschrift gebunden ist, kann sie auch konkludent erteilt werden. Von der ausdrücklichen Einwilligung unterscheidet sich die konkludente dadurch, dass sie sich aus den gesamten Umständen erkennbar und offenkundig ergibt. Das Verhalten des Patienten muss also absolut schlüssig sein. Aus den Umständen, namentlich aus dem Schweigen des Betroffenen, darf aber nicht ohne Weiteres auf eine konkludente Einwilligung geschlossen werden. Erstens ergibt sich schon aus dem Verhältnismässigkeitprinzip, dass die Einwilligung um so klarer sein muss, je heikler die Daten sind (vgl. unseren 7. Tätigkeitsbericht 1999/2000, Abschnitt 3.1). Zweitens ist zu beachten, dass der Arzt bei der Eintreibung seiner Honorarforderung nicht im Interesse des Patienten, sondern in seinem eigenen privaten Interesse handelt. Genau für die Fälle, in denen der Betroffene die Einwilligung nicht erteilt, der Arzt aber aus persönlichem Interesse auf eine Befreiung von der Schweigepflicht angewiesen ist, hat der Gesetzgeber ausdrücklich den Weg über die vorgesetzte Behörde vorgeschrieben. Drittens sagt das Bundesgericht in langjähriger Rechtsprechung, dass eine blosse Geldschuld keine Grundrechtsverletzung – hier in Form einer Persönlichkeitsverletzung durch Datenweitergabe – zu rechtfertigen vermag.

Aus all diesen Gründen genügt eine konkludente Einwilligung sowohl für die administrative Auslagerung der Rechnungsstellung wie auch für die Betreibung des Patienten,

der ein säumiger Zahler ist, nicht. Es liegt überdies im Interesse des Arztes, über eine eindeutige schriftliche Einwilligung des Patienten oder eine schriftliche Bewilligung der vorgesetzten Behörde zu verfügen, riskiert er doch eine Strafanzeige, sollte er sich bei der Datenweitergabe an Dritte auf eine ungenügende oder nicht rechtsgültige Einwilligung abstützen.

Beide Fälle sind bezüglich Notwendigkeit und Klarheit der Einwilligung des Patienten vergleichbar. In der Praxis ist es wichtig, dass die entsprechenden Einwilligungserklärungen voneinander getrennt und eindeutig formuliert werden, so dass der Patient völlig frei eine oder beide Einwilligungen erteilen kann. Nachstehend eine mögliche Formulierung:

Ich bin damit einverstanden, dass Dr. XY die für die Rechnungsstellung und das Inkasso erforderlichen Daten jeweils an die Inkassostelle (Name/Adresse) weiterleitet.

Ort, Datum ..... Unterschrift: .....

Ich bin damit einverstanden/nicht damit einverstanden (Unzutreffendes streichen), dass Dr. XY bzw. die von ihm beauftragte Inkassostelle (Name/Adresse) im Falle meines Zahlungsverzugs die Schuldbetreibung beim zuständigen Betreibungsamt anheben und durchführen kann.

Ich nehme zur Kenntnis, dass ohne diese Einwilligung der Arzt die Möglichkeit hat, bei der vorgesetzten Behörde oder Aufsichtsbehörde eine Befreiung vom Berufsgeheimnis zu beantragen, um die Schuldbetreibung einzuleiten.

Ort, Datum ..... Unterschrift: .....

6. Versicherungen

6.1 Sozialversicherungen

6.1.1 Regelungslücken im medizinischen Datenschutz

Der Bericht über den medizinischen Datenschutz im Sozialversicherungsbereich wurde dem Bundesamt für Sozialversicherung (BSV) und dem EDSB unterbreitet (siehe Postulat Kommission für Rechtsfragen NR 00.3178). Für uns ist von Bedeutung, dass unsere Stellungnahme im anschliessenden Vernehmlassungsverfahren berücksichtigt wird.

Ein Postulat beauftragte das BSV, einen umfassenden Bericht über den medizinischen Datenschutz im gesamten Sozialversicherungsbereich zu verfassen. Wir wurden zur Mitarbeit eingeladen (mehr dazu in unserem 10. Tätigkeitsbericht 2002/2003, Abschnitt 6.1.2). Insbesondere sollen die Chancen und Risiken der technologischen Entwicklung im medizinischen Datenschutz aufgezeigt und analysiert werden. Ausgangspunkt der Untersuchung ist das im Strafgesetzbuch verankerte Patientengeheimnis. Der Bericht wurde schliesslich durch das Institut für Gesundheitsrecht der Universität Neuenburg fertig erstellt.

Das BSV hat uns den (noch nicht öffentlichen) Bericht zu einer ersten Begutachtung unterbreitet. Betreffend den Inhalt des Berichts gibt es zwischen dem BSV und uns verschiedene Ansichten. Die Meinungen gehen bei der Frage auseinander, wie der datenschutzrechtliche Vollzugsnotstand im Sozialversicherungsbereich behoben werden kann.

Das BSV wird in naher Zukunft ein Vernehmlassungsverfahren bei den interessierten Kreisen durchführen (Versicherer, Patientenorganisationen etc.). Wir gehen davon aus, dass wir in der Folge ebenfalls Gelegenheit zur Stellungnahme erhalten. Wichtig für uns ist es, dass unsere Beurteilung entweder im Bericht direkt integriert oder separat dem Parlament unterbreitet wird.

6.1.2 Die SUVA und der Einsatz von Privatdetektiven

Die Beschattung und Videoüberwachung von Versicherten durch die SUVA sind nur unter gewissen Voraussetzungen möglich. Insbesondere ist dazu eine gesetzliche Grundlage notwendig, welche den Zweck und den Umfang solcher Überwachungen klar regelt.

Das Thema der Beschattung bzw. Videoüberwachung von Versicherten hat in der täglichen Arbeit des EDSB an Bedeutung zugenommen. Die Frage der Privatdetektiveins-

ätze hat sich im Berichtsjahr vor allem mit der SUVA gestellt (siehe auch BGE 5C 187/1997 und Einfache Anfrage Leutenegger Oberholzer 03.1077: Beschattung und Videoüberwachung von Versicherten). Die SUVA ist als obligatorischer Unfallversicherer tätig.

Uns ist bekannt, dass im obligatorischen Unfallversicherungsbereich vermehrt Privatdetektive eingesetzt werden. Zweck dieser Abklärungen ist es, allfällige unberechtigte Leistungsansprüche der Versicherten zu vermeiden bzw. aufzudecken. Solche Untersuchungen werfen aus datenschutzrechtlicher Sicht gewisse Fragen auf. (Auf die strafrechtlichen Aspekte wird vorliegend nicht eingegangen.)

Fotos und Videoaufnahmen von Versicherten (inkl. das Erstellen von Berichten) sind Datenbearbeitungen im Sinne des DSG. Sie stellen einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der Versicherten dar. Erst recht gilt dies, wenn Gesundheitsdaten bearbeitet werden, ohne dass die betroffene Person vorher informiert worden ist.

Bundesorgane – wie vorliegend obligatorische Unfallversicherer – dürfen Personendaten im Rahmen von Beschattungen und Videoüberwachungen in der Regel nur dann bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. Zudem sind die datenschutzrechtlichen Grundsätze wie etwa Transparenz und Verhältnismässigkeit soweit wie möglich einzuhalten. Nach unserer Auffassung gibt es in der gesamten Sozialversicherungsgesetzgebung keine Rechtsnormen, welche den Einsatz von Privatdetektiven rechtfertigen würden.

Beschattungen und Videoüberwachungen durch obligatorische Unfallversicherer müssen zudem im öffentlichen Interesse sein und vor allem dem Verhältnismässigkeitsprinzip entsprechen. So wäre es heikel, etwa die finanziellen Interessen des Unfallversicherers in jedem Fall höher zu werten als die Persönlichkeitsrechte der Versicherten. Entscheidend ist jedoch, dass die Unfallversicherer im Rahmen ihrer Abklärungspflicht zuerst andere, weniger stark in die Privatsphäre eingreifende Massnahmen treffen müssen. Beschattungen oder Videoüberwachungen von Versicherten müssen notwendig und somit das einzige Mittel sein, um etwa einen Versicherungsbetrug aufdecken zu können. Zudem dürfen geheime Überwachungen von Versicherten nicht präventiv durchgeführt werden, sondern es muss auch ein konkreter Verdachtsgrund für einen allfälligen Missbrauch von unberechtigten Leistungen vorliegen.

Ob und inwiefern Beschattungen und Videoüberwachungen überhaupt geeignet sind, einen allfälligen Versicherungsmissbrauch aufzudecken, bleibt grundsätzlich fraglich. Insbesondere dürfte die Beweiskraft solcher Erhebungen, die stets nur Momentaufnahmen darstellen, beschränkt sein.

Wir sind der Ansicht, dass die Frage der Beschattungen und Videoüberwachungen durch Unfallversicherer aus datenschutzrechtlicher Sicht noch nicht befriedigend gelöst ist und einer vertieften Analyse bedarf. Zu prüfen ist insbesondere, ob Beschattungen und Videoaufnahmen im Unfallversicherungsbereich im Einzelfall überhaupt geeignet sind, die Leistungsansprüche der Versicherten abzuklären. Sollte dies tatsächlich der Fall sein, wäre eine entsprechende gesetzliche Grundlage zu schaffen, welche Zweck, Umfang und Voraussetzungen solcher Überwachungen klar regelt. Auf alle Fälle gilt es zu vermeiden, dass ohne Weiteres neue Beweismittel bzw. Methoden im Unfallversicherungsbereich zugelassen werden. Denn dies könnte zu einer Tendenz führen, wonach der Zweck die Mittel heiligt.

6.2 Privatversicherungen

6.2.1 Die Beschaffung von Personendaten durch Haftpflichtversicherer

Wir haben Mindeststandards darüber aufgestellt, unter welchen Voraussetzungen ein Haftpflichtversicherer Gutachten über Geschädigte einholen darf. Grundsätzlich ist dafür ein Rechtfertigungsgrund sowie die umfassende und vorherige Information des Geschädigten notwendig. Wir haben die Grundsätze in einem Merkblatt festgehalten, welches auch im Internet abrufbar ist (siehe unter http://www.edsb.ch/d/doku/merkblaetter/haftpflicht.htm sowie im Anhang 13.4).

6.2.2 Bekämpfung des Versicherungsmissbrauchs und Datenschutz

Die Privatversicherer haben ihre Bemühungen verstärkt, den Versicherungsmissbrauch zu bekämpfen. Oftmals geraten sie dabei mit der Datenschutzgesetzgebung in Konflikt.

Die Privatassekuranz ist daran, Strukturen zu schaffen, welche betrügerische Praktiken aufdecken sollen. Bereits seit Jahren existiert das Zentrale Informationssystem (ZIS) des Schweizerischen Versicherungsverbandes, welches den einzelnen Versicherungsgesellschaften zugänglich ist. Das ZIS führt eine (beim EDSB) angemeldete Datensammlung über hängige und bereits abgeschlossene Straf- und Zivilverfahren (mehr dazu in unserem 7. Tätigkeitsbericht 1999/2000, Abschnitt 7.9) Die Versicherer ihrerseits haben Massnahmen getroffen, um den Versicherungsmissbrauch zu bekämpfen. So werden etwa Privatdetektive eingesetzt, um möglichen ungerechtfertigten Leistungsansprüchen von Versicherten entgegenzuwirken. Wir wurden im Berichtsjahr vermehrt mit Fällen aus diesem Bereich konfrontiert.

Privatversicherer unterstehen dem DSG und müssen somit bei ihren Abklärungen das DSG einhalten. Insbesondere sind die datenschutzrechtlichen Grundsätze wie die Datensicherheit, das Verhältnismässigkeits- und das Transparenzprinzip zu beachten.

In einem Fall wurde zufällig aufgedeckt, dass ein Privatversicherer seit einigen Jahren interne Datensammlungen geführt hat. Die Datensammlungen waren weder den betroffenen Personen bekannt noch wurde sie beim EDSB angemeldet. Diese «schwarzen Listen» betreffen den Privatversicherungsbereich einerseits und den KVG/UVG-Bereich andererseits. Die Datenbanken dienen u.a. der Übersicht von Massnahmen zur Bekämpfung des Versicherungsmissbrauchs. Sie enthalten besonders schützenswerte Personendaten wie strafrechtliche Verfolgungen. Die betroffene Versicherung hat in der Zwischenzeit die zwei Datensammlungen beim EDSB angemeldet.

Wir sind zur Zeit daran, weitere Abklärungen zu machen. Insbesondere haben wir den Versicherer gebeten, die notwendigen technischen und organisatorischen Massnahmen zu treffen. So ist etwa der Zugriff auf die Datensammlungen durch unberechtigte Personen zu unterbinden. Ein weiterer Problembereich ist die Datenkategorie «allgemeine Bemerkungen», welche für persönlichkeitsverletzende Texte missbraucht werden kann.

Hauptproblem ist jedoch die mangelnde Transparenz der erwähnten Datensammlungen. Eine Datensammlung, welche mit dem Strafregister des Staates zu vergleichen ist, muss für die Betroffenen erkennbar sein. Datensammlungen mit besonders schützenswerten Personendaten sind daher grundsätzlich beim EDSB anzumelden. «Schwarze Listen» in diesem sensiblen Bereich sind somit vom Gesetzgeber nicht vorgesehen und werden sogar unter bestimmten Voraussetzungen unter Strafe gestellt. Die gegenwärtige Revision des DSG sieht zudem vor, das Transparenzprinzip zu verstärken. So soll etwa eine unmittelbare Informationspflicht gegenüber den betroffenen Personen eingeführt werden, wenn besonders schützenswerte Personendaten bearbeitet werden.

6.2.3 Die VAG- und VVG-Revision

Der Bundesrat hat die Botschaft zum revidierten Versicherungsaufsichtsgesetz (VAG) und zur Teilrevision des Versicherungsvertragsgesetzes (VVG) verabschiedet. Die Gesetzesrevisionen sehen auch eine Verbesserung des Datenschutzes im Privatversicherungsbereich vor.

Nach mehreren Ämterkonsultationen hat der Bundesrat die überarbeiteten VAG- und VVG-Revisionen der Öffentlichkeit vorgestellt. Oberstes Ziel der Gesetzesrevisionen sind die Sicherheit der Versicherungsunternehmen und ein verbesserter Konsumentenschutz. Wichtige Postulate des EDSB wurden dabei berücksichtigt.

Ein Anliegen des Konsumentenschutzes ist die verstärkte Informationspflicht der Versicherer gegenüber den Versicherungsnehmern. Der VVG-Entwurf sieht denn auch vor, dass Versicherer die Versicherungsnehmer über den wesentlichen Inhalt des Versicherungsvertrages informieren müssen. Dazu gehört auch die Information über die Bearbeitung der Personendaten einschliesslich Zweck und Art der Datensammlung sowie Empfänger und Aufbewahrung der Daten. Analog dazu sollen – gemäss dem revidierten VAG – auch die Versicherungsvermittler die Versicherten über die Datenbearbeitung informieren. Wir begrüssen es sehr, dass die Datenbearbeitung für die Versicherungsnehmer und Versicherten transparenter werden soll. Denn die mangelnde Transparenz der Datenbearbeitung ist tatsächlich eines der Hauptprobleme im Privatversicherungsbereich.

Im Weiteren verpflichtet der VAG-Entwurf die Versicherungsunternehmen neu, externe Revisionsstellen zu schaffen. Der Revisionsstelle obliegt eine Meldepflicht gegenüber der Aufsichtsbehörde, wenn ein Versicherungsunternehmen u. a. die Interessen der Versicherten gefährdet. Gemäss Botschaftstext sind die Interessen der Versicherten auch dann gefährdet, wenn Datenschutzverletzungen vorliegen. Dies bedeutet, dass das Bundesamt für Privatversicherungen als Aufsichtsbehörde auch bei Datenschutzverstössen von Amtes wegen einschreiten muss.

Wir anerkennen die Bemühungen, den Datenschutz im Privatversicherungsbereich zu verbessern. Es bleibt zu hoffen, dass im Rahmen der anstehenden VVG-Totalrevision datenschutzrechtlichen Anliegen noch mehr Gewicht beigemessen wird. Wir haben der zuständigen Expertenkommission für die Totalrevision VVG die verschiedenen Problembereiche und Lösungsmöglichkeiten aufgezeigt. Als ausgezeichnete Grundlage dafür erachten wir die Europarats-Empfehlung über den Schutz von zu Versicherungszwecken beschafften und bearbeiteten Personendaten. Die Empfehlung sieht etwa vor, dass die Datenbearbeitung von medizinischen Daten im Privatversicherungsbereich grundsätzlich nur von Berufspersonen des Gesundheitswesens vorgenommen werden darf. Wir werden die Totalrevision des VVG weiterhin verfolgen.

7. Arbeitsbereich

7.1 Rechtliche Aspekte einer telefonischen Beschwerdeanlaufstelle

Eine telefonische Beschwerdeanlaufstelle wird zur Feststellung und Verfolgung rechtswidriger oder unethischer Verhaltensweisen innerhalb eines Unternehmens eingerichtet. Letzteres ist verpflichtet, die Angestellten darüber zu informieren. Die Beschwerdeanlaufstelle soll überparteilich, neutral und vertrauenswürdig verwaltet werden. Sie hat die Beteiligten gleich zu behandeln und in ihrer Persönlichkeit zu schützen.

Ein internationales Unternehmen ist an uns mit dem Projekt gelangt, eine firmeninterne Beschwerdeanlaufstelle (Ethik-Hotline) aufzustellen. Danach sollen sich Angestellte wie auch aussenstehende Dritte anonym an sie wenden können, um auf ethisch oder rechtlich problematisches Verhalten der Firma oder ihrer Mitarbeiter hinzuweisen. Ein Angestellter soll sich bei der Anlaufstelle über eine bestimmte Person beschweren können, ohne dabei identifiziert zu werden. Er soll von einer direkten Konfrontation sowohl mit dem betroffenen Mitarbeiter als auch mit der Firma verschont bleiben. Dadurch soll der Angestellte bewusst in die Lage versetzt werden, ungeniert und offen problematische Sachverhalte wie z. B. die sexuelle Belästigung am Arbeitsplatz anzusprechen. Weiter soll der Angestellte dank der Anonymität vor Mobbing oder Drohungen geschützt werden. Wir haben dem Unternehmen mitgeteilt, dass die Anonymität den Denunzianten aber auch in die Lage versetzen kann, einen Arbeitnehmer aus einer völlig geschützten Position ungerechtfertigt anzuschwärzen. Eine Ethik-Hotline kann somit ungewollt auch die willkürliche Denunziation fördern. Die betroffene Person befindet sich in einer verwundbaren, ungeschützten Position gegenüber dem anonymen Denunzianten. Der angeschuldigte Arbeitnehmer kann möglicherweise zwar ein Gegendarstellungsrecht gegenüber der Firma geltend machen, eine faire und transparente Konfrontation mit dem anonymen Denunzianten ist aber nicht möglich. Es wird beispielsweise nicht möglich sein, den Hinweisgeber wegen eventueller Verleumdung oder übler Nachrede erfolgreich verfolgen zu lassen. Die Gleichbehandlung von Hinweisgeber und betroffenem Arbeitnehmer wird aufgrund des Kräfteungleichgewichts nicht gewährleistet. Um dem entgegenzuwirken, hat der Hinweisgeber Koordinaten zumindest in Form einer nicht namentlichen E-Mail-Adresse anzugeben. Bei Bedarf ist auch die volle Identität an die Beschwerdeanlaufstelle bekannt zu geben. Damit soll wenigstens eine Kontaktaufnahme und gegebenenfalls eine Konfrontation mit der Gegendarstellung des beschuldigten Arbeitnehmers ermöglicht werden. Fehlt die Kontaktmöglichkeit, sollte auf die Beschwerde grundsätzlich nicht eingetreten werden. Überparteilichkeit und Neutralität der Beschwerdeanlaufstelle sowie Vertraulichkeit sollen die involvierten Personen vor

Nachteilen wie Vorurteile oder Mobbing innerhalb der Firma schützen. Ideal wäre es, wenn die Beschwerdeanlaufstelle unabhängig wäre. Dies könnte sich aber dadurch nachteilig auswirken, dass sensible Sachverhalte kostenpflichtig an ein drittes Unternehmen bekannt gegeben werden müssen. Eine Kompromisslösung könnte darin bestehen, dass jede Filiale des internationalen Konzerns einen Vertreter an einer gemeinsamen Ethik-Hotline bereitstellt. Anrufe betreffend eine bestimmte Filiale würden dann nur vom Vertreter einer anderen Filiale entegegengenommen und bearbeitet. Somit könnte eine gewisse Überparteilichkeit und Neutralität gewährleistet werden.

Die Angestellten sind über das Bestehen einer unabhängigen Beschwerdeanlaufstelle und deren Zweck vorgängig ausdrücklich zu informieren, da die Ethik-Hotline Datenbearbeitungen ins Leben ruft und die betroffenen Personen ein Auskunftsrecht haben. Das Auskunftsrecht kann jederzeit, auch ohne konkrete Anzeichen einer Beschwerde, geltend gemacht werden. Neben dem Auskunftsrecht ist auch das Berichtigungs- und Vernichtungsrecht der betroffenen Personen zu gewährleisten. Sollte der Arbeitgeber aus arbeitsrechtlichen Gründen personenbezogene Informationen durch die Beschwerdeanlaufstelle erhalten haben, müsste er sie, analog der Beschwerdeanlaufstelle, vertraulich behandeln. Eine Datenbekanntgabe an Dritte (z. B. an die Arbeitskollegen der betroffenen Person) durch den Arbeitgeber ist nicht oder nur bei Vorliegen eines überwiegenden Interesses zulässig. Sobald der Zweck der Datenbearbeitung erfüllt ist, sind die Daten zu vernichten. Was das Mitschneiden von Anrufen auf Tonträgern betrifft, gelten die Bestimmungen des Strafgesetzbuches. Danach wird derjenige mit Gefängnis oder mit Busse bestraft, welcher als Gesprächsteilnehmer ein nichtöffentliches Gespräch ohne die Einwilligung der andern daran Beteiligten mit einem Abhörgerät abhört oder auf einen Tonträger aufnimmt.

7.2 Entscheid der EDSK in Sachen Drogentests in der Lehre

Nach Weiterzug unserer Empfehlung an die EDSK (vgl. unseren 9. Tätigkeitsbericht 2001/2002, Abschnitt 7.8 und Anhang 13.6.3) ist Ende August 2003 das entsprechende Urteil gefällt worden. Dabei wurde unserem Begehren weitgehend stattgegeben. Die Firma Roche hat laut Urteil der EDSK ihr Drogenkonzept dahingehend anzupassen, dass Drogentests nur auf begründeten Verdacht hin im Einzelfall und nur bei Vorliegen einer auf diesen Einzelfall bezogenen Einwilligung vorgenommen werden dürfen. Sämtliche bisher im Rahmen des Konzeptes der drogenfreien Lehre erhobenen Daten sind laut EDSK zu vernichten, soweit im Einzelfall kein begründeter Verdacht Anlass für den Test war. Das Urteil der EDSK ist in Anhang 13.9 zu finden.

7.3 Empfehlung des EDSB zur Entlassungsliste von Orange

Die Firma Orange SA hat als Entscheidungsgrundlage für eine Massenentlassung eine Entlassungsliste erstellt. Die Liste hat zum Teil subjektive Verhaltenswertungen sowie zweckwidrige und unverhältnismässige Daten aus der Privatsphäre enthalten. Die betroffenen Angestellten sind über das Bestehen der Entlassungsliste nicht informiert worden. Wir haben der Orange SA empfohlen, die betroffenen Personen über das Bestehen der Liste zu informieren und das Auskunftsrecht zu gewährleisten. Weiter haben wir empfohlen, die Liste nur solange aufzubewahren, bis allfällige Gerichtsentscheide in Rechtskraft erwachsen sind. Ferner haben wir die Orange SA aufgefordert, bei allfälligen weiteren Massenentlassungen den Kündigungsschutz, die Rechtsgleichheit, die Koalitionsfreiheit und die Gleichstellung von Frau und Mann zu beachten und sich auf jene Datenkategorien zu beschränken, welche für die ordnungsgemässe Durchführung einer Massenentlassung nötig und geeignet sind. Die Empfehlung ist in Anhang 13.10.1 zu finden.

7.4 Erläuterungen zur Videoüberwachung am Arbeitsplatz

Videoüberwachungsanlagen lösen erfahrungsgemäss bei den betroffenen Arbeitnehmern negative Gefühle aus und verschlechtern das allgemeine Betriebsklima. Sie können das Wohlbefinden, die psychische Gesundheit und damit die Leistungsfähigkeit des Personals beeinträchtigen. Unsere Erläuterungen zur Videoüberwachung am Arbeitsplatz sollen das bestehende Merkblatt über die Videoüberwachung durch private Personen (vgl. http://www.edsb.ch/d/doku/merkblaetter/video.htm) ergänzen. Die Erläuterungen sind in Anhang 13.1 zu finden.

7.5 Erläuterungen zur Telefonüberwachung am Arbeitsplatz

Nach dem Einzug der mobilen Telefonie in die Arbeitswelt hat es sich als nötig erwiesen, das 1999 publizierte Merkblatt der Arbeitsgruppe der kantonalen und eidgenössischen Datenschutzbeauftragten über das Telefonieren am Arbeitplatz zu ersetzen. Die Erläuterungen des EDSB sind in Anhang 13.2 zu finden.

7.6 Erläuterungen zu Referenzauskünften im Bewerbungsverfahren

Lehre und Praxis sehen im Zusammenhang mit der Erteilung von Referenzauskünften unterschiedlich aus. Insbesondere ist es umstritten, ob Referenzauskünfte nur mit der Einwilligung des Bewerbers erteilt werden dürfen. Nach Inkrafttreten des DSG erhoffte man sich eine Lösung. Die Rechtslage und die Praxis blieben aber weiterhin unsicher. Mit unseren Erläuterungen wird eine Klärung dieser Frage angestrebt. Die Erläuterungen zu den Referenzauskünften im Bewerbungsverfahren sind sowohl auf http://www.edsb.ch/d/themen/weitere/referenzauskuenfte_d.pdf als auch in Anhang 13.3 zu finden.

8. Handel und Wirtschaft

8.1 Änderung von Artikel 179quinquies Strafgesetzbuch: Straflosigkeit der Aufnahme bestimmter Telefongespräche

Am 1. März 2004 ist die neue Fassung des Artikel 179quinquies Strafgesetzbuch (StGB) in Kraft getreten. Mit der Änderung dieser Bestimmung ist es nun möglich, bestimmte Telefongespräche im Geschäftsverkehr ohne Einwilligung der Gesprächsteilnehmer aufzunehmen. Die Ausnahmebestimmung ist aber sehr eng gefasst und die gemachten Aufnahmen dürfen lediglich zu Beweiszwecken verwendet werden.

Mit der Neufassung von Artikel 179quinquies StGB wird die Aufnahme von Fernmeldegesprächen in zwei Fällen für straflos erklärt:

- Wenn Gespräche mit Hilfs-, Rettungs- und Sicherheitsdiensten aufgenommen werden (Art. 179quinquies Abs. 1 Bst. a); und
- wenn Gespräche im Geschäftsverkehr aufgenommen werden, welche «Bestellungen, Aufträge, Reservationen und ähnliche Geschäftsvorfälle zum Inhalt haben» (Art. 179quinquies Abs. 1 Bst. b).

Nach der bisher geltenden Fassung der Bestimmung war lediglich die Aufnahme von Notrufen straflos. Im Zusammenhang mit der Änderung stellte sich insbesondere die Frage, ob die neu vorgesehene Straflosigkeit auch von der Erfüllung der datenschutzrechtlichen Transparenzpflicht – und damit von der Pflicht zur Information der betroffenen Gesprächsteilnehmer – entbindet.

Die Analyse des Regelungszwecks, wie er in den parlamentarischen Beratungen zum Ausdruck kam, führt zum Ergebnis, dass es klares Ziel des Gesetzgebers war, in bestimmten Fällen Aufnahmen zu ermöglichen und dabei auf das Erfordernis der Einwilligung der Betroffenen – und damit seine vorgängige Information – zu verzichten. Aus Sicht des Datenschutzrechts ist daher die vorgenommene Änderung des StGB so zu interpretieren, dass der Datenbearbeiter in den von der Änderung erfassten Fällen den Rechtfertigungsgrund der gesetzlichen Grundlage im Sinne von Artikel 13 Absatz 1 DSG geltend machen kann.

Nach der neuen Fassung des Artikels dürfen Gespräche mit Hilfs-, Rettungs- und Sicherheitsdiensten auch dann aufgenommen werden, wenn es sich nicht um Notrufe handelt. Die Straflosigkeit der Aufnahme ist nicht darauf beschränkt, dass der Anruf auf eine bestimmte Nummer (Notrufnummer) erfolgt. Eine vorgängige Information der anrufenden Person ist nicht erforderlich. Die Gespräche dürfen durch alle Beteiligten aufgenommen werden.

Die Formulierung der Ausnahme für den Geschäftsverkehr ist im Rahmen der Beratungen in den eidgenössischen Räten gegenüber dem ursprünglichen Vorschlag stark eingeschränkt worden. Die Entstehungsgeschichte macht deutlich, dass die neue Fassung sich auf ganz bestimmte Gesprächssituationen bezieht.

Eine Aufnahme des Gesprächs ohne vorherige Information ist nach Absatz 1 Buchstabe b nur dann möglich, wenn es um *Bestellungen, Aufträge, Reservationen sowie «ähnliche Geschäftsvorfälle»* geht. Im Nationalrat wurde präzisiert, dass «Massengeschäfte» gemeint seien. Begründet wurde der Verzicht auf die Information in diesen Fällen damit, dass es in bestimmten Situationen zu aufwändig sei, auf die Aufnahme hinzuweisen, z.B. in der Tourismusbranche. Die vom Gesetzgeber mit der Änderung angestrebten Erleichterungen beschränken sich also auf Gesprächssituationen, in denen vom Kontext her eindeutig ausschliesslich ein bestimmter, massenhaft vorkommender «Geschäftsvorfall» betroffen und ein gewisser «Zeitdruck» für dessen Abwicklung gegeben ist. Somit fällt die Aufnahme von Gesprächen, die über ein «Bestelltelefon» oder ein «Reservationstelefon» laufen, eindeutig unter die mit der vorliegenden Bestimmung gewollten Erleichterungen.

Wird dagegen z.B. ein Vertrag telefonisch ausgehandelt, so ist es ohne weiteres möglich, zumutbar und verhältnismässig, dass derjenige, der das Gespräch aufnehmen will, den anderen informiert. Auch dort, wo bereits eine Vertragsbeziehung zwischen den beteiligten Geschäftspartnern besteht, ist es keineswegs so, dass überhaupt keine Information mehr erfolgen muss. Vielmehr wurde es als problemlos machbar angesehen, dass in solchen Fällen z.B. ein entsprechender Hinweis im Rahmen eines Vertrages bzw. von allgemeinen Geschäftsbedingungen erfolgen kann.

Die Tragweite der Ausnahmeklausel wurde in den Räten auch anhand von Beispielen verdeutlicht: So sei die Aufnahme eines Gesprächs ohne Information zulässig, wenn es sich um die Reservation eines Flugbilletts oder Hotelzimmers handle. Eine Information wird indessen erforderlich, wenn ein Gespräch aufgenommen werden soll, bei dem es um eine Reklamation betreffend einen Flug oder ein Hotelzimmer geht.

Bezüglich der nun straflos ohne vorgängige Information möglichen Aufnahmen gilt darüber hinaus eine *strikte Zweckbindung*. Sie dürfen ausschliesslich zur Beweissicherung verwendet werden. Namentlich die Bekanntgabe an Dritte bleibt weiterhin strafbar. Besonders hervorzuheben ist, dass auch die *Auswertung* der Aufnahmen unzulässig ist. Damit ist es ausgeschlossen, dass Aufnahmen, die gestützt auf die neu gefasste Ausnahmebestimmung angefertigt wurden, z.B. für Marketingzwecke analysiert werden. Falls solche Auswertungen vorgenommen werden sollen oder falls die Aufnahmen für Ausbildungszwecke oder für die Kontrolle des Verkaufsverhaltens der Angestellten verwendet werden sollen, ist – wie bisher – eine vorgängige Information erforderlich.

8.2 Unerwünschte Werbung: Anspruch auf Löschung seiner Personendaten

Personendaten dürfen nicht gegen den ausdrücklichen Willen der betroffenen Person bearbeitet werden. Sie kann verlangen, dass der Datenbearbeiter ihr die Löschung der sie betreffenden Angaben bestätigt. Im Wiederholungsfall muss der betroffenen Person auch mitgeteilt werden, von wem ihre Personendaten bezogen worden sind, damit sie auch dort eine Löschung der Daten verlangen kann.

Ein Privater ist an uns gelangt und hat uns darüber informiert, dass er immer wieder von einer Religionsgmeinschaft kontaktiert wird, obwohl er sie bereits mehrmals schriftlich aufgefordert hat, ihn nicht mehr anzuschreiben und aus der Adressliste zu streichen. Da schon wiederholt Beschwerden gegen diese Gemeinschaft bei uns eingegangen sind, haben wir interveniert und sie unmissverständlich auf die klaren gesetzlichen Bestimmungen hingewiesen.

Laut DSG kann eine Person nämlich ausdrücklich verlangen, dass ihre Persondaten nicht gegen ihren Willen bearbeitet werden und alle sie betreffenden Daten in der Datensammlung des Bearbeiters gelöscht werden. Sie kann zudem verlangen, dass ihr der Datenbearbeiter bestätigt, dass die Daten gelöscht worden sind. Den Datenbearbeiter trifft die Pflicht, die notwendigen organisatorischen und technischen Massnahmen zu treffen, damit der Wille dieser Person respektiert wird. Als logische Konsequenz darf der Datenbearbeiter daher zu diesem Zweck (aber nur zu diesem!) eine Liste mit Personendaten (d.h. Name und Adresse) führen, die inskünftig nicht mehr kontaktiert werden möchten.

Wir forderten die Religionsgemeinschaft auf, die Löschung dem Betroffenen und uns zu bestätigen. Ausserdem verlangten wir von der Gemeinschaft, die notwendigen Massnahmen zu ergreifen, damit der ausdrückliche Wille all jener, die keine (auch brieflichen) Kontakte mehr wünschen, respektiert und das DSG eingehalten wird.

Zudem wiesen wir darauf hin, dass der Datenbearbeiter im Wiederholungsfall der betroffenen Person mitteilen muss, warum er ihrem Wunsch nicht bereits nachgekommen ist respektive bei wem in der Zwischenzeit die Adresse neu eingekauft worden ist. Denn nur so kann die betroffenen Person auch beim Datenlieferanten die Löschung ihrer Adresse durchsetzen.

Hält sich der Datenbearbeiter nicht an den ausdrücklich geäusserten Willen der betroffenen Person und kontaktiert er sie weiterhin, so kann sie eine Klage zum Schutz ihrer Persönlichkeit einreichen. Ausserdem behalten wir uns in diesen Fällen ausdrücklich vor, bei einem Datenbearbeiter, der wiederholt das Sperrrecht nicht beachtet, eine Kontrolle durchzuführen.

8.3 Weitergabe von Kundendaten aus einem Vertrauensverhältnis

Bei der unternehmensinternen Weitergabe von Kundendaten, die aus einem Vertrauensverhältnis stammen, kommt dem Transparenzprinzip besondere Bedeutung zu. Nur wenn der Kunde Kenntnis davon hat, dass der Kreis der Datenbearbeiter und die ursprünglich vereinbarten Bearbeitungsmodalitäten ändern, kann er in die Weitergabe einwilligen. Die Zustimmung muss ausdrücklich und sollte bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen sogar schriftlich erfolgen.

Im Rahmen einer laufenden Reorganisation plante ein Finanzunternehmen, ein Beratungscenter in der Stadt A. aufzuheben und mit jenem in der Stadt B. in einer neuen Organisationseinheit zusammenzufassen. Wir wurden angefragt, ob eine Weitergabe der Kundendaten ohne weiteres möglich sei. Bei den in Frage stehenden Kundendaten handelte es sich laut Angaben des Unternehmens einerseits um besonders schützenswerte Personendaten (unter anderem Angaben zur Gesundheit) und anderseits um Persönlichkeitsprofile (umfassende Auflistung der Vermögensverhältnisse).

Zentral für den vorliegenden Fall ist der Grundsatz von Treu und Glauben (Transparenzprinzip). Er besagt, dass die Datenbeschaffung und jeder weitere Bearbeitungsschritt für die betroffene Person transparent, d.h. erkennbar, erfolgen muss. Mit anderen Worten dürfen die Daten nicht auf eine Art und Weise bearbeitet (also auch bekannt gegeben) werden, mit der die betroffene Person nicht einverstanden gewesen wäre.

In der Vergangenheit hatte das Finanzberatungscenter seinen Kunden stets zugesichert, dass ihre Personendaten nur den zuständigen, namentlich bekannten Sachbearbeitern im Finanzberatungscenter in A. zugänglich sind. Dadurch wurde die Grundlage für ein *Vertrauensverhältnis* zwischen dem Kunden und seinem Finanzberater geschaffen, das es dem Kunden ermöglichte, ihm bestimmte sensible Angaben zu seiner Person mitzuteilen. Diese Zusicherung kann damit als wesentlicher, subjektiver Vertragsbestandteil gewertet werden und schliesst eine Bekanntgabe der Kundendossiers an Personen ausserhalb dieses Vertrauensverhältnisses aus.

Mit der Zusammenlegung der beiden Finanzberatungscenter änderte sich zwangsläufig nicht nur der Kreis der Datenbearbeiter, sondern auch die ursprünglich vereinbarten Bearbeitungsmodalitäten und damit das Vertragsverhältnis als solches. Aufgrund des bestehenden Vertrauensverhältnisses und des vertraulichen Inhalts der Kundendossiers verlangt das Transparenzprinzip, dass die Betroffenen über die Weitergabe ihrer Daten an ein neues Finanzberatungscenter (und damit an neue Sachbearbeiter) informiert werden. Nur so kann sichergestellt werden, dass die Kunden damit einverstanden sind.

Mit dieser Einwilligung liegt sodann der von Art. 12 Abs. 2 Bst. c DSG geforderte Rechtfertigungsgrund vor. Dabei gilt es Folgendes zu beachten: Je sensibler die Daten sind, desto höhere Anforderungen sind an die Transparenz der Einwilligung zu stellen. Daher müssen die Kunden *umfassend* darüber informiert werden, dass ihre Daten an ein neues Finanzberatungscenter bekannt gegeben werden. Die Einwilligung von Seiten jedes einzelnen Betroffenen zur Weitergabe kann in diesem Fall nicht stillschweigend, sondern muss ausdrücklich und – da es sich besonders schützenswerte Personendaten handelt – schriftlich erfolgen.

Aus datenschutzrechtlicher Sicht können die betroffenen Personen nur dann rechtsgültig einwilligen, wenn sie den künftigen Bearbeitungszweck, den Umfang der Datenbekanntgabe und den neuen Datenbearbeiter hinreichend kennen.

8.4 Unzulässige Werbung per Mail / Spam

Angesichts der rapiden Zunahme der Anzahl unerwünschter Werbemails ist die Rechtslage beinahe weltweit in Bewegung geraten. In der Schweiz zeichnet sich ab, dass das Prinzip des Opting Out durch dasjenige des Opting In abgelöst wird, welches in der EU seit Oktober vergangenen Jahres Gültigkeit hat.

In unserem vergangenen Tätigkeitsbericht (10. Tätigkeitsbericht 2002/2003, Abschnitt 8.1) haben wir das Thema Spam im Grundsatz geschildert und dargestellt, welche Voraussetzungen erfüllt sein müssen, damit die ungefragte Zustellung von Werbemails rechtmässig ist. Zusammengefasst lauten diese Voraussetzungen gemäss aktueller Rechtslage in der Schweiz folgendermassen: Erstens dürfen nur rechtmässig gesammelte Adressen verwendet werden und zweitens muss den Empfängern ein einfacher Weg angeboten werden, um ihr Widerspruchsrecht (Recht auf Opting Out) auszuüben.

Analog zur Entwicklung im EU-Raum ist auch in der Schweiz eine Tendenz in Richtung strengere Voraussetzungen für die Rechtmässigkeit zu beobachten. In den Staaten der EU gilt seit Ende Oktober 2003 das Prinzip des Opting In, d.h. die Zustellung von Werbemails ist nur noch dann erlaubt, wenn entweder der Empfänger vorgängig ausdrücklich zugestimmt hat oder wenn zwischen Empfänger und Absender schon eine Geschäftsbeziehung besteht. Wenn auch noch unklar ist, welche Formulierung genau in die schweizerische Gesetzgebung einfliessen wird, so scheint doch die Absicht klar, auch bei uns das Prinzip des Opting In einzuführen. Zumindest steht dies in der Botschaft zur Revision des Fernmeldegesetzes (FMG, BBl 2003 7966). Die Formulierung im Entwurf zum entsprechenden Artikel, welcher ins Bundesgesetz über den unlauteren Wettbewerb (UWG) eingefügt werden soll, entspricht dieser Absicht aber

nicht. Denn danach betreibt unlautere Werbung, wer Massenwerbung fermeldetechnisch sendet «und es dabei unterlässt, vorher die Einwilligung der Kunden einzuholen, den korrekten Absender anzugeben oder auf eine problemlose und kostenlose Ablehnungsmöglichkeit hinzuweisen» (aus dem Entwurf für Art. 3 Buchstabe o UWG). Entsprechend wäre ein blosser Hinweis auf eine Ablehnungsmöglichkeit eine Alternative zur vorgängigen Einwilligung der Empfänger, womit wieder das Prinzip des Opting Out Gültigkeit hätte.

Im Rahmen der aktuellen Revision des FMG sind darüber hinaus zwei Punkte wesentlich. Einerseits ist bei der vorgesehenen Revision des UWG von Bedeutung, dass ein Verstoss gegen die Verhaltensregel durch Werbetreibende mit Strafe bedroht wird. Andererseits wird im Zuge derselben Gesetzesrevision den Anbieterinnen von Fernmeldedienstleistungen auch die Verpflichtung auferlegt, unlautere Massenwerbung zu bekämpfen. Es scheint wahrscheinlich, dass diese Bestimmung dort am bedeutsamsten wird, wo die Provider selbst aus der Tatsache Kapital schlagen können, dass Werbung an ihre Benutzer gesendet wird. Hierbei ist in erster Linie an das noch wenig entwickelte Gebiet des Location Based Advertising zu denken, welches ohne die Provider überhaupt nicht machbar ist.

Die in unserem 10. Tätigkeitsbericht erwähnte Empfehlung betreffend den in Zürich wohnhaften Werbetreibenden ist im Moment bei der EDSK hängig. Strittig ist mit Bezug auf diese Empfehlung, welchen Aufwand der Werbetreibende betroffenen Personen bei der Ausübung ihres Rechtes auf Opting Out zumuten darf. Der Werbetreibende bietet gemäss seiner Aussage Briefpost oder Telefax als Möglichkeiten an, während der EDSB eine Widerspruchsmöglichkeit über dasselbe Kommunikationsmedium verlangt.

9. Finanzen

9.1 Datenschutzfragen bei der Ausübung von Aktionärsrechten

Wir wurden ersucht, die Problematik der Erfassung des Stimmverhaltens der Aktionärinnen und Aktionäre an der Generalversammlung (GV) unter dem Aspekt des Datenschutzes zu prüfen, insbesondere wenn die Betroffenen auch Arbeitnehmerinnen oder Arbeitnehmer des betreffenden Unternehmens sind. Es zeigt sich, dass grundsätzlich kein Recht des Aktionärs auf geheime Stimmabgabe besteht und dass bestimmte Bearbeitungen von Personendaten im Zusammenhang mit der Ausübung von Aktionärsrechten aufgrund von aktienrechtlichen Vorschriften erforderlich sind. Hingegen ist eine Verwendung von Daten über das Stimmverhalten im Zusammenhang mit dem Arbeitsverhältnis höchstens bei Geschäftsleitungsmitgliedern zu rechtfertigen. Insgesamt ist vor allem zu fordern, dass Transparenz über die vorgenommenen Bearbeitungen geschaffen wird.

Das Aktienrecht sieht zugunsten der Aktionäre eine Anzahl von Beteiligungsrechten vor. Dazu gehören insbesondere das Stimmrecht an der Generalversammlung (GV) sowie das Recht, an der GV unter bestimmten Voraussetzungen Verhandlungsgegenstände zu traktandieren. In der Folge wird bezüglich dieser Beteiligungsrechte untersucht, inwiefern sie eine Bearbeitung von Personendaten der Aktionärinnen und Aktionäre erfordern bzw. rechtfertigen können.

Erfassung des Stimmverhaltens

Wird das Stimmverhalten an der GV so erfasst, dass ermittelt werden kann, wie ein einzelner Aktionär gestimmt hat, so sind dies Angaben, die sich auf einen bestimmten oder zumindest bestimmbaren Aktionär beziehen. Damit handelt es sich um Personendaten im Sinne des DSG.

Das Aktienrecht äussert sich zur Form der Stimmabgabe an der GV nicht. Gängig sind sowohl die öffentliche Stimmabgabe durch Handzeichen als auch die schriftliche Stimmabgabe. Sofern die Statuten keine entsprechende Regelung enthalten, bestimmt der Verwaltungsrat (VR) das Abstimmungsprozedere, da in erster Linie er für die Durchführung der GV verantwortlich ist. Denkbar ist zudem, dass die GV selbst beschliesst, eine bestimmte Abstimmung öffentlich oder schriftlich und geheim durchzuführen. Der Aktionär hat – soweit die Statuten der AG dies nicht vorsehen – keinen aktienrechtlichen Anspruch auf schriftliche und absolut geheime (d.h. eine nicht nur gegenüber dem Aktionariat, sondern auch gegenüber dem VR geheime) Stimmabgabe.

Als Rechtfertigungsgrund für eine Erfassung des Stimmverhaltens kann die AG namentlich geltend machen, dass es ihr im Falle einer Anfechtungsklage oder einer Stimmrechtsklage bzw. im Rahmen eines Prozesses möglich sein muss, zu beweisen, wie der klagende Aktionär gestimmt hat. Nach bundesgerichtlicher Rechtsprechung sind nämlich nur diejenigen Aktionäre klageberechtigt, die dem fraglichen GV-Beschluss nicht zugestimmt haben.

Traktandierungsrecht

Aktionäre, die Aktiennennwerte in einer gewissen Höhe vertreten, können die Traktandierung eines Verhandlungsgegenstandes verlangen. Sie haben dabei gegenüber der Gesellschaft die Erreichung der gesetzlichen Quoren darzulegen. Dies erfordert die eindeutige Identifikation der antragsstellenden Aktionäre. Der Nachweis kann nur erbracht werden, indem die betreffenden Gesellschafter sich – unter Angabe des von ihnen vertretenen Aktienkapitals – direkt gegenüber der Gesellschaft zu erkennen geben beziehungsweise eine entsprechende schriftliche Vollmacht zu Gunsten eines Stimmrechtsvertreters erteilen, die von diesem der AG vorzulegen ist. Das betroffene Unternehmen benötigt die fraglichen Informationen zur Feststellung der rechtskonformen Ausübung des Traktandierungsrechts. Die aktienrechtliche Regelung verlangt damit zwingend die fragliche Datenbearbeitung.

Stimmrechtsvertretung

Das Aktienrecht lässt die Vertretung des Aktionärs in der GV durch einen Vertreter grundsätzlich zu. Es kennt drei Formen der institutionellen Stimmrechtsvertretung: den Organ-, den unabhängigen Stimmrechts- sowie den Depotvertreter. Die institutionellen Stimmrechtsvertreter sind dazu verpflichtet, der Gesellschaft Anzahl, Art, Nennwert und Kategorien der von ihnen vertretenen Aktien bekannt zu geben. Diese Informationen sind wiederum durch den Vorsitzenden der Versammlung der anwesenden Aktionäre weiterzugeben und im Protokoll der GV festzuhalten.

Der Stimmrechtrechtsvertreter hat demnach gegenüber der AG den Nachweis zu erbringen, dass einer oder mehrere Aktionäre ihn beauftragt haben, sie in der GV zu vertreten. Die einfache Schriftlichkeit der Vollmacht ist gemäss herrschender Lehre Gültigkeitserfordernis. Sie dient der einwandfreien Legitimation des Vertreters gegenüber der Gesellschaft und gegebenenfalls andern GV-Teilnehmern.

Der institutionelle Stimmrechtsrechtsvertreter ist gesetzlich dazu verpflichtet, den Weisungen des Aktionärs grundsätzlich Folge zu leisten. Die überwiegende Lehrmeinung geht jedoch davon aus, dass diese Verpflichtung lediglich das Innenverhältnis zwischen Vertreter und Vertretenen betreffe. Die AG sei nicht dazu angehalten, den Stimmrechtsvertreter in seinem Abstimmungsverhalten zu überwachen.

Für das Unternehmen ist es im Hinblick auf einen allfälligen Anfechtungsprozess lediglich von Bedeutung zu wissen, wie der institutionelle Stimmrechtsvertreter abgestimmt hat, nicht aber welcher Aktionär ihm welche Weisungen gegeben hat. Das Anbringen von Weisungen durch den Aktionär auf der Vollmachtsurkunde selbst erscheint demnach unter dem Blickwinkel des Gesellschaftsrechts nicht zwingend notwendig. Es spricht also nichts dagegen, die Weisungen auf einem separaten Formular zu erteilen, das im Besitz des Stimmrechtsvertreters verbleibt.

Darüber hinaus stellt sich die Frage, ob die Gesellschaft berechtigt ist, die Herausgabe der schriftlichen Weisungen zu verlangen. Aus datenschutzrechtlicher Sicht besteht dafür kein gesetzlicher Rechtfertigungsgrund. Zudem sind keine Interessen der AG als Ganze ersichtlich, die jene des einzelnen Aktionärs überwiegen. Nur wenn der Aktionär bereit ist, diese Angaben freiwillig offen zu legen, dürfen sie von der AG beschafft und bearbeitet werden.

Aktionärinnen und Aktionäre als Arbeitnehmende

Die Pflichten des Arbeitgebers bei der Bearbeitung von Personendaten der Arbeitnehmenden sind im Arbeitsvertragsrecht geregelt. Demnach darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Darüber hinaus wird auf die Bestimmungen des DSG verwiesen.

Das Stimmverhalten des Aktionärs darf zwar, wie oben ausgeführt, grundsätzlich an der GV erfasst werden. Hingegen ist es aus datenschutzrechtlicher Sicht unzulässig, Angaben zum Stimmverhalten im Zusammenhang mit dem Arbeitsverhältnis zu verwenden, wenn der Arbeitnehmer auch gleichzeitig Aktionär ist. Aus der Perspektive des datenschutzrechtlichen Transparenzgebotes wäre es daher sinnvoll, dass sich der Arbeitgeber explizit vertraglich dazu verpflichtet, Personendaten aus dem Aktionärsverhältnis nicht mit Bezug auf das Arbeitsverhältnis zu bearbeiten.

Diese Feststellung gilt grundsätzlich auch für Geschäftsleitungsmitglieder. Da aber sowohl deren Stimmverhalten wie auch deren Tätigkeit am Arbeitsplatz die Unternehmenspolitik der AG wesentlich bestimmen, stehen beide Bereiche bei dieser Kategorie von Arbeitnehmern in einem direkten Zusammenhang. Zudem haben die Aktionäre ein überwiegendes Interesse daran, das Stimmverhalten und damit auch die Positionen der Geschäftsleitungsmitglieder zu kennen. In diesen Fällen kann also die Verwendung von Angaben über das Stimmverhalten unter Umständen zu rechtfertigen sein. Es ist auch hier ratsam, diese Datenbearbeitung im Arbeitsvertrag vorzusehen.

Zweckgebundene Datenbearbeitung zulässig

Im Zusammenhang mit den Datenbearbeitungen, die im Rahmen der Ausübung dieser Rechte erforderlich sind, ist immer zu berücksichtigen, dass diese Aktionärsrechte Ausfluss eines vertragsähnlichen Verhältnisses sind, welches auf freiwilliger Basis eingegangen wurde. Damit unterwerfen die Betroffenen sich bestimmten Rechtsvorschriften, welche die Bearbeitung ihrer Personendaten legitimieren können.

Zusammenfassend lässt sich festhalten, dass das Erfassen des Stimmverhaltens (und anderer Personendaten im Zusammenhang mit der Ausübung von aktienrechtlichen Beteiligungsrechten) durch die AG zulässig ist, soweit ein Rechtfertigungsgrund vorliegt. In der Regel wird sich dieser in einer Bestimmung im Aktienrecht finden. Die Datenbearbeitung muss sodann zweckgebunden erfolgen, d.h. nur zu dem Zweck, der gesetzlich vorgesehen ist. Eine Verwendung zu einem anderen Zweck ist nicht möglich, es sei denn, ein neuer Rechtfertigungsgrund liegt vor.

Dies kann im Einzelfall beispielsweise das überwiegende Interesse des Aktionariats am Stimmverhalten der Mitglieder der Geschäftsleitung oder des Verwaltungsrats sein. Es zeigt u.a. die Strategien der Unternehmenspolitik auf und hat einen direkten Einfluss auf den künftigen Geschäftsgang der AG.

Der VR trägt die Verantwortung dafür, dass die an der GV erfassten Personendaten in der Folge datenschutzkonform bearbeitet werden. Er muss die erforderlichen organisatorischen oder technischen Massnahmen treffen bzw. anordnen und Weisungen zu den weiteren Bearbeitungsmodalitäten (Zugriffsberechtigungen, Aufbewahrungsdauer usw.) erlassen. Das Transparenzprinzip verlangt, dass die Aktionäre über diese Datenbearbeitungen informiert werden.

9.2 Beitritt zu einer Selbstregulierungsorganisation

Bei der Frage, ob für die Mitgliedschaft zu einer Selbstregulierungsorganisation gemäss Geldwäschereigesetz die Unterzeichnung eines bestimmten Formulars resp. Vollmacht verlangt werden könne, handelt es sich nicht primär um ein datenschutzrechtliches Problem, sondern vielmehr um die Frage, ob dies für die Erfüllung der Pflichten gemäss dem Geldwäschereigesetz nötig ist. Die Selbstregulierungsorganisation ihrerseits untersteht der Aufsicht der Kontrollstelle für die Bekämpfung der Geldwäscherei, die zur Beantwortung der Frage auch notwendigen Fachkenntnisse besitzt. Betroffenen Personen steht es frei, sich einer anderen Selbstregulierungsorganisation oder der Kontrollstelle zu unterstellen.

Uns wurde die Frage unterbreitet, ob für die Mitgliedschaft zu einer Selbstregulierungsorganisation die Unterzeichnung eines Formulars «Vollmacht betreffend die Erfüllung der Pflichten nach Art. 9 und 10 GwG» (GwG = Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor) verlangt werden könne. Diesbezüglich handelt es sich nicht primär um ein datenschutzrechtliches Problem. Aufgrund der allgemein im Zusammenhang mit dem GwG stattfindenden Datenbearbeitungen erlaubte sich der EDSB folgende Bemerkungen:

Vorliegend ging es vor allem um die Frage, ob für die Erfüllung der Pflichten gemäss dem GwG (Meldepflicht und Vermögenssperre) die Erteilung einer Vollmacht nötig ist. Aus dem Wortlaut der entsprechenden Bestimmungen (Art. 9 und 10 GwG) geht dies nicht hervor. Auf der anderen Seite muss eine Selbstregulierungsorganisation gemäss dem GwG darüber wachen, dass die ihr angeschlossenen Finanzintermediäre ihre Pflichten nach dem zweiten Kapitel des GwG (darunter auf Art. 9 und 10) einhalten. Die Selbstregulierungsorganisation ihrerseits untersteht der Aufsicht der Kontrollstelle für die Bekämpfung der Geldwäscherei. Die Kontrollstelle genehmigt auch die von den Selbstregulierungsorganisationen erlassenen Reglemente. Aus diesem Grund, aber auch weil die Kontrollstelle betreffend das GwG die notwendigen Fachkenntnisse hat, ersuchten wir die betroffene Person, ihre Anfrage direkt der Kontrollstelle zu unterbreiten.

Wir wiesen die betroffene Person darauf hin, dass es ihr freistehe, sich einer anderen Selbstregulierungsorganisation oder aber der direkten behördlichen Kontrolle (d.h. der Kontrollstelle) zu unterstellen.

10. Statistik und Forschung

10.1 Rolle des Datenschutzes in der Statistik

Im Zusammenhang mit einer Anfrage des Bundesamtes für Statistik haben wir es begrüsst, dass dieses Amt sich Datenschutzgrundsätze geben will. Was den Inhalt der präsentierten Grundsätze betrifft, scheint uns in erster Linie mit Bezug auf die Klarheit des Verhältnisses zwischen administrativen und statistischen Datenbearbeitungen noch Handlungsbedarf zu existieren.

Im Anschluss an die Verabschiedung der Datenschutzgrundsätze des Bundesamts für Statistik durch dessen Geschäftsleitung wurden wir vom Datenschutzberater dieses Amtes um eine Stellungnahme angegangen. Wir haben sowohl die Initiative an sich als auch die Tatsache begrüsst, dass die Grundsätze zum Teil recht konkret und damit auch umsetzbar formuliert sind.

Auf der anderen Seite haben wir bemängelt, dass zum Verhältnis zwischen administrativen und statistischen Datenbearbeitungen keine greifbaren Überlegungen gemacht wurden, obwohl dieses Verhältnis für den Datenschutz in der Statistik zentral ist. Im Gegenteil, im Dokument «Datenschutzgrundsätze» steht die unseres Erachtens bedenkliche Formulierung, wonach die Bürger zunehmend bereit seien, «die Verknüpfung von Daten und ihre multifunktionale Verwendung für statistische und administrative Zwecke hinzunehmen», falls «der Datenschutz gewährleistet wird». Diese beiden Arten von Datenbearbeitungen sind jedoch aus der Optik des Datenschutzes vollständig gegensätzlich, und eine Klarstellung ihres Verhältnisses ist für die Statistik unseres Erachtens dringend. Denn in den vergangenen Jahren ist vermehrt zu beobachten, dass die Statistik als Treiber für eine Vermehrung und Intensivierung administrativer Datenbearbeitungen wirkt. Zwei Beispiele seien dafür genannt: Zunächst gibt es seit der Einführung des eidgenössischen Gebäude- und Wohnungsregisters für die Einwohnerkontrollbehörden die Verpflichtung, jeden Einwohner einer Gebäudenummer und einer Wohnungsnummer zuzuordnen. Als zweites Beispiel mag der sogenannte eidgenössische Personenidentifikator dienen, welcher Erleichterungen beim Verknüpfen administrativer Register auch und gerade für den administrativen Bereich mit sich bringt. Dass eine solche Verknüpfbarkeit bedeutend grössere Gefahren für die Persönlichkeitsrechte beinhaltet als blosse Statistikbearbeitungen, liegt auf der Hand. Tatsache ist aber, dass hier unter dem Zeitdruck der Volkszählung 2010 eine Infrastruktur geschaffen wird, welche z.B. flächendeckende Rasterfahndungen erlauben könnte. Daran ändert im Grunde auch nichts, dass heute von «koordinierten sektoriellen Personenidentifikatoren» die Rede ist. Statt eines Verknüpfungselements ohne klaren Verwendungszweck werden so einfach mehrere geschaffen, ohne deren Zwecke vorgängig genügend präzise zu definieren.

Angesichts solcher Auswirkungen auf den administrativen Bereich haben wir angeregt, dass das Bundesamt für Statistik in einem Konzept darstellt, wie in Zukunft verhindert werden kann, dass administrative Tätigkeit durch die Statistik beeinflusst wird.

10.2 Forschungsprojekte und klinische Studien: Konsequenzen einer widerrufenen Einwilligung

Die Teilnahme an Forschungsprojekten oder Studien ist immer freiwillig und kann jederzeit widerrufen werden. Widerruft der Teilnehmer seine Einwilligung, so kann er davon ausgehen, dass seine Daten vernichtet werden, es sei denn, er habe in die Weiterverwendung seiner Daten ausdrücklich eingewilligt. Wurde die Frage nicht geregelt, so darf nicht stillschweigend davon ausgegangen werden, der Teilnehmer sei mit der Weiterverwendung seiner Daten einverstanden. Da beim Widerruf der entsprechenden Einwilligung die Daten nicht mehr für das Forschungsprojekt oder die Studie zur Verfügung stehen, ist es ratsam, Daten immer so früh wie möglich zu anonymisieren. Anonymisierte Daten sind keine Personendaten mehr, da sie nicht mehr zugeordnet werden können.

Die Teilnahme an einem Forschungsprojekt oder an einer Studie erfolgt immer freiwillig. Die Einwilligung zur Teilnahme kann jederzeit ohne Angabe von Gründen widerrufen werden. Die Einwilligung, die in der Regel schriftlich erfolgen muss, ist nur gültig, wenn der Teilnehmer vorher über Ziel und Zweck des Projektes und die darin vorgesehenen Datenbearbeitungen genügend aufgeklärt worden ist. In der Praxis werden dazu Informationsblätter abgegeben und Informationsgespräche geführt. Wir wurden durch ein Institut angefragt, welche Konsequenzen der Widerruf einer solchen Einwilligung habe.

Das informationelle Selbstbestimmungsrecht soll den Bürger in die Lage versetzen, über seine Daten selber zu bestimmen. Es ermöglicht ihm, den Überblick über die Bearbeitung seiner Daten zu behalten. Dasselbe gilt, wenn er die Einwilligung in die Bearbeitung seiner Daten gibt. Neben der Freiwilligkeit ist die jederzeitige Widerrufbarkeit eine Grundanforderung an Einwilligungserklärungen.

Damit eine Einwilligung gültig ist, muss der Betroffene die Tragweite (Umfang und Zweck) der Einwilligung erkennen können, was als «informed consent» bezeichnet wird. Ausschlaggebend ist dabei die Einhaltung des Transparenzprinzips bei der Formulierung von Einwilligungsklauseln und Informationsformularen. Die an einer Studie teilnehmende Person muss ausführlich über Zweck und Ablauf der Studie informiert werden. Ebenso müssen alle Datenbearbeitungen und Datenschutzvorkehren (Über-

mittlung, Speicherung, Vernichtung der Daten, Schutz vor unbefugtem Zugriff Dritter, allenfalls vorgesehene Pseudonymisierungs- und Anonymisierungsmassnahmen usw.) erläutert werden. Zudem muss ausdrücklich auf die Freiwilligkeit der Einwilligung und die jederzeitige Widerrufsmöglichkeit hingewiesen werden.

Widerruft jemand seine Einwilligung zur Teilnahme an einer Studie, so kann er davon ausgehen, dass seine Daten vernichtet werden. Es empfiehlt sich, zur Sicherheit eine Bestätigung der Löschung der Daten zu verlangen.

Selbstverständlich kann sich der Teilnehmer jederzeit damit einverstanden erklären, dass seine bis zum Zeitpunkt des Widerrufs im Rahmen der Studie bearbeiteten Daten weiter verwendet werden. Ein entsprechender Passus sollte in der Einwilligungserklärung figurieren. Dieses Einverständnis kann er gestützt auf sein Recht zur informationellen Selbstbestimmung ebenfalls jederzeit widerrufen. Ist die Frage nicht geregelt, so darf nicht ohne weiteres angenommen werden, dass die Daten weiter verwendet werden dürfen. Kein Problem stellt sich, wenn die Daten anonymisiert wurden. Dies ist der Fall, wenn alle Merkmale entfernt wurden, welche eine Identifizierung der betroffenen Person ermöglichen (vgl. unseren 3. Tätigkeitsbericht 1995/96, Abschnitt I.9.3). Der Teilnehmer kann keine Löschung von nicht mehr identifizierbaren Daten verlangen.

Wurden die Daten lediglich pseudonymisiert, so können sie durch Personen, die Zugriff auf die entsprechende Relationstabelle mit den Zuordnungsfunktionen haben, jederzeit wieder in personenbezogene Daten zurückgeführt werden. Pseudonyme Daten können durch Löschen der Zuordnungsfunktionen anonymisiert werden. Widerruft ein Teilnehmer seine Teilnahme an der Studie, so können seine pseudonymen Daten wie folgt behandelt werden: Vernichtung der Zuordnungsfunktion, wodurch die Daten in anonymer Form für die Studie nutzbar bleiben, oder Vernichtung der Zuordnungsfunktion und der dazugehörenden Daten. Letzteres sollte im Interesse der Studie bzw. des Forschungsprojektes nur auf ausdrücklichen Wunsch des Betroffenen erfolgen, da in diesem Fall die Daten für die Studie bzw. das Forschungsprojekt verloren gehen. Diese Gefahr kann in der Praxis minimiert werden, indem die Daten immer so früh wie möglich vollständig anonymisiert werden oder, wenn eine Zuordnung zwar noch möglich, aber nicht unbedingt personenbezogen sein muss, das Pseudonym vernichtet und durch eine Identifikation ohne Zuordnungsfunktion ersetzt wird.

Schliesslich sei noch darauf hingewiesen, dass solange Daten im Rahmen von Forschungsprojekten und Studien personenbezogen bearbeitet werden, dem Teilnehmer selbstverständlich auch jederzeit das datenschutzrechtliche Auskunftsrecht zusteht.

10.3 Angaben von Gesundheitsdaten in einem Statistikfragebogen

Arbeitsgemeinschaften von Leistungserbringern im Gesundheitswesen sammeln Daten, welche den Beteiligten einen Vergleich der erbrachten Leistungen ermöglichen. Bei der Prüfung des Projektes der ASF (Arbeitsgemeinschaft Schweizer Frauenkliniken) ergaben sich neben den «klassischen» Problemen des Datenschutzes auch Fragestellungen, die mehrheitlich auf Missverständnisse beim Umgang mit datenschutzrechtlichen Fragen beruhen.

Nach dem Hinweis eines Spitals analysierten wir die Datenerhebung der ASF. Auf einem Formular wurden Personendaten zusammen mit medizinischen und statistischen Daten erfasst. Weitergeleitet an eine dritte Stelle, wurden die Daten zum Zweck der Statistik und Qualitätskontrolle weiterverarbeitet. Die Methode der Erhebung ist vergleichbar mit dem bereits in unserem 9. Tätigkeitsbericht 2001/2002 in Abschnitt 5.1.6 beschriebenen System. Es soll an dieser Stelle nicht weiter darauf eingegangen werden.

Erwähnenswert erscheinen uns aber drei Fragen, die sich während der Untersuchung der ASF-Lösung stellten.

Es stellt sich zunächst die Frage, ob das schriftliche Einverständnis der Chefärzte für eine Weitergabe von Gesundheitsdaten an Dritte genügt. Die Antwort ist klar nein. Das schriftliche Einverständnis ist keine genügende Legitimation für eine nicht anonymisierte Weitergabe von besonders schützenswerten Personendaten an Dritte.

Ferner ist zu klären, ob ein sorgfältiger Umgang mit Gesundheitsdaten ausreicht oder ob es mehr braucht. Dies hängt davon ab, wie sich die Sorgfalt gestaltet. Sie kann kein Ersatz sein für ein genau geprüftes und geregeltes Verfahren im Umgang mit Patientendaten. Erst nach einer umfassenden Analyse der gesetzlichen Grundlagen, der Bedürfnisse und des Zwecks der Datenbearbeitung kann eine Lösung entworfen werden, deren Einführung und Nutzung dann mit Sorgfalt erfolgen sollte.

Schliesslich bleibt noch die Frage, warum eine 20-jährige Periode ohne datenschutzrelevante Ereignisse nicht als Beleg dafür gelten kann, dass der Datenschutz eingehalten wird. Es ist erfreulich, wenn ein Unternehmen während einer 20-jährigen Periode keine datenschutzrelevanten Ereignisse zu beklagen hat. Häufig wird aber Datenschutz mit Datensicherheit oder auch Informatiksicherheit verwechselt. Auch wenn Daten, welche über gut geschützte Netze transportiert und auf hochgesicherten Systemen gelagert und verarbeitet werden, nie verloren gingen oder von einem «Cracker» manipuliert wurden, kann eine Datenschutzverletzung vorliegen. Zum Beispiel dann, wenn die Bearbeitung der Daten nicht rechtmässig und verhältnismässig ist und nicht nach Treu und Glauben erfolgt, oder wenn die Personendaten nicht mehr zu dem ursprünglich angegebenen Zweck bearbeitet werden.

11. International

11.1 Europarat

11.1.1 Entwurf eines Protokolls über genetische Untersuchungen beim Menschen

Der Europarat hat den ersten Teil des Protokolls interessierten Kreisen zur Stellungnahme unterbreitet. Das Ergebnis der Vernehmlassung liegt vor. Die Mitglieder der zuständigen Arbeitsgruppe erhielten nochmals Gelegenheit, sich dazu zu äussern.

Das Protokoll über genetische Untersuchungen beim Menschen ist eines der Zusatzprotokolle zum Übereinkommen des Europarates über Menschenrechte und Biomedizin (Konvention von Oviedo). Der Geltungsbereich des Protokolls soll genetische Untersuchungen im medizinischen Bereich sowie im Arbeits- und Versicherungsbereich regeln (mehr dazu in unserem 10. Tätigkeitsbericht 2002/2003, Abschnitt 11.1.4). Mit dem Protokoll sollen Diskriminierungen aufgrund des Erbgutes vermieden werden.

Der erste Teil des Protokolls betrifft den medizinischen Bereich. Die Mitgliedsstaaten sowie weitere interessierte Kreise haben sich dazu geäussert. In der Folge wurde der Arbeitsgruppe nochmals die Möglichkeit gegeben, zu den Vernehmlassungsresultaten Stellung zu nehmen.

Aus datenschutzrechtlicher Sicht wichtig ist, dass die bereits existierende Datenschutzgesetzgebung des Europarates im Protokoll Berücksichtigung findet. Insbesondere sei auf die diversen Europarats-Empfehlungen verwiesen. Die Empfehlungen haben die Bearbeitung von Gesundheitsdaten im Allgemeinen und genetische Untersuchungen im Speziellen zum Inhalt.

Die Bearbeitung von genetischen Personendaten verlangt vor allem erhöhte Anforderungen an die Datensicherheit und Vertraulichkeit. Im Protokoll ist daher festzuhalten, unter welchen Voraussetzungen biologisches Material bzw. die damit zusammenhängenden Informationen anonymisiert oder pseudonymisiert werden.

Es ist vorgesehen, dass der erste Teil des Protokolls in den diversen Gremien des Europarates nochmals überarbeitet wird. In der Berichtsperiode fand zudem die zehnte Tagung der Arbeitsgruppe in Strassburg statt. Ziel der Tagung war es, den zweiten Teil des Protokolls auszuarbeiten, welcher genetische Untersuchungen im Arbeitsbereich regeln soll.

11.1.2 Arbeiten der CJPD: Chipkarte und Biometrie

Die Projektgruppe für den Datenschutz (CJPD) versammelte sich vom 24. bis zum 28. November 2003 zum letzten Mal und verabschiedete einen Entwurf zu Leitgrundsätzen über den Datenschutz betreffend Chipkarten.

Die CJPD verabschiedete anlässlich ihrer 41. und letzten Tagung einen Entwurf zu Leitgrundsätzen über den Schutz der Personendaten in Zusammenhang mit Chipkarten. Darin werden die Grundsätze aufgeführt, welche zur Verbesserung des Datenschutzes bei der Verwendung der Chipkartentechnologie zu berücksichtigen sind. Die vom Ausschuss ausgearbeiteten Leitgrundsätze sollen keine erschöpfende Lösung für alle Datenschutzprobleme bieten, welche mit der Verwendung von Chipkarten zusammenhängen. Die Chipkarten sind immer in ein breiteres Informationssystem integriert. Die Wirksamkeit des Schutzes hängt von zahlreichen Faktoren und Voraussetzungen sowie vom Verhalten der am System beteiligten Personen ab. Die Leitgrundsätze definieren die Basisregeln, die beim Beschaffen und bei der Bearbeitung von Personendaten mit Hilfe einer Chipkarte zu beachten sind. Der Schwerpunkt liegt dabei insbesondere auf den Grundsätzen der Zweckbindung, der Verhältnismässigkeit und der Transparenz (Informationspflicht gegenüber den Benutzern). Die CJPD prüfte ausserdem in der ersten Lesung einen Entwurf zu Leitgrundsätzen über den Datenschutz bei der Verwendung von biometrischen Daten. Der Europarat hat indessen aus haushaltspolitischen Gründen beschlossen, die Tätigkeiten der CJPD nach 20 Jahren zu beenden. Die Arbeit der CJPD – insbesondere die Aktivitäten über die Biometrie – werden vom Beratenden Ausschuss (T-PD) weitergeführt. Die Experten haben dies zur Kenntnis genommen und die abrupte Auflösung des Gremiums, das massgeblich zur Entwicklung des Datenschutzes in Europa beigetragen hat und ein Laboratorium für Staaten bildete, welche keine Datenschutzgesetzgebung kannten, bedauert. So forderten die Sachverständigen den Europarat auf, zu untersuchen, inwieweit diejenigen Staaten, welche das Übereinkommen 108 nicht ratifiziert haben, an den Arbeiten der Übereinkommensparteien im Rahmen des T-PD beteiligt werden können.

11.1.3 Arbeiten des T-PD: Arbeitsprogramm und grenzüberschreitender Datenfluss

Der Beratende Ausschuss des Übereinkommens 108 (T-PD) hielt vom 27. bis zum 29. November 2003 seine 19. Tagung ab. Der Ausschuss verabschiedete sein Arbeitsprogramm sowie die Prioritäten für die nächsten Jahre. Ausserdem prüfte er den Entwurf einer Stellungnahme betreffend die regelmässige und umfassende Übermittlung von Personendaten an einen Drittstaat, der über kein angemessenes Datenschutzniveau verfügt.

Der T-PD nahm unter schweizerischem Vorsitz das Arbeitsprogramm und die Prioritäten für die nächsten Jahre an. Er wird sich vorrangig mit der Biometrie befassen und den vom CJPD vorbereiteten Entwurf abschliessen. Danach wird er sich mit den Rechten der betroffenen Personen auseinander setzen und namentlich einen Leitfaden für die betroffenen Personen ausarbeiten. Der Leitfaden soll einen Überblick über den Rechtsrahmen des Datenschutzes vermitteln sowie die Rechte und Pflichten der betroffenen Personen und die Geltendmachung ihrer Rechte und Ansprüche in allen Konventionsparteien aufführen. Der Ausschuss wird sich daneben mit dem angemessenen Schutzniveau von Drittstaaten befassen und dazu Stellungnahmen ausarbeiten. Schliesslich soll er die Anwendung der Datenschutzgrundsätze auf das Internet prüfen.

Der T-PD untersuchte den Entwurf einer Stellungnahme betreffend die regelmässige und umfassende Übermittlung von Personendaten an einen Drittstaat, welcher kein angemessenes Schutzniveau garantiert. In der Stellungnahme werden unter anderem die minimalen Rahmenbedingungen beschrieben, die erfüllt sein müssen, wenn ein Datenbearbeitungsverantwortlicher aufgrund von Verpflichtungen einem Drittstaat, der über kein angemessenes Schutzniveau verfügt, Daten übermitteln muss. Allerdings erzielte der Ausschuss keinen Konsens zum Entwurf und einigte sich darauf, später erneut auf die Frage zurückzukommen. Daneben verabschiedete der T-PD eine Änderung der Geschäftsordnung mit dem Ziel, die Arbeitsweise und die Beschlussfassung zu verbessern. Frau W. Kotschy aus Österreich wurde als Datenschutzbeauftragte des Europarates wiedergewählt.

11.2 Europäische Union

11.2.1 Europäische Arbeitsgruppe über die Behandlung von Klagen und über den Informationsaustausch

Die Arbeitsgruppe, in der wir mitwirken, hat anlässlich der Oktobertagung von 2003 im Wesentlichen konkrete Fälle geprüft, um die verschiedenen Kontrollmethoden zu vergleichen, welche die Datenschutzbehörden bei der Behandlung von Klagen anwenden. Einen weiteren Schwerpunkt bildete die Erweiterung der Arbeitsgruppe und die dadurch bedingte Überarbeitung ihrer Funktionsweise.

Auf der Grundlage des von der Europäischen Konferenz der Datenschutzbeauftragten erteilten Mandates versammelte sich die Europäische Arbeitsgruppe «Behandlung von Klagen und Informationsaustausch» (Complaints handling Workshop) am 23. und 24. Oktober 2003 in Rom. Wir beteiligten uns an den Arbeiten der Gruppe, welche die unterschiedlichen Behandlungsmethoden für Klagen, die bei den Datenschutzbehörden eingehen, prüfen und die gegenseitige Zusammenarbeit fördern soll.

Anlässlich dieser Tagung setzte die Arbeitsgruppe die Untersuchungen fort, welche sie auf den vorhergehenden Tagungen in Angriff genommen hatte. Während diese den Aufsichtsmethoden gewidmet waren, welche die Datenschutzbehörden gemäss ihren gesetzlichen Kompetenzen einsetzen, wurden anlässlich der Tagung in Rom diese Methoden anhand der Prüfung konkreter Fälle veranschaulicht. So wurden verschiedene Fälle untersucht, welche die Bearbeitung von biometrischen Daten, grenzüberschreitende Datenflüsse, Videoüberwachung am Arbeitsplatz oder das Aufbewahren von Daten durch Kreditinformationsstellen betrafen. Dabei wurden die Vor- und Nachteile der jeweiligen Aufsichtsmethoden sowie die unterschiedlichen Resultate verdeutlicht. Ausserdem zeigte sich, dass in jedem Einzelfall unbedingt geklärt werden muss, ob die Datenschutzbehörde im Rahmen ihrer Aufsichts- und Beratungskompetenzen handelt.

Angesichts der unterschiedlichen Ansätze und Ergebnisse bei der Behandlung von Klagen wies die Arbeitsgruppe auf die Wichtigkeit des Informations- und Erfahrungsaustausches unter den Datenschutzbehörden hin. So bekräftigte sie die zentrale Rolle des Informatiksystems CIRCA (Communication & Information Resource Centre Administrator). Dieses gesicherte Extranetsystem, das mit dem IDA-Programm (Interexchange of Data between Administrations, Informationsaustausch zwischen öffentlichen Verwaltungen) der Europäischen Kommission verknüpft ist, bildet eine Plattform für den Informationsaustausch über die Ergebnisse der durchgeführten Kontrollen

und über Ratschläge und Lösungen, die für ähnliche Datenschutzprobleme gefunden wurden.

Schliesslich befasste sich die Arbeitsgruppe insbesondere mit der Zunahme der Mitgliederzahl. Anfangs bestand sie aus rund zwanzig Teilnehmern, den Vertretern der Europäischen Union und bestimmter Staaten mit einem angemessenen Datenschutzniveau, so auch der Schweiz. Mit der Ankunft von neuen Teilnehmern (Tschechien, Slowakei, Slowenien, Litauen, Polen usw.) wurde die Gruppe stark erweitert. Heute zählt sie knapp fünfzig Mitglieder. Eine Neuregelung ihrer Arbeitsweise wird damit unumgänglich. Die Arbeitsgruppe möchte einerseits den dem Erfahrungsaustausch förderlichen informellen Rahmen beibehalten, muss aber andererseits die Interventionen der Teilnehmer besser organisieren und die Themenwahl – besonders für die laufenden Arbeiten der Gruppe der Europäischen Union betreffend Artikel 29 – besser koordinieren. Verschiedentlich wurde vorgeschlagen, einen Programmausschuss einzusetzen und mit den Folgearbeiten und der Verwaltung der anfallenden Themen zu beauftragen.

Die Arbeitsgruppe wird diese Tätigkeiten fortsetzen mit dem Ziel, die Zusammenarbeit unter den nationalen Kontrollbehörden im Rahmen der Untersuchung von Klagen und der Durchführung von Inspektionen zu verbessern. Die Reflexionen über die Funktionsweise der Arbeitsgruppe sollen ausserdem der nächsten Europäischen Konferenz der Datenschutzbeauftragten, die im April 2004 in Rotterdam tagt, vorgestellt werden.

11.2.2 Europäische Konferenz der Datenschutzbeauftragten

Die europäischen Datenschutzbeauftragten tagten am 3. und 4. April 2003 in Sevilla. Wir nahmen als Beobachter daran teil. Der schweizerische Vorschlag, die Konferenz sämtlichen Datenschutzbehörden der Staaten, welche das Übereinkommen 108 ratifiziert haben, zu öffnen, wurde von den Datenschutzbeauftragten positiv aufgenommen.

Die Europäische Konferenz der Datenschutzbeauftragten umfasst die Datenschutzbeauftragten der Länder der Europäischen Union. Die Mitgliedsstaaten des Europäischen Wirtschaftsraumes, die Beitrittskandidaten der Europäischen Union sowie die Schweiz werden als Beobachter eingeladen. Die Vertreter der Europäischen Kommission, des Europarates und der Datenschutz-Aufsichtsstelle von Europol beteiligten sich ebenfalls an den Arbeiten.

Die Konferenz der europäischen Datenschutzbeauftragten fand im Berichtsjahr unter dem Vorsitz der spanischen Datenschutzbehörde in Sevilla statt. Die Konferenz behandelte komplexe und aktuelle Fragen. So setzte sie sich mit der Rolle der Datenschutz-Aufsichtsbehörden in Europa auseinander, zog eine erste Bilanz zur Umset-

zung der Europäischen Richtlinie und prüfte den Stand des Datenschutzes in den EU-Beitrittskandidaten. Ausserdem befassten sich die Datenschutzbeauftragten mit dem Datenschutz in der Telekommunikation und im E-Marketing sowie mit Fragen des grenzüberschreitenden Datenflusses. Die Datenschutzbeauftragten forderten eine Neubeurteilung der Rolle und Ziele der nationalen Aufsichtsbehörden in einer Welt, in welcher der Einsatz von Informationstechnologien eine universale Dimension annimmt und in welcher das Recht auf Datenschutz mehr denn je massgeblich zur Lebensqualität beiträgt. Ein besonderer Akzent lag auf der erforderlichen Stärkung der internationalen Zusammenarbeit besonders hinsichtlich der grenzüberschreitenden Datenflüsse. Die Datenschutzbeauftragten betonten, dass die Dienstleistungsanbieter im Telekommunikationsbereich die notwendigen Mechanismen für den Schutz der Personendaten der Benutzer einführen sollten. Ausserdem bot die Konferenz Gelegenheit für eine Bilanz zu den Massnahmen, welche nach den Attentaten von September 2001 ergriffen worden waren. So betonten die Datenschutzbeauftragten, dass die Sicherheitsbedürfnisse und die Terrorismusbekämpfung einerseits und die Achtung des Privatlebens andererseits gegeneinander abgewogen werden müssen; diese Abwägung darf nicht zu Lasten des Datenschutzes gehen. Schliesslich plädierten wir dafür, dass die Konferenz über ihre Zukunft nachdenkt: Sie soll sich zu einer Konferenz entwickeln, der alle Aufsichtsbehörden der Vertragsparteien der Europaratskonvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten angehören. Die Konferenz hat diesen Vorschlag begrüsst.

11.3 OECD

11.3.1 Arbeitsgruppe über die Informationssicherheit und den Schutz der Privatsphäre (WPISP)

In den zwei Sitzungen der Arbeitsgruppe wurden die Implementierung der revidierten Richtlinien über die Informationssicherheit, die elektronische Authentifizierung, der Bericht über die Anwendungen von Biometrie und die Problematik des Spam debattiert. Schwerpunkt der Arbeiten der Arbeitsgruppe war für das zweite Jahr in Folge die Entwicklung einer globalen Sicherheitsstruktur. Dem Thema der globalen Sicherheit wurde auch eine speziell dafür einberufene Konferenz in Oslo gewidmet.

Die revidierten Sicherheitsrichtlinien der OECD wurden auch von der UNO übernommen. Aber auch nach der Veröffentlichung der Richtlinien ist der Stand der Implementierung bei den Mitgliedländern nicht ausreichend. Daher wird die Wichtigkeit der Vertrauensbildung bei der Bevölkerung in Sachen Sicherheit unterstrichen. Die Lösungs-

findung in Sachen Sicherheit und Datenschutz darf nicht auf den Benutzer abgewälzt werden. Dabei wird verlangt, dass Unternehmen bei der Entwicklung von Soft- und Hardware Sicherheits- und Datenschutzmassnahmen mitentwickeln.

In Sachen Authentifizierung und digitale Signaturen wurde der aktuelle Stand in den Mitgliedländern analysiert. Den Mitgliedländern wird empfohlen, Regulierungsbarrieren bei der internationalen Anerkennung von digitalen Signaturen zu vermeiden. Arbeiten in diesem Bereich sind intensiver mit anderen internationalen Organisationen zu koordinieren.

Der Bericht über die Anwendungen der Biometrie wurde veröffentlicht. Die Risiken für die Privatsphäre und Sicherheit stehen im Mittelpunkt, insbesondere die Problematik der Identifikation (identity thief). Die bereits vorhandenen biometrische technische Anwendungen der Biometrie sind im Bericht aufgezählt, und die Notwendigkeit der Definition von internationalen Standards wird hervorgehoben.

Die Arbeitsgruppe hat ausserdem ein Basisdokument zum Thema Spam erarbeitet, das als Grundlage für die Arbeiten in diesem Bereich dienen soll.

Für das zweite Jahr in Folge stand das Thema der globalen Sicherheit im Mittelpunkt der Arbeiten der Arbeitsgruppe. Abgesehen von der dafür speziell organisierten Konferenz in Oslo befasste sich die Arbeitsgruppe auch mit der internationalen Verkehrssicherheit. Dafür fand am 26. und 27. September 2003 eine Ad-hoc-Expertensitzung in London statt. Die Resultate dieser Ad-hoc-Sitzung wurden der Arbeitsgruppe WPISP vorgestellt. Danach sollten bereits existierende Informationssysteme bestmöglich genutzt und miteinander verknüpft werden. Das Datenvolumen soll auf die maschinenlesbaren Daten von Reisedokumenten beschränkt werden. Einige Staaten haben die Erstellung einer zentralen Datenbank vorgeschlagen, insbesondere für die Länder, die für eine eigene Datenbank finanziell nicht aufkommen können. Aber auch die Aufnahme von zusätzlichen Daten soll ermöglicht werden, sofern zwischenstaatliche bilaterale Verträge dies erlauben. Schliesslich wird auch eine international anerkannte Kontrollstelle für den Datenschutz und die Sicherheit zu bestimmen sein. Die WPISP-Arbeitsgruppe hat in dieser Angelegenheit einen Bericht in Aussicht gestellt, damit entschieden werden kann, ob gegebenenfalls in Sachen Verkehrssicherheit OECD-Empfehlungen herauszugeben sind. Die Mehrzahl der teilnehmenden Mitgliedstaaten anerkennt die Risiken, die mit einem raschen Vorgehen in dieser Angelegenheit verbunden sind, und bestimmt, dass in einen späteren Zeitpunkt noch zu entscheiden ist, ob die WPISP-Expertengruppe die Arbeiten in diesem Bereich fortführen sollte oder ob eine andere Organisation (IATA, ICAO) dafür geeigneter wäre.

An der am 13. und 14. Oktober 2003 in Oslo stattgefundenen Konferenz über die globale Sicherheit wurden verschiedenen Themen angeschnitten. Die Problematik der Entwicklung einer globalen Sicherheitsstruktur kann nicht ausschliesslich im Dialog zwischen Behörden und Wirtschaft gelöst werden, auch die Bürger sind in diesen Dialog einzubeziehen. Gleichzeitig sind in Sachen Sicherheit auch Ethik- und Demokratieprinzipien zu berücksichtigen. Denn die Abwägung zwischen den Sicherheitsbedürfnissen und den demokratischen Prinzipien ist eine ständige Gradwanderung. Daher darf die Einschränkung von demokratischen Rechten nur – und sofern tatsächlich erforderlich – innerhalb einer politisch-gesellschaftlichen Auseinandersetzung erfolgen.

Nach dem Abschluss der Konferenz ist erkennbar, dass in der aktuellen Sicherheitsdebatte innerhalb der OECD minimale Anliegen zum Schutz der Privatsphäre zu wenig Bedeutung finden. Obwohl unbestritten bleibt, dass Sicherheitsmassnahmen insbesondere für den Schutz der Informationssysteme erforderlich sind, darf der legitime Rahmen von staatlichen Überwachungen nicht verletzt werden.

11.4 Weitere Themen

11.4.1 Internationale Konferenz der Datenschutzbeauftragten

Die XXV. Internationale Konferenz der Datenschutzbeauftragten fand vom 9. bis zum 11. September 2003 in Sydney statt. An der Konferenz beteiligten sich Delegationen aus 35 Staaten und vier Kontinenten. Die Konferenz legte den Schwerpunkt auf die praktischen Aspekte des Datenschutzes und deren Folgen für die Einzelpersonen, die Verwaltungen und die Unternehmen. Zum Abschluss wurden fünf Entschliessungen verabschiedet.

Der erste, offene Konferenzteil war neben den Datenschutzbeauftragten auch den Vertretern der Industrie, des Dienstleistungssektors, der öffentlichen Verwaltungen, der Verbraucher, der Forschung und der akademischen Welt zugänglich. Die Konferenz legte den Akzent auf die praktischen Aspekte der Umsetzung der Datenschutzauflagen (siehe http://www.privacyconference2003.org/program.asp). Sie bot Gelegenheit, die unterschiedlichen Ansätze der verschiedenen Kulturen und Rechtssysteme zu vergleichen. Ausserdem wurden die Probleme eines gemeinsamen Ansatzes des Datenschutzes in einer globalisierten und von gegenseitiger Abhängigkeit geprägten Welt aufgezeigt und hervorgehoben, dass der universale Charakter der Datenschutzgrundsätze, die sich aus den Leitlinien der OECD und aus dem Übereinkommen des Europarates ergeben, anerkannt werden muss. Eine flexible und dynamische

Herangehensweise an den Datenschutz ist zwar zur Gewährleistung der Effizienz unverzichtbar, aber das setzt die Achtung bestimmter Basisgrundsätze voraus, welche nicht in Frage gestellt werden dürfen; ansonsten droht die Gefahr, dass nicht nur die Grundlage der individuellen Rechte und Freiheiten, sondern auch der demokratische Charakter unserer Gesellschaften tangiert wird. Gerade zu Zeiten verschärfter Kontrollmassnahmen gegen Privatpersonen überall auf der Welt, besonders in der Terrorismusbekämpfung, spielt die Achtung dieser Grundsätze eine Schlüsselrolle. Der Datenschutz bildet einen festen Bestandteil der Sicherheitspolitik. Die Konferenz befasste sich zudem mit der Entwicklung der Informationstechnologien und mit den damit verbundenen Risiken für die individuellen Rechte und Freiheiten. Mit den heutigen Netzwerken, in denen verschiedene Technologien kombiniert werden, lassen sich immer umfangreichere Daten verwalten bis hin zur lückenlosen Verfolgung der Aktivitäten einer Privatperson. Die Konferenz stellte anhand konkreter Projekte fest, dass es möglich ist, die Technologie in Übereinstimmung mit den Datenschutzauflagen zu nutzen. Schliesslich wies die Konferenz auf die Bemühungen zahlreicher Unternehmen um die Entwicklung von Datenschutzvorschriften (Ethikkodex, interne Reglemente) hin und nahm den Wunsch nach einer weitergehenden Harmonisierung der Datenschutzbestimmungen und -praktiken positiv auf.

Der zweite, den Datenschutzbeauftragten vorbehaltene Konferenzteil bot Gelegenheit zu einem Meinungsaustausch über die wesentlichen Entwicklungen seit 2002. Die Datenschutzbeauftragten nahmen zudem fünf Entschliessungen einstimmig an (http://www.privacyconference2003.org/commissioners.asp). Die erste Entschliessung betrifft die Verbesserung der Kommunikation über Praktiken des Datenschutzes. Die Datenbearbeitungsverantwortlichen werden darin auf die Bedeutung der Information der betroffenen Personen hingewiesen. Die Entschliessung schlägt eine Vorgehensweise im Bereich der Information vor und empfiehlt die Verwendung von klar umrissenen, standardisierten Formaten. Die von Australien eingereichte Entschliessung wurde in enger Zusammenarbeit mit den Vertretern der Bearbeitungsverantwortlichen und der Verbraucher ausgearbeitet. Die zweite, von Neuseeland vorbereitete Entschliessung betrifft den Datenschutz und die internationalen Organisationen. Die internationalen Organisationen werden aufgefordert, Prinzipien zu befolgen, die mit den wichtigsten internationalen Datenschutzübereinkommen vereinbar sind. Die dritte, von Deutschland eingereichte Entschliessung behandelt die automatisierte Aktualisierung von Software. Die Softwareanbieter werden aufgefordert, Verfahren einführen, welche die Rechte der betroffenen Personen gewährleisten. Namentlich müssen die Aktualisierungen auf transparente Weise und mit der Zustimmung der betroffenen Person erfolgen. Die vierte Entschliessung über den Transfer von Personendaten wurde von der Schweiz eingereicht; sie fordert, dass «regelmässige internationale Trans-

fers von Personendaten, soweit nötig, nur innerhalb eines bestimmten Datenschutzrahmens erfolgen dürfen, z.B. auf Basis eines internationales Abkommens, welches den datenschutzrechtlichen Anforderungen ... gerecht wird.» Schliesslich reichte Deutschland eine Entschliessung zur Radio Frequency Identification (RFID) ein, welche verlangt, beim Einsatz dieser Technologie, die massive Eingriffe in die Privatsphäre mit sich bringen kann, die Datenschutzgrundsätze zu beachten.

12. Der Eidgenössische Datenschutzbeauftragte

12.1 Neuorganisation und Neuausrichtung der Tätigkeiten

Wie bereits anlässlich der Vorstellung des 10. Tätigkeitsberichts angekündigt, haben wir unsere Tätigkeiten neu ausgerichtet und unser Sekretariat neu strukturiert mit dem Ziel, die Beratungs- und Aufsichtsaufgaben neu auszubalancieren. Das bessere Gleichgewicht soll einen «proaktiveren» Ansatz im Datenschutz erlauben und Kapazitäten für die Aufsichtstätigkeiten freisetzen.

Seit dem Inkrafttreten des DSG am 1. Juli 1993 hat sich die Welt grundlegend geändert. Der Datenschutzbereich wurde von der elektronischen Revolution, welche uns in die virtuelle Welt katapultiert und gleichzeitig die Risiken der Persönlichkeitsverletzung markant gesteigert hat, besonders stark getroffen. Die Risiken der Verletzung des Privatlebens treten in allen Aktivitätsbereichen auf. Die Globalisierung der Gesellschaft und des Informationsaustausches führte dazu, dass die Bearbeitung von Personendaten zunehmend fragmentiert wird und an verschiedenen Stellen erfolgt. Diese Situation droht die Wirksamkeit des Datenschutzes zu schwächen und unterstreicht gleichzeitig die unverzichtbare Rolle des Datenschutzes. Der Datenschutzbeauftragte muss deshalb einen neuen Ansatz für die Erfüllung seiner Aufgaben verfolgen. In den ersten Tätigkeitsjahren setzten wir auf Beratungstätigkeiten und bemühten uns, sämtliche Anfragen der Bürgerinnen und Bürger zu beantworten. In Zukunft werden wir dagegen – unter Beibehaltung der Beratungstätigkeiten – unsere Aufsichtstätigkeiten stärker entwickeln müssen. Um die Herausforderungen der Informationsgesellschaft besser zu bewältigen, müssen wir ausserdem in einer «proaktiveren» Haltung an unsere gesetzlichen Aufgaben herangehen und uns nicht darauf beschränken, die Achtung der Gesetzesbestimmungen zu überprüfen. Der Schwerpunkt unserer Massnahmen soll auf der Sensibilisierung von Einzelpersonen und von Bearbeitungsverantwortlichen für die Risiken der Personendatenbearbeitung liegen. Im Vordergrund stehen:

- aktive Informationspolitik;
- Risikoevaluation, Ausarbeitung von «Werkzeugen» zur Einhaltung der datenschutzrechtlichen Anforderungen und zur Verringerung der Risiken von Persönlichkeitsverletzungen der betroffenen Personen;
- Appell an die Bearbeitungsverantwortlichen, ihre Verantwortung wahrzunehmen;
- Kontrolle der Einhaltung der Gesetzesvorschriften.

Der «proaktive» Ansatz des Datenschutzes setzt Folgendes voraus:

- neue Praktiken zu antizipieren; unter Abstimmung mit den betroffenen Kreisen Studien durchzuführen, um bessere Praktiken zu fördern, welche sich in Verhaltenskodizes und interne Reglemente umsetzen lassen;
- sich auf die neuen Technologien einzustellen und dazu Empfehlungen zu verabschieden,
- neue Entwicklungen zu antizipieren; die öffentlichen Körperschaften auf Themen für Gesetzgebung und Verordnungen aufmerksam zu machen.

Im Interesse eines wirksameren Datenschutzes werden wir uns künftig nicht mehr vorrangig mit der Behandlung von individuellen Beschwerden oder Anfragen befassen, sondern den Schwerpunkt auf die Prävention legen und uns prioritär auf die Untersuchung von Risikosektoren ausrichten; Ziel ist es, angemessene Datenschutzauflagen für die fraglichen Sektoren auszuarbeiten und Lösungen vorzuschlagen, damit diese Sektoren unter Achtung des Datenschutzes funktionieren können. Zur Prävention gehört auch die Definition und Förderung von Werkzeugen zum Schutz des Privatlebens der Einzelperson. Mit dem präventiven Vorgehen müssen die für die Bearbeitung Verantwortlichen aufgefordert werden, Verantwortung zu übernehmen und Instrumente wie z.B. das Datenschutz-Audit einzusetzen. Dabei sollen sie ihre Organisation und ihre Bearbeitungsprozesse mit den gesetzlichen Anforderungen in Einklang bringen. Die Wirksamkeit des Datenschutzes setzt ferner Kontrollen der Einhaltung der Gesetzesvorschriften sowie Sanktionen bei etwaigen Missbräuchen voraus. In dieser Hinsicht weist die schweizerische Gesetzgebung noch Lücken auf. Es wäre wünschenswert, die Sanktionen schlagkräftiger zu gestalten (siehe auch unseren 10. Tätigkeitsbericht 2002/2003, S.17f.).

Daneben möchten wir die Informationspolitik stärker ausbauen, um vor Risiken zu warnen und um die Datenschutzvorschriften und die Mittel zur Konkretisierung der Anforderungen bekannt zu machen.

Die Reduzierung der Beratungstätigkeiten zwecks Ausbau der Aufsichtstätigkeit hat Konsequenzen für die betroffenen Personen und für die für die Datenbearbeitungsverantwortlichen. In Zukunft werden wir nicht mehr alle individuellen Anfragen systematisch beantworten können. Dagegen werden wir unsere Informationsplattform weiter entwickeln und dort Antworten auf die am häufigsten gestellten Fragen geben.

Was die Bundesverwaltung anbelangt, haben wir die Eidgenössischen Departemente und die Bundesämter über unsere Neuorientierung informiert. Wir haben sie darauf hingewiesen, dass wir nicht länger in der Lage sein werden, alle Projekte durch Teilnahme an Kommissionen und Arbeitsgruppen zu begleiten. Abgesehen von den Ver-

nehmlassungsverfahren zu Gesetzesentwürfen gehen wir in der Regel nicht mehr auf die Anfragen der Departemente und der Bundesämter ein, es sei denn, sie stammen vom Datenschutzberater des Amtes bzw. des Departements. Künftig werden die Datenschutzberater der Departemente und Ämter mehr Aufgaben in der Projektbegleitung und in der Beratung übernehmen. Im Wesentlichen sind diejenigen Stellen, die Personendaten bearbeiten und Informatikprojekte umsetzen, für die Einhaltung der Datenschutzbestimmungen des Bundes verantwortlich. Sie müssen sich das einschlägige Fachwissen selbst beschaffen. Wir werden die Bundesorgane –in erster Linie die Datenschutzberater – im Rahmen unserer Kapazitäten weiterhin unterstützen. Gleich wie für den Privatsektor konzentriert sich unsere Beratungstätigkeit allerdings auf besonders heikle Fälle oder auf solche, die besonderes Fachwissen erfordern. Das schliesst indessen nicht aus, dass wir aus geeignetem Anlass im Rahmen unserer Aufsichtsaufgaben zu einem spezifischen Vorhaben Position beziehen.

12.2 Die zehnte schweizerische Konferenz der Datenschutzbeauftragten

Die zehnte schweizerische Konferenz der Datenschutzbeauftragten fand am 20. November 2003 in Genf statt. Das Thema der Konferenz war die unerwünschte elektronische Werbung (Spam).

Unerwünschte elektronische Werbung (Spam) ist ein weltweites Problem, mit dem vor allem Unternehmen zu kämpfen haben, denn es werden Speicherkapazitäten beansprucht und dementsprechend auch Kosten verursacht. Daneben sind auch die elektronischen Briefkästen der Bürger betroffen, weil sie des öfteren mit nicht angeforderten Informationen vollgestopft werden, und auch die private E-Mail-Adresse wird häufig beliebig oft angeschrieben und ohne Wissen des Betroffenen an Dritte weitergegeben.

An der Konferenz wurden die verschiedenen rechtlichen und technischen Aspekte der Problematik behandelt und diskutiert. Es wurde erkannt, dass die Problematik von Spam nicht alleine mit nationalen rechtlichen Bestimmungen in den Griff zu bekommen ist. Vielmehr sind internationale Regelungen erforderlich, damit einerseits die Absender identifiziert werden können und andererseits auch Klagen der Betroffenen über die Grenzen hinweg zum Durchbruch kommen.

Schliesslich wurden auch die verschiedenen technischen Aspekte von Spam analysiert und auf praktische Möglichkeiten, um sich von Spam zu schützen, hingewiesen. Dabei wurde erwähnt, dass unabhängig von rechtlichen Regelungsbestimmungen, deren Wirksamkeit zur Zeit beschränkt sind, auch die Benutzer von E-Mail die bereits vorhandenen technischen Mittel gegen Spam einsetzen sollten.

12.3 Publikationen des Eidgenössischen Datenschutzbeauftragten – Neuerscheinungen

- Merkblatt über das Einholen von Gutachten durch Haftpflichtversicherer
- Erläuterungen zur Videoüberwachung am Arbeitsplatz
- Erläuterungen zur Telefonüberwachung am Arbeitsplatz
- Erläuterungen über Referenzen im Bewerbungsverfahren
- Überarbeitung des Leitfadens über die Internet- und E-Mail-Überwachung am Arbeitpslatz

Der 2001 publizierte Leitfaden über die Internet- und E-Mail-überwachung ist einer eingehenderen Revision unterzogen worden. Sowohl die technischen Aspekte als auch der Ablauf der Überwachung wurden überarbeitet. Ein neues Musterreglement über die Überwachung sowie neue Schemas vervollständigen den Leitfaden. Der überarbeitete Leitfaden ist auf unsere Webseite (http://www.edsb.ch/d/doku/leitfaeden/internet/index.htm) zu finden.

Website des EDSB

Wir haben auf unserer Website in der Rubrik «Über uns» neu eine Seite «Kontakt» eingerichtet, deren Ziel es ist, die Bürgerinnen und Bürger bei Ihrer Suche nach Informationen zu Datenschutzfragen zu unterstützen. Wer Fragen zum Datenschutz hat, findet auf dieser Seite eine übersichtliche, nach Sachgebieten gegliederte Zusammenstellung von Links zu Informationen, die auf unserer Website verfügbar sind. Sollte dennoch eine Frage offen sein, besteht die Möglichkeit, uns mit Hilfe eines Kontaktformulars eine kurze Anfrage zukommen zu lassen (für längere Anfragen sollte die Briefform gewählt werden). Die Anfrage wird in verschlüsselter Form von der Arbeitsstation des Absenders bis zum Server der Bundesverwaltung und danach unverschlüsselt zu uns übermittelt. Wer möchte, dass seine Anfrage von der Arbeitsstation bis zu uns in verschlüsselter Form übermittelt wird, kann ein PGP-verschlüsseltes E-Mail senden. Weitere Informationen zum Kontaktformular finden sich auf der Seite https://sec3.admin.ch/edsb/d/service/kontaktD.htm [frz.: https://sec3.admin.ch/edsb/f/service/kontaktF.htm]

Neue Informationen zu folgenden Bereichen

- Erläuterungen zum datenschutzkonformen Betrieb von Webcams

  (http://www.edsb.ch/d/themen/video/webcam_d.pdf)

- Erläuterungen zu Referenzauskünften im Bewerbungsverfahren

  (http://www.edsb.ch/d/themen/weitere/referenzauskuenfte_d.pdf)

- Erläuterungen zu heutigen Anwendungen der Steganographie

  (http://www.edsb.ch/d/themen/sicherheit/technik/index.htm)

- Fragen und Antworten zum Bereich Versicherungen

  (http://www.edsb.ch/d/fragen/versicherungen/index.htm)

- Fragen und Antworten zum Bereich Handel und Wirtschaft

  (http://www.edsb.ch/d/fragen/handel/index.htm)

- Merkblatt über das Einholen von Gutachten durch Haftpflichtversicherer

  (http://www.edsb.ch/d/doku/merkblaetter/haftpflicht.htm)

- Gutachten über einen Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes

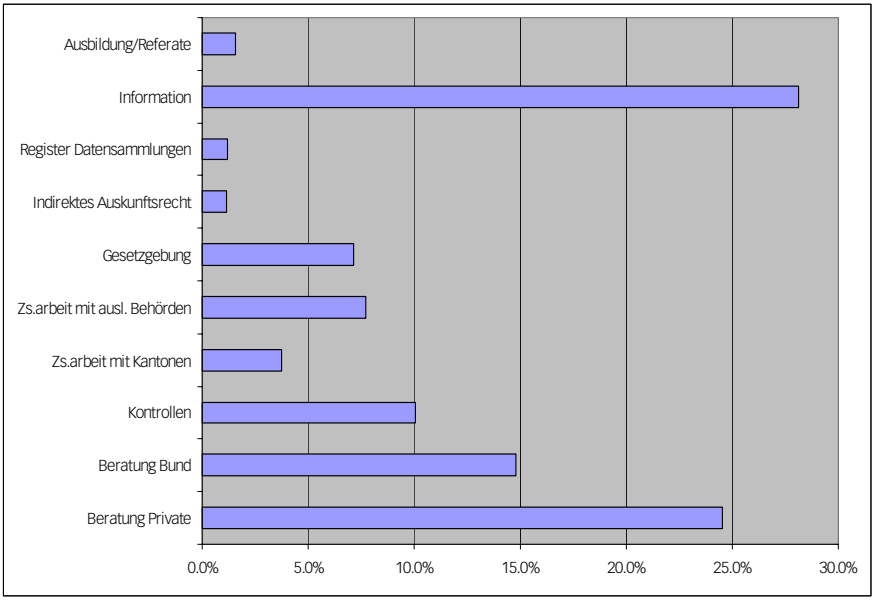
  (http://www.edsb.ch/d/themen/weitere/epid/epid.htm)

- Grundsatzpapier des EDSB über Möglichkeiten, Grenzen und Bedingungen für einen koordinierten eidgenössischen Personenidentifikator aus der Sicht des Persönlichkeitsschutzes

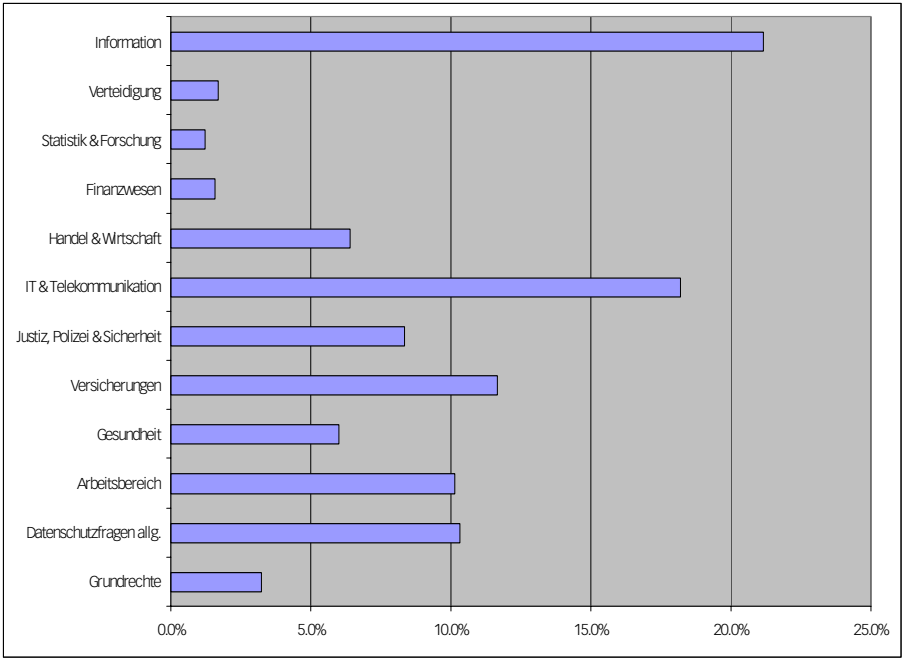
  (http://www.edsb.ch/d/themen/weitere/epid/epid.htm)

12.4 Statistik über die Tätigkeit des Eidgenössischen Datenschutzbeauftragten vom 1. April 2003 bis 31. März 2004

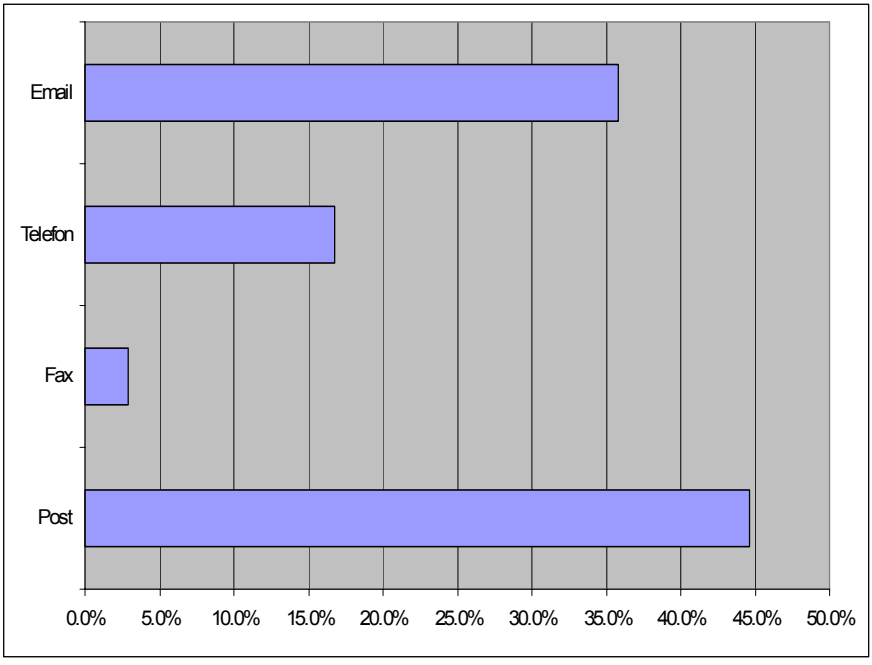
Aufwand nach Aufgabenbereich



Aufwand nach Sachgebiet



Herkunft der Anfragen



12.5 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.
Einheit Beratung und Information:	8 Personen
Einheit Aufsicht:	9 Personen
Kanzlei:	3 Personen

13. Anhang

13.1 Erläuterungen zur Videoüberwachung am Arbeitsplatz

1. Problematik

Videoüberwachungsanlagen, heutzutage oft auch als Webcam vorhanden, lösen erfahrungsgemäss bei den betroffenen Arbeitnehmern negative Gefühle aus und verschlechtern das allgemeine Betriebsklima. Sie können das Wohlbefinden, die psychische Gesundheit und damit die Leistungsfähigkeit des Personals beeinträchtigen. Es liegt deshalb im Interesse aller Beteiligten, wenn Videoüberwachungsanlagen nur dann eingesetzt werden, wenn weniger einschneidende Massnahmen den angestrebten Zweck nicht zu erreichen vermögen.

2. Gesetzliche Grundlagen

Der Arbeitgeber ist gehalten, die Gesundheit und die Persönlichkeit des Arbeitnehmers zu schützen und zu achten[1]. Im Zusammenhang mit der Überwachung bedeutet dies, dass Überwachungssysteme, die das Verhalten einer Person überwachen sollen, nicht eingesetzt werden dürfen. Wenn sie aus anderen Gründen erforderlich sind, sind sie insbesondere so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigt werden[2]. Der Arbeitgeber darf im Übrigen nur Daten über den Arbeitnehmer bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Im übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1)[3]. Zu denken ist insbesondere an Art. 13 DSG, wonach eine Verletzung der Persönlichkeit widerrechtlich ist, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

3. Voraussetzungen

Es gelten die gleichen Voraussetzungen wie bei der Videoüberwachung durch private Personen (vgl. Merkblatt über die Videoüberwachung durch private Personen). Zusätzlich soll das Mitspracherecht der Mitarbeiter bzw. seiner Vertretungen vor Einsatz einer Videoüberwachungsanlage gewährt werden.

[1] Art. 328 Obligationenrecht (OR, SR 220).
[2] Art. 26 der Verordnung 3 zum Arbeitsgesetz (SR 822.113).
[3] Art. 328b OR.

Ausserdem empfiehlt es sich, datenschutzfreundliche Technologien wie z. B. «Privacy Filters» einzusetzen. Diese *Filter* verschlüsseln die gefilmten Gesichter in Echtzeit und garantieren so die Privatsphäre. Werden die Aufnahmen zur Identifizierung (z. B. bei der strafrechtlichen Verfolgung) gebraucht, können die Aufnahmen durch die autorisierten Personen entschlüsselt werden.

4. Zweck

- Die Videoüberwachung aus organisatorischen Gründen, aus Gründen der Sicherheit oder zur Produktionssteuerung ist zulässig. Der Arbeitnehmer darf dabei nicht oder nur ausnahmsweise betroffen sein, da sonst eine Gefährdung seiner Gesundheit und seiner Bewegungsfreiheit möglich wird. Denkbar sind Videokameras ausserhalb der Gebäude und bei den Parkplätzen, bei Zugängen oder Eingängen, bei Durchgängen, bei gefährlichen Maschinen und Anlagen, in Tresorräumen, bei Gasinstallationen im Freien, bei Lagern mit gefährlichen oder wertvollen Gütern, bei Schalterhallen einer Bank, usw.

- Denkbar sind auch stichprobenartige Videoüberwachungen der Angestellten zu Schulungszwecken. Dabei ist es mit dem Persönlichkeitsschutz nicht unvereinbar, wenn die Angestellten nur über die ausgewählte Aufnahmeperiode informiert werden. Die Aufnahmeperiode darf aus Gründen der Verhältnismässigkeit und des Persönlichkeits- und Gesundheitsschutzes am Arbeitsplatz so kurz wie möglich gehalten werden. Eine Dauer von drei Tagen scheint grundsätzlich genügend zu sein.

- Videoüberwachungssysteme, welche die gezielte Überwachung des Verhaltens des Arbeitnehmers zum Ziel haben, ist verboten. Die Verhaltensüberwachung durch den Arbeitgeber ist nicht zulässig, weil sie verschiedene Elemente der Persönlichkeit des Arbeitnehmers verletzen kann. Tangiert wird vor allem die Privatsphäre, aber auch die Intimsphäre oder die familiären Verhältnisse eines oder mehreren Arbeitnehmer. Sie kann auch die Gesundheit eines Arbeitnehmers tangieren, wenn die Überwachung permanent erfolgt und sich Letzterer einem ständigen Druck ausgesetzt fühlt. Die unangekündigte Verhaltensüberwachung stellt ausserdem eine Verletzung des Prinzips von Treu und Glaube[4] dar.

[4] Art. 4 Abs. 2 DSG.

5. Videoüberwachung im Falle einer Straftat oder eines Straftatverdachts

Denkbar ist eine Überwachung des Arbeitnehmers im Falle einer Straftat oder eines Straftatverdachts, wenn die Massnahme nach Einreichung einer Anzeige gegen Unbekannten richterlich oder gerichtspolizeilich angeordnet wurde. Für die Ausübung des Auskunftsrechtes im Rahmen eines hängigen Verfahrens ist nicht das Datenschutzgesetz, sondern sind die entsprechenden Verfahrensregeln anwendbar[5].

Ausnahmsweise ist der Einsatz eines Überwachungssystems durch den Arbeitgeber zulässig, wenn Notstand[6] besteht. Möglich ist auch der Einsatz einer Videokamera, wenn Verdacht auf einer Straftat und vorherige Information über zeitlich beschränkte Überwachungen besteht.

6. Ansprüche des Arbeitnehmers bei unzulässiger Überwachung

Wenn kein Notstand bestanden hat, können Verhaltensüberwachungen durch den Arbeitgeber nicht nur als unzulässige Beweismittel im Rahmen eines Prozesses betrachtet werden, sondern auch zivile[7] wie auch strafrechtliche[8] Folgen nach sich ziehen.

7. Beispiele

7.1 Beispiel 1: Die Videoüberwachung auf Baustellen

Heutzutage werden immer mehr Videoüberwachungen auf Baustellen vorgenommen. Angegebener Zweck solcher Videoüberwachungen ist einerseits die Diebstahlskontrolle, andererseits die Kostenersparnis dank Kontrolle des Baufortschritts auf Distanz. Der Zweck der Videoüberwachung wird den Arbeitnehmern oft nicht kommuniziert.

Der nächtliche Einsatz der Videokamera ist grundsätzlich gerechtfertigt. Die Überwachungsanlage wird aus Sicherheitsgründen (Prävention gegen Diebstahl) eingesetzt und betrifft nicht das Personal.

Der tägliche Einsatz ist hingegen problematisch. Auf den Einsatz einer Videoüberwachungsanlage für die Kontrolle des Baufortschritts muss grundsätzlich verzichtet werden, weil es unverhältnismässig ist (Verhältnismässigkeitsprinzip, Art. 4 Abs. 2 DSG). Die fehlende Verhältnismässigkeit zeigt sich auch in der Beziehung zwischen Anzahl der an die Überwachung interessierten Personen einerseits und Anzahl der

[5] Art. 2 Abs. 2 lit. c DSG.
[6] Art. 34 StGB.
[7] Art. 15 bzw. 25 DSG.
[8] Art. 179quater StGB.

betroffenen Arbeitnehmer andererseits. Eine Überwachungsanlage kann auch als Mittel zur Verhaltensüberwachung empfunden werden, wenn die betroffenen Arbeitnehmer nicht genau über den beabsichtigten Zweck orientiert werden. Der Arbeitnehmer kann sich aber auch trotz Information ständig beobachtet fühlen. Dies umso mehr, da Videokameras in der Regel mit Zoom-Funktionen ausgestattet sind, welche eine Identifikation von Personen ermöglichen und somit zur Verhaltensüberwachung missbraucht werden können.

Die Videoüberwachung auf Baustellen ist nur unter Einhaltung folgender kumulativer Voraussetzungen gestattet:

- Unzumutbarkeit des täglichen Augenscheins und Erforderlichkeit der Aufnahmen (Architekt und Baumeister müssten täglich aus einer grösseren Distanz kommen, um den Baufortschritt zu kontrollieren);
- Ersatz der Videokameras mit einem digitalen Fotoapparat ohne Zoom, welcher nur ein Paar mal pro Tag den Baufortschritt aufnimmt. Dadurch soll die Gefahr einer ständigen Verhaltensüberwachung vermieden werden. Der Einsatz der Videokamera wäre nur möglich, wenn sie schwenkbar ist, d. h. wenn sie nur während der Fotoaufnahmen auf die Baustelle gerichtet ist. Ansonsten müsste sie auf etwas gerichtet sein, das weder die Interessen der Arbeitnehmer noch jene von Dritten tangieren kann.
- Die Aufnahmen werden möglichst nur während Arbeitspausen oder nach Beendigung der Arbeit gemacht;
- Es sollen datenschutzfreundliche Technologien wie Privacy Filter (vgl. § 3) eingesetzt werden;
- Der Zweck der Fotoaufnahmen (Kostenersparnisse, Senkung des Koordinationsaufwandes, Rapportierung des Baufortschrittes) sowie die Erforderlichkeit der Aufnahmen, ihren Grund und ihre Häufigkeit pro Tag (z. B. 2x/Tag) wird den betroffenen Arbeitnehmern genau und schriftlich mitgeteilt und die Verhaltensüberwachung ausdrücklich ausgeschlossen;
- Die Aufnahmen werden im Internet nur passwortgeschützt und nur einer beschränkten Anzahl zugriffsberechtigten Personen für eine bestimmte, im Voraus festgelegte und beschränkte Dauer (z. B. während der Bauzeit) zur Verfügung gestellt.

7.2 Beispiel 2: Die Videoüberwachung von Kioskangestellten

Die Videoüberwachung von Kioskangestellten ist verboten, weil sie, meist unangekündigt, die Privatsphäre, aber auch die Intimsphäre oder die familiären Verhältnisse des Angestellten tangieren kann. Sie kann auch die Gesundheit des Angestellten tangieren, wenn sie einen ständigen, kränkenden Druck auf ihn ausübt. Die Verletzung des Geheim- oder Privatbereich durch Aufnahmegeräte ist strafrechtlich relevant. Denkbar ist eine Überwachung des Kioskangestellten im Falle einer Straftat oder eines Straftatverdachts (Diebstahlsüberwachung), wenn die Massnahme richterlich angeordnet wird. Ausnahmsweise könnte man sich eine durch den Arbeitgeber vorgenommene Videoüberwachung vorstellen, wenn Notstand besteht. Der Arbeitgeber wäre aber in einem solchen Falle gehalten, so bald als möglich eine eventuelle weitere Überwachung durch die zuständige Behörde bewilligen zu lassen.

Denkbar ist auch der Einsatz einer Videokamera durch den Arbeitgeber, welche sich nur beim Öffnen der Kasse aktiviert. Beim Verschliessen der Kasse deaktiviert sich die Videokamera automatisch und in einer für den Angestellten erkennbaren Weise. Auf jeden Fall sind auch «Privacy Filters» (vgl. § 3) angebracht.

Vorbehalten bleibt die Kioskü̈berwachung gegenüber Dritten.

7.3 Beispiel 3: Die Videoüberwachung in Warenhäusern und in Banken

Viele Überwachungsanlagen werden in Verkaufsgeschäften eingesetzt. Dabei dürfen diese Anlagen nicht zur Überwachung der Angestellten verwendet werden. Die Angestellten sind aber oft davon mitbetroffen. Die Videokameras sind deshalb so zu positionieren und deren Bildausschnitt ist so zu wählen, dass das Verkaufspersonal kaum bzw. nicht ständig miterfasst und aufgezeichnet wird. Die Positionen und Einstellungen der Videokameras sind deshalb mit dem Personal zu besprechen, damit dieses den unüberwachten Bereich kennt. Es sollen auch in einem solchen Fall «Privacy Filters» (vgl. § 3) eingesetzt werden.

Die Videokameras in einer Bankschalterhalle, welche aus Sicherheitsgründen eingesetzt werden, sind so zu positionieren, dass das Bankpersonal sich nur ausnahmsweise im Kamerabereich aufhält.

7.4 Beispiel 4: Die Videoüberwachung in einem Postzentrum

Die Videoüberwachung in einem Postzentrum wird im 7. Tätigkeitsbericht 1999/2000 des Eidg. Datenschutzbeauftragten behandelt:

http://www.edsb.ch/d/doku/jahresberichte/tb7/kap7.htm#61

7.5 Beispiel 5: Die Videoüberwachung in einer Goldjuwelenfabrik

Sofern keine permanente Überwachung des Arbeitsplatzes erfolgt, ist der Arbeitgeber zum Schutze seiner eigenen Interessen berechtigt, Videoüberwachungssysteme an strategischen Orten innerhalb der Firma einzusetzen, wie z. B. an Ein-/Ausgängen, Fenstern, Garderoben. Die Videoüberwachung der Garderobe einer Goldjuwelenfabrik kann geeignet sein, Diebstähle durch die Angestellten aufzudecken, ist aber u. E. nicht die geeigneteste Massnahme. Eine wirkungsvollere Massnahme könnte ein Metal-Detector-System darstellen, sofern sie aus dem Blickwinkel der Kosten verhältnismässig ist. Metall-Detector-Systeme können verschiedene Arten von Metallen erkennen und je nach erkannte Metallart ein spezifisches Signal aussenden. Der Angestellte würde sich vor Antritt seiner Arbeitsstelle im Garderoberaum umziehen und einen möglichst metallfreien Arbeitsanzug anziehen. Beim Verlassen des Arbeitsplatzes würde er sich einer Kontrolle durch Metal-Detector unterziehen, bevor er seine eigenen Kleider wieder anziehen und die eigenen Metallgegenstände wieder erhalten kann. Brillen, Uhren und andere Metallgegenstände, die der Arbeitnehmer auch während der Arbeit unbedingt auf sich haben muss, sind gesondert zu behandeln.

13.2 Erläuterungen zur Telefonüberwachung am Arbeitsplatz

1. Allgemeines

Der Telefonapparat gehört zu den meist gebrauchten Kommunikationsmitteln am Arbeitsplatz und wird in der Regel sowohl für geschäftliche als auch für private Zwecke gebraucht. Der Arbeitgeber ist im Zusammenhang mit der Überwachung des Telefonverkehrs gehalten, die Persönlichkeit des Arbeitnehmers, insbesondere seine Privatsphäre, zu schützen und zu achten[1].

Der Arbeitnehmer ist seinerseits verpflichtet, die ihm übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen des Arbeitgebers in guten Treuen zu wahren[2]. Der Einsatz von Überwachungssystemen zur Kontrolle der Einhaltung der Nutzungsregelung für die Telephonie kann zu unzulässigen Eingriffen in die Persönlichkeit des Arbeitnehmers führen, wenn gewisse Voraussetzungen nicht eingehalten werden[3]. Neben den zivilrechtlichen Ansprüchen wegen Persönlichkeitsverletzung steht dem betroffenen Arbeitnehmer in solchen Fällen auch die Möglichkeit der Strafanzeige zu[4].

Der Arbeitgeber hat die Daten, die im Zusammenhang mit der Telefonie bearbeitet werden, durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen. Er sorgt insbesondere für die Vertraulichkeit, Verfügbarkeit und Integrität der Daten[5]. Der Arbeitnehmer kann vom Arbeitgeber jederzeit Auskunft darüber verlangen, ob und welche Daten über ihn zu welchem Zweck bearbeitet werden[6].

2. Die Voraussetzungen der Überwachung

Wenn kein Nutzungsreglement erlassen wird, besteht Unklarheit über die Berechtigung zur privaten Telefonnutzung. Ohne ausdrückliche Einschränkung oder Verbot privater Telefongespräche am Arbeitsplatz darf der Arbeitnehmer davon ausgehen, dass das private Telefonieren im Rahmen des Verhältnismässigen zulässig ist und keine Überwachung vorgenommen wird. Die Interessen und Mittel des Arbeitgebers müssen jedenfalls gewährleistet bleiben.

[1] (Art. 328 Schweiz. Obligationenrecht, OR, SR 220).
[2] Art. 321a OR.
[3] Art. 26 der Verordnung 3 zum Arbeitsgesetz, SR 822.113.
[4] Art. 179bis Schweiz. Strafgesetzbuch, StGB, SR 311.0.
[5] Art. 8 Abs. 1 der Verordnung zum Datenschutzgesetz, VDSG, SR 235.11.
[6] Art. 8ff Datenschutzgesetz, DSG, SR 235.1.

Will der Arbeitgeber den Telefonverkehr am Arbeitsplatz überwachen, sollten folgende Voraussetzungen erfüllt werden:

2.1 Die vorherige Information

2.1.1 Nutzungsreglement

Ob Arbeitnehmer das Recht haben, das Telefon für private Telefonate zu nutzen, hängt in erster Linie vom Willen des Arbeitgebers ab (Weisungsrecht des Arbeitgebers, Art. 321d Obligationenrecht, OR, SR 220). Zu bemerken ist, dass eingehende private Telefonate auch beim Vorliegen eines Verbotes des privaten Telefonierens am Arbeitsplatz nicht ausgeschlossen werden können.

Es ist ratsam, eine schriftliche Weisung über die Benutzung des Telefons am Arbeitsplatz zu erlassen, obschon dies nicht obligatorisch ist. Ein solches Nutzungsreglement schafft Transparenz und Rechtssicherheit in den Beziehungen zwischen Arbeitgeber und Arbeitnehmer. Ein nur mündlich kommuniziertes Reglement ist zwar ebenfalls verbindlich, kann aber im Streitfall zu Nachweisschwierigkeiten führen.

Die private Benutzung des Telefons am Arbeitsplatz kann je nach Nutzungsreglement entweder zugelassen, eingeschränkt oder verboten werden. Eine Einschränkung kann auf unterschiedliche Weise erfolgen. Es können beispielsweise internationale Anrufe technisch verunmöglicht oder bestimmte Telefonnummer gesperrt werden. Denkbar ist auch das Festlegen eines Zeitfensters, während dessen das private Telefonieren gestattet ist, oder eines Zeitpunktes, ab welchem eine private Benutzung erlaubt ist. Viele Firmen übernehmen bspw. die Kosten der privaten Telefonate ihrer Angestellten bis zu einem bestimmten, im voraus festgelegten Betrag.

2.1.2 Information über die Überwachung

Anders als beim Nutzungsreglement, das nicht obligatorisch ist, hat der Arbeitgeber die Pflicht, eine eventuelle Überwachung des Telefonverkehrs transparent zu kommunizieren, da sie einen Eingriff in die Privatsphäre des Arbeitnehmers darstellen kann (Prinzip von Treu und Glaube, Art. 4 Abs. 2 DSG). Diese vorherige Information hat namentlich über das eingesetzte Überwachungssystem und über das Überwachungsprozedere zu informieren. Der Arbeitgeber hat insbesondere darüber zu informieren, dass die Möglichkeit der personenbezogenen Kontrolle der telefonischen Protokollierungen besteht und dass die Auswertungsresultate Grundlage einer Sanktionierung darstellen können, falls ein Missbrauch festgestellt wird. Falls vorgesehen, hat die vorherige Information auf die Überwachung des Gesprächsinhaltes aus Leistungskontroll- oder Beweissicherungszwecken und auf deren Voraussetzungen hinzuweisen. Empfehlenswert ist auch darüber zu informieren, wer für die personenbezogene Aus-

wertung der Protokollierung oder für die Überwachung des Gesprächsinhaltes zuständig ist, welche konkreten arbeitsrechtlichen Sanktionen ergriffen werden können und wie bei Verdacht auf eine Straftat vorgegangen wird. Es ist auch über die Mechanismen zur Unterscheidung zwischen privaten und geschäftlichen Telefonaten zu informieren. Der Inhalt und die Aufbewahrungsdauer der Protokollierungen sowie die Zugriffsrechte bilden ebenfalls Gegenstand der Information.

Es empfiehlt sich, ein Überwachungsreglement zu erlassen. Letzteres wird aus Gründen der Transparenz und Rechtssicherheit schriftlich und in der Regel zusammen mit dem Nutzungsreglement in einem einzigen Dokument verfasst.

2.2 Die Unterscheidung zwischen privaten und geschäftlichen Telefonaten:

Damit die Privatsphäre des Arbeitnehmers am Arbeitsplatz vor Eingriffen geschützt wird, müssen die privaten von den geschäftlichen Telefonaten unterschieden werden können. Die Unterscheidung soll einerseits dazu führen, dass bei der Auswertung der telefonischen Randdaten nur die Ortskennziffern der als privat angewählten Telefonnummern ersichtlich sind, andererseits die Gesprächsinhalte privater Telefonate nicht abgehört werden.

Bei der Fixnetz-Telefonie erfolgt die Unterscheidung zwischen privaten und geschäftlichen Telefondaten beim ausgehenden Telefonverkehr durch Drücken einer entsprechenden Taste vor dem Telefonat. Voraussetzung dafür ist, dass eine firmeneigene Telefonzentrale besteht, die eine solche Funktion ermöglicht.

Besteht diese Unterscheidungsmöglichkeit nicht oder gestattet die Besetzung eines Büros das Führen von privaten Gesprächen nicht, so ist der private Telefonverkehr mit einem von der Firma zur Verfügung gestellten, unüberwachten und von den Arbeitnehmern finanzierten Münzapparat (z. B. Telefonkabine) oder, soweit möglich, mit einem privaten Telefonapparat (z. B. Mobiltelefon) abzuwickeln.

Sowohl die Unterscheidung mit einer Taste als auch die Benutzung einer vom Arbeitgeber zur Verfügung gestellten Telefonkabine weisen den Nachteil auf, dass die Firma als Vertragspartnerin des Telekommunikationsanbieters bei der Rechnungsstellung die vollständigen Randdaten ausgehender geschäftlicher und privater Telefonate einsehen kann. Tatsächlich lässt das Fernmeldegesetz zu, dass der Vertragspartner durch den Anbieter von Telekommunikationsdienstleistungen bei der Rechnungsstellung vollständige Randdaten des Telefonverkehrs erhält. Es empfiehlt sich, dieses Problem sowohl mit den Anbietern als auch mit dem Arbeitnehmer zu regeln und in den firmen- oder verwaltungsinternen Richtlinien über die Telefonbenutzung am Arbeitsplatz zu berücksichtigen. Der Arbeitgeber hat beim Telekommunikationsanbieter die Abkürzung der Randdaten der als «privat» gekennzeichneten Telefonaten auf die Ortskennziffern ausdrücklich zu verlangen.

Die Unterscheidung zwischen privaten und geschäftlichen Telefonaten beim eingehenden Telefonverkehr ist problematischer. Die Unterscheidung wäre aufgrund einer Kontrolle des Gesprächsinhaltes denkbar; diese ist aber nur gemäss den in Abschnitt 2.1.2 genannten Voraussetzungen rechtlich zulässig. Eine teilweise Unterscheidung aufgrund der Randdaten eingehender Telefonate wäre auch möglich, wenn letztere protokolliert und mit einer Liste privater Telefonnummer verglichen würden. Diese Art von Kontrolle kann mit Interessen wie der Verfügbarkeit einer freien Telefonlinie gerechtfertigt werden, darf aber nicht den Zweck verfolgen, die Erreichbarkeit eines Angestellten zu untergraben.

Bei der mobilen Telefonie erfolgt die Unterscheidung zwischen ausgehenden privaten und geschäftlichen Telefondaten am einfachsten durch Benutzung zweier SIM-Karten, die eine für geschäftliche, die andere für private Zwecke.

3. Gegenstand und Zweck der Überwachung

3.1 Die Überwachung der telefonischen Randdaten:

Die Überwachung der Randdaten des Telefonverkehrs durch den Arbeitgeber dient hauptsächlich der Beweisbarkeit des Telefonverkehrs im Zusammenhang mit der Einhaltung der Nutzungsregelung sowie mit der Kostenverrechnung an den Mitarbeiterund/oder an den Kunden.

Die Überwachung der Randdaten des Telefonverkehrs darf regelmässig erfolgen und betrifft folgende Daten:

- Vollständige Telefonnummer des Anrufers;
- Auf die Ortskennziffern abgekürzte, angewählte Rufnummer privater Telefonate;
- Volle Rufnummer angewählter geschäftlicher Telefonate;
- Datum und Zeitpunkt der Verbindung;
- Dauer;
- Verbindungskosten;
- Angabe über Art der Netzverbindung (mobil, fix);
- Angabe, ob Inland- oder Auslandgespräch (+ Land).

Wird ein Missbrauch festgestellt, soll dem betroffenen Arbeitnehmer Gelegenheit zur Begründung gegeben werden.

Vollständige Rufnummer privater Telefonaten dürfen nur aus Beweisgründen erstellt werden, sofern dies auf expliziten Wunsch des Mitarbeiters erfolgt oder im Streitfall nötig ist.

Er bewahrt die telefonischen Randdaten während höchstens sechs Monate auf.

3.2 Die Überwachung des Gesprächsinhalts

3.2.1 Private Gesprächsinhalte

Der Arbeitgeber ist nicht berechtigt, private Telefongespräche abzuhören oder aufzunehmen, da eine solche Überwachung zur Durchführung des Arbeitsvertrages nicht erforderlich ist[7], einen Verstoss gegen den Persönlichkeitsschutz[8] darstellt und strafrechtlich[9] verfolgt werden kann. Eine Beweissicherung zu Strafverfolgungszwecken darf nur auf Anordnung der zuständigen Strafverfolgungsbehörde erfolgen. Vorbehalten bleibt die Ausnahmesituation des Notstandes[10]. In einem solchen Fall bleibt der Arbeitgeber gehalten, eine eventuelle weitere Überwachung der zuständigen Behörde zu überlassen.

3.2.2 Geschäftliche Gesprächsinhalte

a. Zwecke

Die Gesprächsabhörung oder -aufnahme durch den Arbeitgeber darf folgenden Zwecken dienen:

- Beweissicherung;
- Leistungskontrolle.

b. Voraussetzungen

Das Strafgesetzbuch setzt für eine rechtmässige Abhörung oder Aufnahme von Gesprächen die Einwilligung beider Gesprächsteilnehmenden voraus[11]. Die Personen, deren Gespräch aufgezeichnet oder mitgehört wird, müssen von der Abhörung oder Aufnahme eindeutig und rechtzeitig in Kenntnis gesetzt werden und damit einverstanden sein. Die vorherige Information verhindert auch die Aufnahme oder Abhörung privater Gespräche. Die Information über die Abhörung oder Aufzeichnung bei jedem einzelnen Gespräch ist nicht unbedingt notwendig, wenn die Telefonabhörun-

[7] Art. 328b OR.
[8] Art. 328 OR, Art. 26 der Verordnung 3 zum Arbeitsgesetz, ArGV 3, SR 822.113.
[9] Art. 179bis Strafgesetzbuch, StGB, SR 311.0.
[10] Art. 34 StGB.
[11] Art. 179bis StGB.

gen 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 Qualitätskontrolle und 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.

Der Arbeitgeber bewahrt die Aufzeichnungen bis zur Erfüllung des entsprechenden Zweckes auf, dann vernichtet er sie.

Aufzeichnungen von Notrufen für Hilfs-, Rettungs- und Sicherheitsdienste sind nicht strafbar[12].

[12] Art. 179quinquies StGB.
Nicht strafbar ist zudem in bestimmten Fällen auch das Aufzeichnen von Telefongesprächen im Geschäftsverkehr ohne vorgängige Information, wenn es zur Beweissicherung dient.

3.3 Die Überwachung im Falle einer Straftat

Wenn der Arbeitgeber den konkreten Verdacht schöpft, dass eine Straftat per Telefon begangen wurde bzw. wird, so kann er die protokollierten telefonischen Randdaten sichern. Der Verdacht kann sich auf ein Verhalten beziehen, das nicht nur gegen Arbeitsvertrag oder Nutzungsreglement verstösst, sondern einen Straftatbestand erfüllt, wie zum Beispiel die Rufschädigung oder die sexuelle Belästigung am Arbeitsplatz[13]. Es besteht für den Arbeitgeber keine Anzeigepflicht, ist jedoch empfehlenswert, zumindest im Zusammenhang mit Offizialdelikten, Anzeige zu erstatten, um die Gefahr der Mittäterschaft zu verhindern. Die Anordnung einer Überwachung des Gesprächsinhaltes zur Beweissicherung und Erhärtung des Verdachts ist Sache der zuständigen Strafverfolgungsbehörde. Der Arbeitgeber darf von sich aus keine Telefonabhörung oder -aufnahme vornehmen (vgl. Kapitel 3.2.a). Eine solche Abhörung durch den Arbeitgeber könnte übrigens im Rahmen eines Gerichtsverfahrens als unzulässiges Beweismittel betrachtet werden. Die Anordnung einer Überwachung durch die zuständige Strafverfolgungsbehörde rechtfertigt sich, wenn aufgrund einer Interessenabwägung ein überwiegendes öffentliches oder privates Interesse festgestellt wird. Der Arbeitgeber muss das Resultat der Ermittlungen gegenüber Dritten, insbesondere gegenüber den anderen Arbeitnehmern, vertraulich behandeln.

Vorbehalten bleiben die arbeitsrechtlichen Sanktionen wegen Verletzung des Nutzungsreglements.

4. Sanktionen bei Missbrauch

Wenn die Voraussetzungen und die Regeln der Überwachung eingehalten worden sind, kann der Arbeitgeber im Falle eines erwiesenen Missbrauchs des Telefons arbeitrechtliche Sanktionen gegen den fehlbaren Arbeitnehmer aussprechen. Der Arbeitnehmer haftet für den Schaden, den er absichtlich oder fahrlässig dem Arbeitgeber zufügt[14].

In Frage kommen z. B. Abmahnungen und Schadenersatzforderungen. In extremen Fällen, wie bei wiederholtem Missbrauch trotz Abmahnung oder bei erwiesenen Straftaten kann der Arbeitgeber sogar die Entlassung aussprechen[15]. 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[16].

[13] Art. 198 StGB.
[14] Art. 321e OR.
[15] Art. 335 OR.
[16] Art. 337 OR.

Für das Aussprechen von Sanktionen sind die Vorgesetzten des fehlbaren Arbeitnehmers zuständig.

Die Sanktionen müssen der Schwere des jeweiligen Missbrauches angepasst und in ihrem Umfang bereits im Überwachungsreglement bestimmt oder bestimmbar sein.

Was die Beweislast betrifft, gilt folgende Regelung: Der Arbeitgeber muss die Verletzung der Pflichten des Arbeitnehmers und den daraus resultierenden Schaden beweisen. In der Folge kann der Arbeitnehmer den Beweis seiner Unschuld oder einer nur leichten Schuld erbringen[17].

5. Ansprüche des Arbeitnehmers bei unzulässiger Überwachung

Wenn der Arbeitgeber die einschlägigen Voraussetzungen und Regeln bei der Telefonüberwachungen nicht einhält, so kann dies als widerrechtliche Persönlichkeitsverletzung gerichtlich angefochten werden (Art. 15 und 25 DSG). Für die Beweislast gilt Art. 97 OR. Der betroffene Arbeitnehmer kann seine Ansprüche (Feststellung der Widerrechtlichkeit, Schadenersatz, usw.) zuerst beim Arbeitgeber geltend machen. Geht dieser nicht auf die Forderungen des Arbeitnehmers ein, so kann der Arbeitsrichter angerufen werden. Dieser wendet in der Regel ein rasches und kostenloses Verfahren an. Auch die arbeitsrechtlichen Sanktionen, die der Arbeitgeber aufgrund einer missbräuchlichen Überwachung ausgesprochen hat, können angefochten werden (z. B. missbräuchliche Kündigung, Art. 336 OR).

Dem Arbeitgeber können im Falle einer missbräuchlichen Überwachung auch strafrechtliche Folgen drohen, z. B. infolge einer Abhörung oder Aufnahme fremder Gespräche[18].

6. Besondere Leistungsmerkmale von Telefonanlagen

Leistungsmerkmale (insbesondere ISDN-Merkmale) moderner digitaler Telefonanlagen bieten manche Erleichterungen und Vorteile für die Benutzer. Es bestehen aber auch Datenschutzrisiken; auf diese wird im Folgenden hingewiesen, und es werden Möglichkeiten zu deren Vermeidung aufgezeigt.

[17] Art. 97 OR
[18] Art. 179bis StGB.

6.1 Freisprecheinrichtung Laut/Hören:

Mit Lautsprecher und Mikrofon ausgestattete Apparate können ohne Abheben des Telefonhörers benutzt werden. Der Gesprächspartner ist gegebenenfalls im ganzen Raum zu hören und kann über das Mikrofon selbst Gespräche im Raum mitverfolgen.

Problematik:

Gespräche von Personen im Umkreis des Telefonapparates können ohne deren Wissen vom externen Telefonteilnehmer mitgehört werden. Seine Aussagen können von den im Raum befindlichen Personen mitverfolgt werden.

- Der Gesprächsteilnehmer, dessen Stimme über Lautsprecher geschaltet ist, muss darüber informiert sein, dass seine Aussagen von weiteren Personen im Raum mitverfolgt werden können.
- Die Personen in einem Raum, in dem ein Telefonat via Freisprecheinrichtung geführt wird, müssen darüber informiert sein, dass ihre Gespräche vom externen Gesprächspartner mitgehört werden können.

6.2 Rufnummeranzeige

Bereits vor Annahme eines Telefongesprächs erscheint auf dem Display die Rufnummer (gegebenenfalls auch Name und Vorname) des anrufenden Teilnehmers. Problematik:

Bei einer systematischen Anzeige der Rufnummer kann der Anrufer seine Telefonnummer bzw. seinen Standort nicht geheim halten (z.B. gegenüber einer betrieblichen Beratungsstelle). Dritte können zudem unter Umständen Einblick in das Display und damit in die Identität des Anrufers haben.

- Der Anrufer soll die Möglichkeit haben, die Anzeige seiner Rufnummer fallweise zu unterdrücken.

6.3 Anruferliste

In der Anruferliste werden die Nummern und der Zeitpunkt der eingehenden Anrufe (beantwortete oder nicht beantwortete) aufgeführt. Der Mitarbeiter kann so nach einer Abwesenheit feststellen, wer ihn zu erreichen versuchte und eventuell zurückrufen

Problematik:

Es wird – möglicherweise ohne das Wissen des Anrufers – die Tatsache festgehalten, dass er zu einem bestimmten Zeitpunkt versucht hat anzurufen. Die Anruferliste kann unter Umständen auch von Dritten eingesehen werden.

- Die fallweise Rufnummernunterdrückung verhindert ungewollte Einträge in Anruferlisten.
- Die Anruferlisten sind vor unberechtigtem Zugriff zu schützen.

6.4 Direktes Ansprechen/Durchsage

Mit diesem Leistungsmerkmal kann der Mitarbeiter direkt über einen Lautsprecher des Telefons angesprochen werden, ohne dass er den Hörer abzunehmen oder eine sonstige Funktion zu betätigen braucht.

Problematik:

Neben der Störung der Mitarbeiter durch Ansprechen kann eine Abhörung durch Lautsprecher stattfinden, falls das Aktivieren nicht bemerkt wird.

Das direkte Ansprechen soll auf bestimmte Ziele beschränkt werden.

- Die Möglichkeit des Ansprechens muss deutlich signalisiert werden.
- Mit einem Ansprechschutz ist ein ungewolltes Ansprechen zu verhindern.

6.5 Telefonkonferenz

Bei einer (variablen) Konferenzschaltung können weitere Teilnehmer in ein Gespräch geschaltet werden.

Problematik:

Es können unter Umständen unbemerkt Teilnehmer zugeschaltet werden und das Gespräch verfolgen, ohne dass dies allen andern Teilnehmern bewusst ist.

- Das Hinzukommen und Verlassen muss durch (unterschiedliche) Signalisierungen allen Beteiligten zur Kenntnis gebracht werden.
- Wünschenswert ist die Möglichkeit der individuellen Abfrage der Anzahl bzw. die Identifikation aller Teilnehmer.

6.6 Leitungstasten/Kontrolllämpchen

Bestimmte Telefonapparate verfügen über besondere Namenstasten mit einer Anzeigefunktion (Kontrolllämpchen). Durch Drücken der Taste kann der Zielteilnehmer angewählt werden. Das Lämpchen zeigt an, ob der Teilnehmer gerade telefoniert, sowie allenfalls, ob es sich um ein internes oder externes Gespräch handelt.

Problematik:

Das telefonische Verhalten der Mitarbeiter kann überwacht werden. Bei gleichzeitigem Aufleuchten/Erlöschen zweier Lämpchen kann sogar mit grosser Wahrscheinlichkeit darauf geschlossen werden, wer mit wem intern telefoniert.

- Dieses Merkmal darf nicht zu einer unbemerkten Kontrolle führen.
- Die Tasten dürfen nicht frei programmierbar sein, damit nicht unvorgesehene Funktionen aktiviert werden können.

13.3 Erläuterungen zu Referenzauskünften im Bewerbungsverfahren

1. Problematik

Lehre und Praxis sehen im Zusammenhang mit der Erteilung von Referenzauskünften unterschiedlich aus. Insbesondere ist es umstritten, ob Referenzauskünfte nur mit der Einwilligung des Bewerbers erteilt werden dürfen. Nach Inkrafttreten des Datenschutzgesetzes erhoffte man sich eine Lösung. Die Rechtslage und die Praxis blieben aber weiterhin unsicher. Mit diesen Erläuterungen wird eine Klärung der Frage angestrebt.

2. Definition, Zweck und beteiligte Personen

Unter Referenzauskünfte versteht man Angaben über Leistung und Verhalten des Arbeitnehmers, welche von einem aktuellen oder früheren Arbeitgeber an potentielle neue Arbeitgeber bekannt gegeben werden. Der Zweck der Referenzauskunft besteht darin, die aus den Bewerbungsunterlagen und sonstigen Entscheidungsgrundlagen hervorgehenden Informationen bei Bedarf zu vervollständigen. Bei der Referenzerteilung sind in der Regel mindestens drei Personen beteiligt: der Bewerber, die aktuellen oder früheren Arbeitgeber und der potentielle Arbeitgeber.

3. Informationserteilung durch den Bewerber

Zum Schutze der eigenen Rechtsgüter und der Rechtsgüter derjenigen Personen, gegenüber denen er haftet, hat der potentielle neue Arbeitgeber ein Interesse, Informationen über den Bewerber zu bearbeiten. Für den Abschluss des Arbeitsvertrages ist der potentielle neue Arbeitgeber deshalb berechtigt, jene Informationen über den Bewerber zu bearbeiten, die er zur Klärung der Eignung für das Arbeitsverhältnis benötigt. Alle weiteren Informationen, die der potentielle neue Arbeitgeber nicht benötigt, darf er nicht bearbeiten (Verhältnismässigkeitsprinzip, Art. 328b OR). Liefert der Bewerber falsche oder verschweigt er wesentliche Angaben, haftet er dem getäuschten

Arbeitgeber gegenüber für den daraus entstandenen Schaden (culpa in contrahendo, Art. 97ff OR). Wenn dem Bewerber allerdings eine unzulässige Frage gestellt wird, darf ihm kein Nachteil entstehen, wenn er keine oder eine falsche Auskunft gibt (Notwehrrecht der Lüge als Ausfluss des informationellen Selbstbestimmungsrechtes).

4. Referenzeinholung durch den potentiellen Arbeitgeber

Der potentielle neue Arbeitgeber darf den aktuellen oder früheren Arbeitgeber nur mit Einwilligung des Bewerbers nach Referenzauskunft fragen. Allerdings darf er von einer stillschweigenden Einwilligung ausgehen, wenn der Bewerber in seiner Bewerbung Referenzen nennt. Liegt keine Einwilligung vor, dürfen keine Referenzen eingeholt werden, da sonst der aktuelle oder frühere Arbeitgeber über die Stellenbewerbung informiert wäre. Dem Bewerber stünden in einem solchen Fall gegenüber dem potentiellen Arbeitgeber die Rechtsansprüche wegen Persönlichkeitsverletzung zur Verfügung (Art. 15 DSG).

5. Referenzauskunft durch den aktuellen oder früheren Arbeitgeber

Wegen der besonderen wirtschaftlichen und persönlichen Abhängigkeit obliegt dem aktuellen oder früheren Arbeitgeber eine besondere Fürsorgepflicht gegenüber dem Bewerber (Persönlichkeitsschutz, Art. 328 OR). Der aktuelle oder frühere Arbeitgeber ist deshalb ohne Einwilligung des Bewerbers nicht berechtigt, Referenzauskünfte zu erteilen. Dies gilt auch für Auskünfte über wesentliche Elemente des Arbeitsverhältnisses. Das leitet sich aus Art. 330a Abs. 2 OR ab. Danach kann ein Arbeitnehmer statt eines Arbeitszeugnisses nur eine Arbeitsbestätigung verlangen, die sich auf Angaben über Art und Dauer des Arbeitsverhältnisses beschränkt. Mit dieser Bestimmung will der Gesetzgeber die Informationserteilung durch Arbeitszeugnis dem informationellen Selbstbestimmungsrecht des Bewerbers überlassen. Das Gleiche muss konsequenterweise auch für die mündliche Informationserteilung gelten. Könnte nämlich der aktuelle oder frühere Arbeitgeber ohne Einwilligung des Bewerbers Referenzauskünfte erteilen, würde diese zwingende Bestimmung (Art. 330a Abs. 2 in Verbindung mit Art. 362 OR) ihres Sinnes entleert. Aus diesem Grund ist der aktuelle oder frühere Arbeitgeber mangels Einwilligung des Bewerbers nicht verpflichtet und nicht legitimiert, Auskunft zu erteilen; wenn er allerdings eine abgibt, haftet er gegenüber dem potentiellen Arbeitgeber für die Folgen einer falschen Auskunft und gegenüber dem Bewerber für die Persönlichkeitsverletzung (Art. 15 DSG). Abgesehen davon kann der betroffene Bewerber aufgrund von Art. 35 DSG strafrechtlich gegen den aktuellen oder ehemaligen Arbeitgeber vorgehen, wenn er vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt. Gegebenenfalls kann der Bewerber auch gemäss Art. 173ff StGB strafrechtlich vorgehen.

13.4 Merkblatt über das Einholen von Gutachten durch Haftpflichtversicherer

I. Worum geht es?

In der Praxis gibt es immer wieder Probleme zwischen Geschädigten und Haftpflichtversicherern betreffend den Datenschutz. Konkret geht es vor allem um die Frage, ob und unter welchen Voraussetzungen ein Haftpflichtversicherer Gutachten über den Geschädigten erstellen lassen darf. Diese Gutachten werden bei verschiedenen Experten (Ärzte, Ingenieure, Biomechaniker, Betriebswirtschafter etc.) eingeholt und haben den Zweck, eine allfällige Leistungspflicht des Haftpflichtversicherers genauer abzuklären.

Unklar ist, unter welchen Voraussetzungen die Haftpflichtversicherer Gutachten über Geschädigte einholen dürfen. Im Weiteren ist zu prüfen, ob die geschädigte Person über das Einholen der Gutachten informiert werden muss.

II. Rechtliches

Die nachfolgenden Bemerkungen beschränken sich allein auf datenschutzrechtliche Überlegungen; es ist vorliegend nicht Sache des EDSB, sich zu strafrechtlichen und sonstigen Aspekten zu äussern.

Holen Haftpflichtversicherer Gutachten über Geschädigte ein, stellt dies eine Datenbearbeitung dar und bedarf in jedem Fall eines Rechtfertigungsgrundes. Haftpflichtversicherer dürfen insbesondere nicht ohne Rechtfertigungsgrund Daten einer geschädigten Person gegen deren ausdrücklichen Willen bearbeiten oder besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekannt geben. Rechtfertigungsgründe im Sinne des Datenschutzgesetzes sind die Einwilligung der betroffenen Person, ein überwiegend privates oder öffentliches Interesse oder ein Gesetz.

Sowohl die Einwilligung des Geschädigten als auch ein überwiegend privates oder öffentliches Interesse des Haftpflichtversicherers stehen als Rechtfertigungsgründe im Vordergrund. Die Einwilligung muss freiwillig sein und ist jederzeit widerrufbar.

Ob ein überwiegend privates Interesse gegeben ist, kann nicht generell beantwortet werden, sondern ist im Einzelfall zu beurteilen. Entscheidend dabei ist die Frage, ob dem Haftpflichtversicherer ein nicht wieder gut zu machender Nachteil entsteht, wenn auf die sofortige Begutachtung verzichtet wird. Ein überwiegend privates Interesse kann etwa dann vorliegen, wenn mit der Begutachtung aus medizinischen Gründen nicht zugewartet werden kann. In jedem Fall hat die Schadenssumme hoch zu sein, damit der Rechtfertigungsgrund des überwiegend privaten Interesses überhaupt gegeben ist (siehe auch Bundesgerichtsurteil 5C.187/1997).

Nichtsdestotrotz ist festzuhalten, dass es primär der Geschädigte ist, welcher die Kausalität zwischen Schaden und schädigendem Ereignis beweisen muss (vgl. Art. 8 ZGB). Es stellt sich somit die Frage, ob dem Versicherer angesichts der klaren Beweislastverteilung überhaupt ein Nachteil entsteht, wenn er den Schadensnachweis mit allfälliger Begutachtung dem Geschädigten überlässt. Dies kann jedoch nicht vom EDSB beantwortet werden, sondern ist im Einzelfall durch den zuständigen Zivilrichter zu entscheiden.

Ein wichtiger datenschutzrechtlicher Grundsatz ist das Transparenzprinzip. Die Datenbearbeitung und insbesondere die Beschaffung von Daten muss grundsätzlich für die betroffenen Personen transparent und nachvollziehbar sein. Dies gilt vor allem für die Beschaffung von besonders schützenswerten Personendaten. Will der Haftpflichtversicherer etwa ein neurologisches Gutachten über die geschädigte Person beschaffen, so hat er diese darüber zu informieren.

III. Der EDSB schlägt folgendes Prozedere vor:

- Der Haftpflichtversicherer darf Gutachten über einen Geschädigten grundsätzlich nur dann einholen, wenn der Rechtfertigungsgrund der Einwilligung oder des überwiegend privaten oder öffentlichen Interesses gegeben ist. Macht der Haftpflichtversicherer ein überwiegend privates oder öffentliches Interesse geltend, hat er dies dem Geschädigten im Einzelfall zu begründen.- Der Haftpflichtversicherer informiert den Geschädigten bzw. dessen Rechtsvertreter, dass ein Gutachten über den Geschädigten erstellt werden soll. Er teilt dem Geschädigten den Umfang und Zweck des Gutachtens mit. Insbesondere wird der Geschädigte in Kenntnis gesetzt, wer der Gutachter ist, wie genau der Auftrag lautet und welche Akten an den Gutachter weitergeleitet werden sollen. Der Haftpflichtversicherer lädt den Geschädigten zur Stellungnahme ein.
- Der Haftpflichtversicherer erteilt dem Gutachter den Auftrag und übermittelt diesem die notwendigen Akten. Der Geschädigte erhält eine Kopie des Auftrages.
- Der Haftpflichtversicherer lässt dem Geschädigten das fertig erstellte Gutachten automatisch zukommen.

13.5 Entschliessung über den Transfer von Passagierdaten

Die 25. Internationale Konferenz der Datenschutzbeauftragten beschliesst folgendes:

A. Die Konferenz stellt fest, dass

1. Im Zuge des legitimen Kampfes gegen de Terrorismus und das organisierte Verbrechen werden in einigen Länder Massnahmen in Betracht gezogen, die die Grundrechte und Freiheiten, insbesondere das recht auf den Schutz der Privatsphäre, gefährden könnten.
2. Ein Risiko besteht, Demokratie und Freiheit zu gefährden, unter der Vorgabe diese Werte zu verteidigen.
3. Gesetzliche Anforderungen an Fluggesellschaften oder andere Transportanbieter den Zugriff an Gesamtdaten von Passagieren, die in Reservationssystemen gespeichert werden, zu gewährleisten oder diese zu übertragen, mit den internationalen Datenschutzgrundsätzen oder den Verpflichtungen der Transportanbieter, die sich auf den nationalen Datenschutzgesetzen stützen, im Konflikt stehen könnten.

B. Die Konferenz bekräftigt infolgedessen, dass

1. In der Bekämpfung des internationalen Terrorismus und des organisierten Verbrechens die Staaten unter vollständiger Achtung der Grundprinzipien des Datenschutzes reagieren sollten, denn diese Werte stellen einen integralen Bestandteil der Werte dar, die sie verteidigen.
2. Regelmässige internationale Transfers von Personendaten, soweit nötig, nur innerhalb eines bestimmten Datenschutzrahmens erfolgen dürfen, z.B. auf Basis eines internationalen Abkommens, welches den datenschutzrechtlichen Anforderungen wie einem klar definierten Zweck, der verhältnismässigen Datenerhebung, einer zeitlichen Begrenzung der Datenspeicherung, der Benachrichtigung der betroffenen Personen, der Gewährleistung der Rechte der betroffenen Person, sowie einer unabhängigen Aufsicht gerecht wird.

13.6 Grundsatzpapier des EDSB zu den Möglichkeiten, Grenzen und Bedingungen für einen koordinierten eidgenössischen Personenidentifikator aus der Sicht des Persönlichkeitsschutzes

Bern, Mai 2003

1. Einführung

Der EDSB ist im Sommer 2002 vom Bundesrat gebeten worden, einen Bericht zu verfassen über die Möglichkeiten, Grenzen und Bedingungen für einen koordinierten eidgenössischen Personenidentifikator aus der Sicht des Persönlichkeitsschutzes. Einführend erlauben wir uns eine allgemeine Bemerkung zu Funktion und Rolle des EDSB im vorliegenden Zusammenhang.

Das vorliegende Dokument wurde im Rahmen von Art. 31 Abs. 1 lit. a des Bundesgesetzes über den Datenschutz (DSG) erstellt, wonach der EDSB Organe des Bundes und der Kantone in Fragen des Datenschutzes unterstützt. Es ist uns wichtig zu betonen, dass diese Unterstützung ihre Grenzen in der Unabhängigkeit findet, welche der EDSB für seine im Verhältnis zu Bundesorganen zentrale Aufsichtsfunktion (Art. 27 DSG) benötigt. Schon daraus folgt, dass die Verantwortung für datenschutzkonformes Vorgehen beim Planen und Umsetzen von Vorhaben bei den jeweiligen Projektverantwortlichen – und nicht beim EDSB – liegt. Dasselbe ergibt sich direkt auch aus Art. 16 Abs. 1 DSG. Die Bundeskanzlei und die Departemente sind im übrigen gemäss Art. 23 der Verordnung zum DSG verpflichtet, eigene Berater für den Datenschutz zu bezeichnen, welche im Departement unter anderem die verantwortlichen Organe unterstützen und beim Vollzug der Datenschutzvorschriften mitwirken. Bei Vorhaben von der Grössenordnung und Datenschutzrelevanz wie vorliegend dürfte es sich von selbst verstehen, dass innerhalb der Projektorganisation Datenschutz-Know-how geschaffen und Verantwortliche für Datenschutzanliegen bezeichnet werden müssen. Der EDSB ist schon aus Ressourcengründen darauf angewiesen, dass die Projektverantwortlichen mit datenschutzspezifischen Fragestellungen auf ihn zukommen.

2. Begriffliches zum Personenidentifikator

Mit dem Personenidentifikator soll ein Mittel zur Identifikation von Personen sowie zum Auffinden und Verknüpfen von Einträgen über dieselbe Person in Registern bzw. Datenbanken geschaffen werden. Damit ist einerseits nichts Präzises gesagt über den Zweck des Verknüpfens von Einträgen[1] und andererseits fehlt Klarheit mit Bezug auf die Bedeutung des Wortes «Identifikator» selbst. Es ist daher nützlich, eingangs kurz auf die Begriffe «Identität» und «Identifikation» einzugehen.

«*Identität*» hat mehrere Dimensionen und entsprechend gibt es für das Wort verschiedene Definitionen. Die allgemeine Definition nach Brockhaus (»völlige Übereinstimmung einer Person oder Sache mit dem, was sie ist oder als was sie bezeichnet wird») scheint auf den ersten Blick klar. Ein zweiter Blick zeigt aber rasch, dass sich daraus für die spezifischen Bereiche nur wenig ableiten lässt. Zwar gibt es präzisere Definitionen für die Bereiche der Logik und Mathematik sowie in beschränkterem Rahmen für Psychologie und Soziologie. Für den Bereich des Verwaltungshandelns sind aber gerade unter dem Gesichtspunkt von Sicherheit und Datenschutz bisher keine Definitionen erarbeitet, welche einen nützlichen Sinngehalt aufweisen. Hier schwingt stets die Vorstellung aus dem allgemeinen Sprachgebrauch mit, wonach «man weiss, um wen es sich handelt». Diese Vorstellung trifft jedoch bloss einen der wesentlichen Aspekte von Identität, den man einen umfassenden nennen kann. Es mag sein, dass der Sprachgebrauch intuitiv mit der Identitätsdefinition aus dem Bereich der Logik verbunden ist und deshalb nur die «äussere Grenze» von Identität betont. Auf jeden Fall besteht die Tendenz zu übersehen, dass jedes Individuum mehrere Teil-Identitäten besitzt. Diese Tendenz ist verbunden mit der (Wunsch-)Vorstellung, es gäbe so etwas wie absolute Sicherheit der Identitätsbestimmung. Diese Vorstellung ist jedoch irrig[2] und wer seine Überlegungen darauf aufbaut, übersieht die daraus entstehenden Risiken. Es sollte nämlich nicht übersehen werden, dass die historisch gewachsene Situation von Individuen mit Teil-Identitäten insbesondere gerade aus Gründen des Risikomanagements eine grundsätzlich sinnvolle Sache ist. Die kriminelle Energie, welche für sogenannten Identitätsdiebstahl (Identity Theft) eingesetzt wird, wird nämlich umso grösser sein, je mehr sich mit einer gestohlenen Identität machen lässt. Dieses

[1] Vgl. dazu unten den Abschnitt 3. „Personenidentifkator und Recht".

[2] Einerseits wäre die Basis zur allfälligen Einführung eines solchen Systems in den herkömmlichen papierbasierten Systemen, deren Mängel und Fehler weitervererbt würden. Andererseits gibt es keine Grund, weshalb nicht auch im elektronischen Umfeld Identitäten irrtümlich verwechselt oder absichtlich gefälscht werden könnten. vgl. dazu Roger Clarke, Certainty of Identity: A Fundamental Misconception, and a Fundamental Threat to Security, http://www.anu.edu.au/people/Roger.Clarke/DV/IdCertainty.html und Stefan A. Brands, Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy, MIT Press Cambridge & London, 2000,

Element des Risikomanagements geht in den meisten Überlegungen zu sogenannten elektronischen Identitäten vergessen, weil die ebenfalls fehlerhafte Annahme dominiert, es liesse sich durch Technik allein Sicherheit herstellen.

Das Wort «*Identifikation*» enthält nebst den Unbestimmtheiten von «Identität» noch zusätzliche. Zum einen sind bei der Identifikation *verschiedene Konstellationen*[3] denkbar, so dass aus dem Wort Identifikation nicht hervorgeht, ob die identifizierte Person dabei eine aktive oder eine passive Rolle spielt. Zum anderen sagt uns das Wort auch nicht, ob die zu identifizierende Person aus einer Menge heraus identifiziert wird oder nicht[4]. Im Zusammenhang mit Identifikation für eGovernment und eBusiness ist Roger Clarkes Definition von «Identity Authentication» vielleicht die nützlichste. Er definiert dies als «den Prozess, wodurch ein genügendes Mass an Vertrauen hergestellt wird, dass die Identifikation ein korrektes Resultat geliefert hat[5]». Diese Umschreibung macht auf zwei Dinge aufmerksam: Erstens handelt es sich beim Resultat einer Identifikation nicht um ein Ergebnis im Sinne eines unumstösslichen mathematischen Beweises. Es ist vielmehr bloss ein gewisser Grad an Zuverlässigkeit erreichbar, wie dies etwas bei Beweisen und Indizien im Rahmen Gerichtsprozessen der Fall ist. Und zweitens geht aus der Formulierung «genügendes Mass an Vertrauen» hervor, dass nicht alle Geschäfte gleich hohe Anforderungen an die Sicherheit der Identifikation stellen. Welches Mass ein genügendes ist, hängt sehr stark vom Umfeld bzw. von den mit dem aktuellen Geschäftsfall verbundenen Risiken ab.

[3] vgl. z.B. die vier folgenden Beispielfälle:
-Ein Polizist identifiziert eine Leiche.
-Herr X geht zum Amtschalter und identifiziert sich.
-Die Flughafenpolizei identifiziert einen gesuchten Verbrecher mittels einer Überwachungskamera in Verbindung mit einem Gesichtserkennungssystem.
-Ein Unique Airport Checkin-System identifiziert eine Reisenden aufgrund der Kennung seines Mobiltelefons.

[4] Ein etwas klarerer Sprachgebrauch wurde im Zusammenhang mit biometrischen Systemen eingeführt: „Identification" bedeutet hier aus einer Menge heraus, während für die 1:1 Identifikation der Begriff „Identity Verification" geschaffen wurde. Dass aus solcher „Verification" hier immer nur ein bestimmtes Mass an Gewissheit entstehen kann, ist zwar der Biometriespezialistin völlig klar, geht aber aus dem Wort nicht hervor. Zusammen mit der Tatsache, dass manche Anbieter von Biometrieprodukten von „Proof of Identity" sprechen, stützt dieser Sprachgebrauch die fehlerhafte Annahme, es gäbe so etwas wie absolut sichere Identität.

[5] „… process whereby a sufficient degree of confidence is established that the identification process has delivered a correct result." Vgl. Roger Clarke, Certainty of Identity: A Fundamental Misconception, and a Fundamental Threat to Security, http://www.anu.edu.au/people/Roger.Clarke/DV/IdCertainty.html

Es zeigt sich somit, dass «Identifikation» für sich allein wenig bedeutet, weil sie immer *in einem bestimmten Zusammenhang* geschieht. Identifiziert wird immer im Hinblick auf etwas, etwa die Inanspruchnahme einer Dienstleistung oder die Verfolgung einer Straftat. Dieser Kontext ist ein wesentliches Element für alle weiteren Überlegungen, welche im Zusammenhang mit der «Identifikation» von Personen bzw. eben einem Personen-»Identifikator» angestellt werden müssen. Sämtliche Überlegungen zu Risiken und insbesondere für die jeweiligen Anforderungen an die Sicherheit in all Ihren Dimensionen[6] müssen hier ansetzen.

Folgerungen für den Datenschutz

Aus dem Gesagten ergeben sich für einen «Personenidentifikator» zwei Folgerungen. Zunächst muss sich jeder die beschriebene Unsicherheit des begrifflichen Fundaments vor Augen halten, der mit dem «Begr iff» operiert. Wer sie übersieht, riskiert durch undifferenzierte Äusserungen Missverständnisse zu propagieren und im Resultat auch schlechten «Lösungen» Vorschub zu leisten, welche u.U. nur Kosten und mangels Akzeptanz keinen bzw. kaum Nutzen bringen. Und zweitens folgt für datenschutzrechtliche Beurteilungen, dass diese jeweils nur im Zusammenhang mit konkreten Verwendungszwecken und Anwendungsbereichen durchgeführt werden können.

3. Personenidentifikator und Recht

Schweiz

Die Rechtsordnung reflektiert den beschriebenen Zustand mit mehreren Teil-Identitäten für jede Person. Entsprechend sind gemäss der *schweizerischen Datenschutzgesetzgebung* dem Einsatz persönlicher Identifikationsnummern[7] recht enge Grenzen gesetzt. Eine solche Nummer darf nach Art. 25 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) grundsätzlich nur durch ein einzelnes Verwaltungsorgan und nur innerhalb seines eigenen Aufgabenbereichs verwendet werden. Durch ein anderes Organ darf die Nummer nur dann verwendet werden, wenn «ein enger Zusammenhang zwischen der vorgesehenen und derjenigen Datenbearbeitung besteht, für welche die persönliche Identifikationsnummer geschaffen wurde[8]».

[6] Darunter sind insbesondere die folgenden vier
– sich zum Teil diametral widersprechenden
– Dimensionen zu verstehen: Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit (Auditability).

[7] Das Wort Identifikationsnummer bezieht sich auf den Aufbau eines Personenidentifikators. Letztlich können in dieser Hinsicht sämtliche denkbaren Varianten von Personenidentifikatoren als Nummern bezeichnet werden. Dementsprechend werden nachfolgend „Personenidentifikator" und „Personennummer" gleichbedeutend gebraucht.

[8] Art. 25 Abs. 3 VDSG

Darüberhinaus setzt eine solche Verwendung eine Bewilligung durch dasjenige Organ voraus, welches die Nummer für seine Zwecke geschaffen hat[9]. Mit dieser Regelung soll der Gefahr begegnet werden, die daraus entsteht, dass aufgrund der Verwendung des gleichen Identifikationsmittels in verschiedenen Bereichen die Verknüpfung von Informationen über eine Person möglich wird[10]. Besondere Verhältnisse herrschen mit Bezug auf die AHV-Nummer, welche aus einer Zeit stammt, als datenschutzrechtliche Überlegungen noch kaum Aktualität hatten. Dementsprechend ist die AHV-Nummer einerseits – im Widerspruch zu Art. 25 Abs. 1 VDSG – eine sprechende Nummer und andererseits wurden bei ihrer Einführung auch keine Grenzen festgelegt mit Bezug auf erlaubte Verwendungszwecke. Dies wiederum hatte zur Folge, dass die AHV-Nummer im Laufe der Zeit immer weitere Verwendung fand. Beide Unzulänglichkeiten konnten anlässlich der Einführung des DSG nicht einfach beseitigt werden. Diesem Umstand trägt der Verweis auf die AHV-Gesetzgebung in Art. 25 Abs. 4 VDSG Rechnung. Im Rahmen des aktuellen Projekts «neue AHV-Nummer» wurde nun sowohl das Problem der sprechenden Nummer als auch das Problem der fehlenden Grenzen für erlaubte Verwendungszwecke erkannt. Es besteht gute Hoffnung, dass beide Probleme im Rahmen des erwähnten Projektes für die neue AHV-Nummer auch gelöst werden. Diese für die AHV-Nummer angestellten Überlegungen gelten für alle Personenidentifikatoren und es dürfte auf der Hand liegen, dass im Rahmen des vorliegenden Vorhabens der Klarheit von Verwendungszwecken besonderes Gewicht zukommt.

Europa

Auch die *Gesetzgebung der EU* erkennt die Verknüpfungsgefahr aus Identifikatoren allgemeiner Verwendung und zählt «nationale Kennziffern oder andere Kennzeichen allgemeiner Bedeutung» zu der Kategorie der sensiblen Personendaten (vgl. Artikel 8 Absatz 7 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr). Die Situation mit Bezug auf Personennummern in den verschiedenen Ländern ist schon aufgrund kultureller Tradition äusserst

[9] Art. 25 Abs. 2 VDSG

[10] Beat Rudin, in Kommentar zum schweizerischen Datenschutzgesetz, Hrsg.: Urs Maurer; Nedim Peter Vogt – Basel; Frankfurt am Main: Helbing und Lichtenhahn, 1995; N 31 zu Art. 36; vgl. dazu auch die Formulierung, welche Bundesrätin Dreifuss am 10. März 1997 im Nationalrat Zusammenhang mit der Beantwortung der Frage Steinemann zum Gesundheitspass gewählt hat: „... Le problème numéro un dans le domaine de la protection des données est celui de ne pas interconnecter des fichiers différents. ..."

unterschiedlich[11]. Dennoch wird im Folgenden kurz der Versuch unternommen, in Form einer Tabelle eine Übersicht zusammenzustellen.

Personennummern und in anderen europäischen Ländern[12]

Die nachstehenden Tabelle gibt eine Übersicht über die *Existenz* von Personennummern in den verschiedenen Ländern:

ohne Identifikationsnummer	mit Identifikationsnummer
Deutschland	Belgien
Griechenland	Dänemark
Portugal[13]	Spanien[15]
Vereinigtes Königreich[14]	Frankreich
	Irland
	Italien
	Luxemburg
	Niederlande
	Österreich
	Finnland
	Schweden

[11] Bemerkenswert ist in diesem Zusammenhang, dass bis vor kurzer Zeit auf der Webseite des BFS zur Modernisierung der Volkszählung folgender Text zu lesen war Eine reine Registerzählung würde demgegenüber die Einführung einer persönlichen Identifikationsnummer (PIN) und die Verknüpfung der Verschiedenen Register (AHV-Daten, Steuerregister usw.) bedingen.
Eine solche Lösung entspricht nicht der politischen Kultur in der Schweiz
„(Hervorhebung durch den EDSB, URL http://www.census.ch/chap02/dmodernisierung.html, letzte Änderung der Seite am 26.2.2001; lesbar bis im Januar 2003).

[12] Die Angaben zur folgenden Aufstellung stammen in erster Linie aus dem Dokument „The Electronic Identification of Citizens and Organisations in The European Union: State of Affairs – Report drawn up by Dr Jean-Michel Eymeri, Senior Lecturer, European Institute of Public Adminstration, Maastricht (NL), erstellt für das 37th Meeting of the Directors-General of the Public Service of the Member States of the European Union, Bruges, 26 and 27 November 2001. Daneben wurden auch telefonische Interviews durchgeführt.

[13] Artikel 35 Absatz 5 der portugiesischen Verfassung verbietet die Zuweisung einheitlicher / eindeutiger Nummern. „É proibida a atribuição de um número nacional único aos cidadãos."

[14] Gesetzlich gibt es eine Basis für die Einführung einer nationalen „Identifikationszahl", eingeführt wurde eine solche bisher nicht.

[15] Besonderheit: Die Nummer befindet sich auf der Identitätskarte.

Die nachstehenden Tabelle gibt eine Übersicht über die *Verwendung* von Personennummern in den verschiedenen Ländern:

Sektorielle Nummern	Allgemein verwendete Nummer
Deutschland	Belgien
Frankreich	Dänemark
Griechenland	Finnland
Irland[16]	Luxemburg
Italien	Schweden
Niederlande	
Österreich	
Portugal	
Spanien	
Vereinigtes Königreich	

Die beiden Tabellen zeigen, dass Personennummern zwar in ca. 2/3 der EU-Länder existieren, nur in der Hälfte dieser Länder aber allgemein – d.h. in verschiedenen Bereichen der Verwaltung – verwendet werden.

In den Ländern mit «allgemein verwendeter» Personennummer enthält die Gesetzgebung i.d.R. einen Passus, wonach diese Nummer nur dann verwendet werden dürfe, wenn eine «sichere Identifikation» erforderlich sei. Die Terminologie[17] schwankt zwischen «sicher» (Norwegen) und «eindeutig» (Finnland). Schweden stipuliert als Voraussetzung für den Gebrauch der Nummer eine klare Rechtfertigung über den Zweck der Bearbeitung, über die Wichtigkeit einer sicheren Identifikation oder über «einen anderen beachtenswerten Grund». Diese Tatsache ist deshalb bemerkenswert, weil sie zeigt, dass auch in Ländern mit grundsätzlich universell verwendbarer Personennummer eine gewisse Zurückhaltung gegenüber «allzu universeller Verwendbarkeit» existiert. Die Nummer soll nur dort verwendet werden dürfen, wo dies durch den konkreten Verwendungszweck auch gerechtfertigt ist.

[16] Zwar gibt es seit 1998 eine sog. „Public Service Number", aber deren Verwendung ist nicht allgemeiner Natur (z.B. Verbot für Gebrauch im Privatsektor und durch die Polizei) und seit ihrer Einführung wurden einige Datenaustausche eingeschränkt.
[17] Feststellung aufgrund inoffizieller englischer Gesetztestexte

Abschliessend ist zur internationalen Betrachtung von Identifikationsnummern auf ein Europarats-Dokument von 1991[18] zu verweisen, dessen Überlegungen auch heute noch gültig sind. Unter den wichtigen Aussagen dieses Dokuments sind hervorzuheben:

- Identifikationsnummern kombiniert mit Informatikeinsatz tragen unzweifelhaft zur Machtsteigerung der Verwaltung bei[19].
- In verschiedenen Ländern – z.B. Frankreich[20] und Niederlande[21] – hat die Debatte um eine Personenidentifikationsnummer zum Inkrafttreten einer Datenschutzgesetzgebung geführt.
- Es gibt Beispiele die zeigen, dass die Gefahr von nach und nach zunehmender Verbreitung und Verwendung einer Personennummer nicht bloss eine theoretische ist[22].
- Es ist notwendig eine präzise Evaluation von Kosten (Datenschutzprobleme) und Nutzen (Effizienssteigerung) durchzuführen, welche sich aus der Einführung von Identifikationsnummern ergeben[23].

Zur rechtlichen Bedeutung des Zwecks

Der EDSB hat den Verfassungsrechtler Prof. Dr. iur. Giovanni Biaggini mit der Ausarbeitung eines Gutachtens zu einem allfälligen Personenidentifkator beauftragt[24]. Der Gutachter kommt darin zum Schluss, dass die rechtliche Bedeutung des Bearbeitungszwecks eine sehr grosse sei. Unter anderem sagt er, Zweckänderungen seien als Einschränkungen des verfassungsrechtlich geschützten Persönlichkeitsschutzes zu betrachten. Sie seien daher zwar möglich, jedoch nur unter bestimmten Bedingungen. Insbesondere müsse jede Zweckänderung selbst in verhältnismässiger Weise stattfinden. Das bedeutet nichts anderes, als dass eine Zweckänderung nur für einen bestimmten definierten Zweck erfolgen darf. Besondere Beachtung verdient die Beurteilung des Gutachters betreffend den Vorschlag im Entwurf zum Bundesgesetz über die Harmonisierung der Personenregister, einen Personenidentifikator nicht bloss in die

[18] Les numéros personnels d'identification: leur mise en oeuvre, leur utilisation et la protection des données – Etude préparée par le Comité d'experts sur la protection des données (CJ-PD) sous l'égide du Comité européen de coopération juridique (CDCJ), les éditions du Conseil de l'Europe, 1991- ISBN 92-871-1934-1
[19] a.a.O. (zit. Fn. 18) S. 23
[20] a.a.O. (zit. Fn. 18) S. 21
[21] a.a.O. (zit. Fn. 18) S. 23
[22] a.a.O. (zit. Fn. 18) S. 24
[23] a.a.O. (zit. Fn. 18) S. 30
[24] Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV), Gutachten im Auftrag des EDSB, verfasst von Prof. Dr. iur. Giovanni Biaggini, Dezember 2002.

Administrativregister einbauen zu lassen, sondern gleich auch noch für administrative Verwendung gleichsam pauschal freizugeben: Eine derartige Vorgehensweise sei nicht statthaft, weil der Bund als Urheber des durch den Identifikator geschaffenen Gefährdungspotenzials sich seiner Schutzpflicht gegenüber den Betroffenen nicht einfach durch «Weiterdelegation» entziehen dürfe.

Ganz allgemein sind im Datenschutz[25] klar definierte Zwecke aus verschiedenen Gründen Voraussetzung für die weiteren Überlegungen. Zunächst ist die Zweckbindung als zentrales Prinzip des Datenschutzes verankert in Art. 4 Abs. 3 DSG. Des weiteren ergibt sich die Verpflichtung, klare Zwecke für Datenbearbeitungen zu kommunizieren, auch aus dem Erfordernis von Transparenz bzw. von Treu und Glauben. Auch die Prüfung der Frage, ob eine Datenbearbeitung verhältnismässig ist, erfordert Klarheit betreffend die konkreten Bearbeitungszwecke. Betrachtete man die Zwecke, die mit dem Personenidentifikator verfolgt werden sollen, so ist zunächst wesentlich, dass die Idee eines Personenidentifkators ihren Ursprung im Bereich der Registerharmonisierung[26] hat, welche aufgrund von Art. 65 Abs. 2 der Bundesverfassung (BV) für statistische Zwecke durchgeführt wird, «um den Erhebungsaufwand möglichst gering zu halten». Hierbei ist bedeutsam, dass Statistik ein privilegierter Zweck ist, weil – und soweit – sie administratives Handeln nicht beeinflusst. Sie darf aus genau diesem Grund bedeutend mehr Daten bearbeiten und insbesondere verknüpfen[27]. Dieses Privileg findet sein Korrelat einerseits darin, dass im Rahmen der Statistik Personendaten so bald wie möglich und insbesondere bei Veröffentlichungen zu anonymisieren sind[28]. Andererseits ist auch das Statistikgeheimnis von Art. 23 des Bundesstatistikgesetzes (BStatG) als Korrelat zum erwähnten Privileg zu betrachten. Dieses hat für die Tätigkeit der Statistik überragende Bedeutung, weshalb dazu einige Bemerkungen am Platze sind. Angesichts der Strafdrohung ist das Statistikgeheimnis auf derselben Stufe anzusiedeln wie das Berufsgeheimnis von Ärzten oder Rechtsanwälten in Art. 321 des Strafgesetzbuches (StGB) und das Amtsgeheimnis nach Art. 320 StGB. Genau so bedeutsam für die Wichtigkeit des Statistikgeheimnisses dürfte sein, dass in Abweichung von der Grundregel des Strafrechts[29] nicht bloss dessen vorsätzliche, sondern

[25] Wenn auch im Grunde nicht nur für den Datenschutz, sondern ebenso sehr für sämtliche Kosten-Nutzen-Überlegungen.

[26] So steht schon im BFS-Papier „Merkmalskatalog Entwurf V 1.0" vom 25. Mai 2000 „Bundespersonennummer" als obligatorisch und harmonisiert zu führendes Merkmal in den Registern.

[27] vgl. loi sur la statistique cantonale, loi-type de janvier 2002, Exposé des motifs, S. 8 f., Publikation der Konferenz der regionalen statistischen Ämter der Schweiz

[28] Art. 22 Abs. 1 DSG

[29] Wortlaut von Art. 18 Abs. 1 StGB: „Bestimmt es das Gesetz nicht ausdrücklich anders, so ist nur strafbar, wer ein Verbrechen oder ein Vergehen vorsätzlich verübt."

auch dessen fahrlässige Verletzung strafbar ist. Ganz unabhängig von der systematsichen Einordnung[30] des Delikts zeugt diese gesetzgeberische Entscheidung davon, dass im Bereich der Statistik eben besondere Sorgfaltspflichten existieren, deren Bedeutung kaum überschätzt werden kann. Schliesslich darf im vorliegenden Zusammenhang nicht übersehen werden, dass aufgrund Art. 23 BStatG nicht bloss Personen, sondern auch Organe – also z.B. das Bundesamt für Statistik – verfolgt werden können[31]. Aus der beschriebenen Bedeutung des Statistikgeheimnisses folgt, dass sich die Statistik im Rahmen der Registerharmonisierung strikt an den Rahmen der Statistik zu halten hat, und keinesfalls verlangen darf, dass mehr Daten in bestehenden Registern erfasst oder neue Register aufgebaut werden. Wenn jedoch im Rahmen der Harmonisierung der Personenregister ein Meldewesen mit weitgehenden Vorschriften für Kantone und Gemeinden eingeführt werden soll, so ist zunächst der Statistikrahmen verlassen. Darüber hinaus erscheint fraglich, ob die Organisationshoheit der Kantone dadurch nicht übermässig eingeschränkt wird. Im übrigen wird durch die Nummer in Verbindung mit den Vorschriften zum Meldewesen nichts anderes geschaffen als ein virtuelles gesamtschweizerisches Einwohnerregister. Es stellt sich aus föderalistischer Sicht die Frage, ob dafür überhaupt eine ausreichende verfassungsrechtliche Kompetenznorm besteht.

4. Risiken

118 Aus der *Verknüpfbarkeit* verschiedener Register ergibt sich die Möglichkeit, Informationen über eine bestimmte Person zusammenzustellen. Es ist daher zunächst wesentlich zu wissen, welche Information dabei betroffen sind und welches Ziel mit der Verknüpfbarkeit verfolgt werden soll. Es sei aber vor der Haltung gewarnt, wonach bestimmte Informationen nicht schützenswert seien. Das Gegenteil ist der Fall: Weil die Sensitivität einer Information vielfach erst im konkreten Fall beantwortet werden kann, ist a priori jede Information als schützenswert zu bezeichnen. Nur in Kenntnis des konkreten Verwendungszwecks und der beteiligten Akteure, kann die Sensitivität wirklich beurteilt werden. Dies trifft auch für Informationen zu, welche auf den ersten Blick harmlos bzw. nicht schützenswert scheinen. Als relativ harmloses Beispiel hiefür mag die eMail-Adresse dienen, welche a priori kaum Schutzbedarf zu haben scheint. Gerät diese Information aber – sei es durch unvorsichtiges Handeln des Inhabers, sei es aus anderen Gründen – in die falschen Hände, so kann dies für die betroffene Person aufgrund unerwünschter Werbung zum wahren Albtraum werden. Die

[30] etwa als abstraktes Gefährdungsdelikt oder als fahrlässiges Erfolgsdelikt
[31] so die Botschaft zum Bundesstatistikgesetz, BBl 1992 I 433

Belästigung kann so weit gehen, dass die Adresse nicht mehr praktisch brauchbar ist, weil die Zahl der Werbemails schlicht zu gross wird. Die daraus entstehende Notwendigkeit, die Adresse zu ändern, ist mit riesigem Aufwand verbunden, wenn dafür gesorgt werden muss, dass die Änderung in den Adressdatenbanken aller Geschäftspartner vorgenommen wird. In solchen Fällen liegen auch entgangene Gewinne im Bereich des Wahrscheinlichen. Aber auch bedeutend schwerer wiegende Konsequenzen sind aufgrund der Zugänglichkeit zu scheinbar nicht schützenswerten Informationen denkbar. Dies hat sich z.B. Ende des vergangenen Jahres in tragischer Weise gezeigt, als die Gattin eines Schweizer Zöllners ermordet worden war. Der Mörder hatte die Wohnadresse aufgrund des Namensschilds des Zöllners und aller Wahrscheinlichkeit nach aufgrund des veröffentlichten Eintrags im Telefonbuch ausfindig gemacht. Analoge Überlegungen gelten für Entführungsfälle.

Zweckvermischung als Risiko:

Fehlerhafte Überlegungen betr. Zweck führen zu fehlerhaften Schlussfolgerungen. Im vorliegenden Fall des Personenidentifikators haben wir insofern eine besondere Konstellation, als hier eine hochgradige Vermischung verschiedener Zwecke zu beobachten ist. Diese Konstellation muss zwar ganz allgemein im Bereich des eGovernment als ausgeprägt bezeichnet werden. Die grössten Probleme entstehen jedoch regelmässig dort, wo ein oder mehrere administrative Zwecke mit Zwecken der Statistik vermischt werden. Denn einerseits ist man im Bereich der Statistik nicht im gleichen Ausmass wie im Administrativbereich gewohnt, die Verknüpfungsproblematik als Problem des Datenschutzes zu sehen. Und andererseits greifen im Bereich der Administrativregister die für die Statistik geltenden Strafbestimmungen nicht. Illustriert sei diese Aussage am Beispiel des im Bundesblatt publizierten Berichts Vote électronique[32]. In diesem Bericht hat der EDSB verschiedene Zweckvermischungen festgestellt und darauf im Beitrag «e-Voting und Datenschutz mit Blick auf Registerharmonisierung»[33] hingewiesen. Gekürzt lauten die Feststellungen folgendermassen: Der Bericht argumentiert einerseits, wie wenn Vote électronique schon beschlossene Sache wäre, obwohl dies gerade nicht der Fall ist. Vote électronique wird angerufen als «dieses weitergehende und begrüssenswerte Ziel», um daraus abzuleiten, dass «die Harmonisierung der Einwohner- und Stimmregister über die statistischen Zwecke hinaus als *erstes* und *umgehend* anzupacken»[34] sei. Aus Datenschutzoptik ist nun aber das

[32] Bericht über den Vote électronique – Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte, BBl 2002 645 ff.
[33] Michael Schnyder, „e-Voting und Datenschutz mit Blick auf Registerharmonisierung", in: E-Voting – Tagungsband der Journées d'informatique juridique 2002, Dr. Hanna Muralt Müller, Prof. Dr. Andreas Auer, Prof. Dr. Thomas Koller (Herausgeber), 2003, Stämpfli, ISBN 3-7272-2162-3, S. 189-197; vgl. zum im Text angesprochenen Thema S. 195-197
[34] BBl 2002 692

«über die statistischen Zwecke» Hinausgehende genau der potentiell problematische Bereich. Im Hinblick auf den Zweck «e-Voting» ist zu sagen, dass dieses sich noch im Versuchsstadium befindet und dass bisher weder dessen Machbarkeit wirklich geprüft noch seine Einführung politisch entschieden ist. Wenn nun aber «über die statistischen Zwecke hinaus» im Hinblick auf e-Voting harmonisiert wird, so geschieht nichts anderes als die Schaffung eines virtuellen eidgenössischen Stimmregisters. Und all dies, ohne dass politisch je darüber entschieden worden wäre.

Um der Gefahr der Zweckvermischung vorzubeugen, braucht es für jeden Einsatzzweck eines allfälligen Personenidentifikator politische Entscheide mit klarer Beschreibung der verfolgten Ziele. Es darf nicht sein, dass unter dem Zeitdruck der Statistik, welche die Volkszählung 2010 registergestützt durchführen möchte, eine potentiell problematische Infrastruktur geschaffen wird.

Zusammenhang mit der sogenannten «digitalen Identität»:

Ein besonderer Fall möglicher Zweckvermischung ist im Zusammenhang mit der sogenannten elektronsichen Identität (eID) festzuhalten. Für diese ist nämlich bisher nicht präzise bestimmt, welches ihre Einsatzzwecke sein sollen[35]. Es wird jedoch nach letztem Kenntnisstand des EDSB im Projekt eID erwogen, eine elektronische Identitätskarte mit einem allfälligen Personenidentifkator zu verbinden. Im Hinblick auf diese Entscheidung muss man sich allerdings im Klaren sein darüber, dass damit ein grosses Risiko geschaffen würde. Wenn nämlich gekoppelt mit den mittels eID authentifizierten Transaktionen jeweils auch noch ein Personenidentifikator bearbeitet wird, so dürfte dies dazu führen, dass mit technischen Mitteln Informationen über diese Transaktionen vereinfacht zusammengeführt werden können. Je nach Umfang der Einsatzzwecke von eID hat dies zur Folge, dass Persönlichkeitsprofile einer Vielzahl von Personen relativ einfach zusammengestellt werden können.

Risikomanagement und falsche Annahmen:

Aus der Sicht von Datensicherheit und Datenschutz muss vor der fehlerhaften Annahme gewarnt werden, es gäbe eine Möglichkeit zur absolut sicheren Feststellung von Identitäten. Einerseits wäre die Basis zur allfälligen Einführung eines solchen Systems in den herkömmlichen papierbasierten Systemen. Beim Übergang vom bisherigen zum neuen System würden aber die Mängel und Fehler weitervererbt. Andererseits könnten auch unter dem neuen System Identitäten irrtümlich verwechselt oder absichtlich gefälscht werden[36].

[35] Insbesondere ist auch keine Grundlagenarbeit zur Frage gemacht, wann denn auf den Einsatz der eID zu verzichten sei. Es geht hierbei um die Untersuchung der Beziehung zwischen Geschäftsfällen und Identitätsfeststellung. Nebst den Fällen, in welchen Interaktionen durchaus anonym erfolgen können, gibt es auch solche, in welchen pseudonyme Interaktion in Betracht zu ziehen wäre.

[36] Vgl. Stefan A. Brands, a.a.O. (Fn 2) S. 11; Roger Clarke a.a.O. (Fn 2)

Im Zusammenhang mit Risikomanagement ist der sogenannte «*Identity Theft*» zu erwähnen. Darunter versteht man eine Deliktskategorie, die heute in den Vereinigten Staaten eine hohe Wachstumsrate aufweist[37]. Dabei verschafft sich der Täter Zugang zu Informationen der betroffenen Person, insbesondere Dokumente mit Kreditkarteninformationen, Geburtsdatum, Arbeitsort und die Sozialversicherungsnummer, welche aufgrund ihrer Verbreitung eine zentrale «Ressource» darstellt. Gemäss Bruce Schneier[38] wird die Begehung dieses Delikts vereinfacht, weil Identitätsfeststellung vermehrt elektronisch geschieht. Zusätzlich wird das Delikt umso profitabler, je mehr Systeme dieselbe elektronische Identitätsfeststellung benutzen. Daraus ergibt sich, dass es sehr gefährlich sein kann, zuviel Bedeutung an eine Nummer zu knüpfen. Denn damit schafft man schlicht ein attraktiveres Angriffsobjekt.

Datenqualität:

Die Erfahrung zeigt, dass nur diejenigen Daten eine gute Qualität aufweisen, welche im auch regelmässig tatsächlich genutzt werden. Daraus ist beispielsweise für die Information «Beruf» in den Einwohnerregistern zu schliessen, dass sie schlechte Qualität aufweisen dürfte. Denn wer seinen Beruf wechselt, hat in der Regel keine Veranlassung, dies seiner Wohngemeinde mitzuteilen. Es gibt für die meisten Berufe schlicht keinen administrativen Ablauf, welcher diese Information benötigen und damit auch à jour halten würde. So ist es irrig zu glauben, dass durch registergestützte Zählung allein die Datenqualität gesteigert würde. Die Statistik hat mit anderen Worten nur Gewähr für eine gute Qualität der aus Registern erhobenen Daten, wenn auch administrative Prozesse geschaffen werden, mit welchen diese Daten bearbeitet werden. Der Versuch, derartige Prozesse zu schaffen, findet sich im Meldewesen, wie es durch den vorliegenden Entwurf für ein Bundesgesetz über die Harmonisierung der Personenregister eingeführt werden soll. Damit ist aber der Verfassungsauftrag von Art. 65 Abs. 2 BV aber überschritten; denn diese Bestimmung zielte in keiner Weise auf die Beeinflussung bzw. Schaffung administrativer Prozesse, sondern einzig darauf, dass die Statistik nicht noch Daten erheben soll, welche schon in Registern vorhanden sind[39]. Es stellt sich somit heraus, dass die gesamte Unternehmung «Personenidentifikator» nur dann Aussichten auf Erfolg hat, wenn im administrativen Bereich

[37] Bruce Schneier, Secrets and Lies – Digital Security in a Networked World, 2000, John Wiley & Sons, ISBN 0-471-25311-1, S. 26

[38] a.a.O. zit. Fn 37

[39] vgl. die Aussage von Bundesrat Koller in der Beratung des Nationalrats vom 29. April 1998, (Amtl. Bull NR, 29. April 1998, S. 949), wonach die Vorschrift [der heutige Art. 65 BV] zwei Schranken enthalte: „Zum einen soll der Bund nur notwendige statistische Daten erheben, und zum anderen kann er harmonisierende Vorschriften erlassen, um den Erhebungsaufwand möglichst gering zu halten."

gründlich abgeklärt wird, wozu ein Personenidentifikator überhaupt geeignet und auch unbedingt erforderlich ist. Falsch ist es demgegenüber, im Hinblick auf die Statistik im administrativen Bereich neuen Bedarf an Informationen zu schaffen. Insbesondere wäre es ein Fehler, unter dem zeitlichen Druck der Statistik (Volkszählung 2010) rasch einen Identifikator in verschiedene Register einzufügen.

Die Komplexität des Nummerierungssystems:

Aus der Sicht des Ingenieurs ist in der Einführung eines Nummerierungssystems bzw. Namenssystems für die Bevölkerung ein Anwendungsfall von Einführung eines Namenssystems in einem verteilten System zu erblicken. Solche Vorhaben können gemäss der Aussage von Ross Anderson zu hartnäckigen und unlösbaren Problemen führen. Dies geschehe insbesondere dann, wenn zwei lokale Nummerierungssysteme vereinigt werden sollen, die auf Annahmen basieren, welche sich im Nachhinein als inkompatibel erweisen [40]. Vorliegend geht es im übrigen um die Vereinigung von bedeutend mehr als zwei Systemen. Im Zusammenhang mit diesen Feststellungen ist darauf hinzuweisen, dass derart inkompatible Annahmen zwischen verschiedenen kantonalen Einwohnermeldesystemen wohl nicht von vornherein ausgeschlossen werden können. Um solche Annahmen effektiv ausschliessen zu können, sind vielmehr detaillierte Analysen der in den verschiedenen Kantonen bestehenden Prozesse erforderlich. Unterlässt man diese Analyse, so könnte es sich zeigen, dass der im Entwurf zum Registerharmonisierungsgesetz versuchte Eingriff in die kantonale Organisationshoheit an rein praktischen Schwierigkeiten scheitert.

Sicherheit der Register:

Es ist davon auszugehen, dass Einwohnerregister – welche in vielen Kantonen nebst anderen Merkmalen auch die Religion enthalten – nicht ohne Schutzbedarf sind. Wenn man sich diese Register in einem Zustand der durch einen Personenidentifikator erleichterten Verknüpfbarkeit vorstellt, dann wird schnell deutlich, dass dadurch Risiken für Betroffene entstehen können. Es dürfte eine grosse Herausforderung darstellen, die Zugangspunkte in den 2'800 Gemeinden mit den erforderlichen Sicherheitsbarrieren zu versehen. Es scheint sogar fraglich, auf welche Weise eine derartige Infrastruktur überhaupt mit angemessener Sicherheit versehen werden kann.

[66] Ross Anderson, Security Engineering – A Guide to Building Dependable Distributed Systems, 2001, John Wiley & Sons, ISBN 0-471-38922-6, S. 128

5. Folgerungen / Vorgaben

Je nach angestrebtem Zweck ist zu hier zu unterscheiden:

Personenidentifikator für statistische Zwecke:

Die statistischen Zwecke sind über eine Lösung im Sinne einer Statistiknummer zu verfolgen. Das bedeutet, dass die für die Statistik eingeführte Nummer sich *ausserhalb* der administrativen Register befinden muss. Gegen eine solche Nummer ist aus Sicht des Datenschutzes nichts einzuwenden. Wird die Nummer in Administrativregister eingefügt, so beeinflusst die Statistik in unrechtmässiger Weise die administrative Tätigkeit. Eine Lösung im Sinne der Statistiknummer wird beispielsweise im Rahmen der medizinischen Statistik der Krankenhäuser vom Bundesamt für Statistik seit mehreren Jahren verwendet. Im übrigen ist darauf hinzuweisen, dass das Bundesamt für Statistik selbst bis vor sehr kurzer Zeit (letztmals gelesen im Januar 2003) noch selbst im Internet die Aussage verbreitete eine Verknüpfbarkeit der administrativen Register entspreche nicht der schweizerischen politischen Kultur.

Personenidentifikator für administrative Zwecke:

Die Frage, wozu eine Personennummer nützlich und erforderlich ist, kann nicht allgemein «für administrative Zwecke», sondern bloss für ganz konkrete und bestimmte Zwecke anhand konkreter Abläufe und Geschäftsfälle beantwortet werden. Erst daraus kann der Wunsch nach einer Personennummer inhaltlich wirklich begründet werden. Und erst im Anschluss daran kann die erforderliche politische Diskussion stattfinden und allenfalls die entsprechende Gesetzgebung geschaffen werden. Im Anschluss daran ist im Rahmen von Design und Entwicklung informatikunterstützter Infrastruktur der Einsatz von sogenannten Privacy Enhancing Technologies zu fördern.

Auch wenn sektorielle – im Gegensatz zu einem universellen – Personenidentifikatoren geschaffen werden, so ist nicht zu vergessen, dass damit virtuelle gesamtschweizerische Register entstehen. Angesichts solcher organisatorischer Veränderungen muss jeweils die Frage nach der genügenden Verfassungsgrundlage gestellt werden.

13.7 Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV)

Giovanni Biaggini

Rechtsgutachten

erstattet dem

Eidgenössischen Datenschutzbeauftragten

Feldeggweg 1

3003 Bern

Zürich, im Dezember 2002

Abkürzungen

BV	Bundesverfassung der schweizerischen Eidgenossenschaft vom 18. April 1999
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (SR 235.1)
EMRK	Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 (SR 0.101)
VDSG	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (SR 235.11)
VE	Vorentwurf

Vorbemerkung

Im Oktober 2002 wurde der Unterzeichnende beauftragt, «ein Gutachten zu den Aspekten des Persönlichkeitsschutzes im Zusammenhang mit der allfälligen Einführung eines Eidgenössischen Personenidentifikators» zu erarbeiten. Das Gutachten soll den Titel «Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV)» tragen und die Frage nach den Möglichkeiten, Bedingungen, Problemen und Grenzen des Einsatzes eines einheitlichen eidgenössischen Personenidentifikators aus grundrechtlicher Sicht beleuchten.

Der Auftrag steht im Zusammenhang mit aktuellen Bestrebungen, einen registerübergreifenden, koordinierten eidgenössischen Personenidentifikator zu schaffen und im Rahmen von personendatenbezogenen Projekten wie z.B. INFOSTAR (Zivilstandswesen), eID (elektronische Identitätskarte), neue Versichertennummer (AHV) einzusetzen.

Dem Stand der Diskussion entsprechend wird es im Folgenden in erster Linie um die *verfassungsrechtlichen* (grundrechtlichen) *Leitplanken* und weniger um Einzelfragen gehen. Die folgende Untersuchung erhebt denn auch nicht den Anspruch, alle grundrechtlichen Fragen anzugehen und erschöpfend zu beantworten.

Dem Gutachter standen namentlich die folgenden Unterlagen zur Verfügung:

- Eidgenössisches Departement des Innern (EDI), «Der eidgenössische Personenidentifikator – Projektskizze» (Bern, 31. Mai 2002).
- Eidgenössisches Departement des Innern (EDI), Aussprachepapier: Der eidgenössische Personenidentifikator (5. Juni 2002).
- Vorentwurf für ein Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (vom 25. Oktober 2002)

I. Ausgangslage und Fragestellung

1. Personenidentifikator: Begriff und Funktion

Der Begriff «Identifikator» steht für eine Nummer (Folge von Zeichen), die als Element eines Datenbestandes die eindeutige Identifizierung einer Person oder einer Sache erlaubt.

Sachidentifikatoren kommen heute z.B. für Gebäude oder Wohnungen zum Einsatz[1]. Personenidentifikatoren[2] dienen Amtsstellen, die ein Personenregister führen, als Schlüssel zu den registrierten Personendaten. Ein Personenidentifikator kann auch zum Einsatz kommen, wenn sich eine Person gegenüber einer staatlichen Stelle identifizieren muss.

Man unterscheidet zwischen sprechenden und nichtsprechenden Identifikatoren. Nichtsprechend ist ein Personenidentifikator dann, wenn aus ihm allein kein Rückschluss auf die Person oder eine Eigenschaft der Person möglich ist (vgl. Art. 25 VDSG). Aus heutiger Sicht sollen Personenidentifikatoren nichtsprechend sein und so ausgestaltet sein, dass sie mit den Mitteln der Informations- und Kommunikationstechnologie genutzt werden können.

[1] Vgl. z.B. Art. 65 Abs. 1 der Technischen Verordnung über die amtliche Vermessung vom 10. Juni 1994 (TVAV; 211.432.21).
[2] Gelegentlich auch „persönliche Identifikationsnummer" (PIN) genannt (vgl. Art. 25 VDSG).

Man kann weiter unterscheiden zwischen sektoriell ausgerichteten, *anwendungsspezifischen* Personenidentifikatoren, die sich lediglich auf ein konkretes Sachgebiet bzw. Register beziehen, und *koordinierten, registerübergreifenden* Personenidentifikatoren.

Die Schweiz kennt heute noch keinen koordinierten eidgenössischen Personenidentifikator mit universellem Charakter bzw. Einsatzgebiet. Über ein weites Einsatzgebiet verfügt die zu den sprechenden Personenidentifikatoren zählende sog. AHV-Nummer.

2. Bestrebungen zur Einführung eines eidgenössischen Personenidentifikators

Im Rahmen verschiedener personendatenbezogener Projekte plant man, Personenidentifikatoren einzuführen oder bestehende Identifikatoren zu revidieren. Dazu gehören Projekte wie die Harmonisierung der Einwohnerregister (Amtliche Statistik), INFOSTAR (Zivilstandswesen), eID (elektronische Identitätskarte), Ausländer 2000, neue Versichertennummer (AHV), Vote électronique. In diesem Zusammenhang wird auch die Schaffung eines koordinierten eidgenössischen Personenidentifikators erwogen, der in den einschlägigen Personenregistern geführt würde und allenfalls auch zur Identifizierung einer Person – z.B. im Rahmen des elektronischen Verkehrs zwischen Bürger und Verwaltung – zum Einsatz kommen könnte[3].

a. Angestrebte Ausgestaltung

Ein solcher eidgenössischer Personenidentifikator soll:

- an jede Person vergeben werden, die mit dem Staat in Kontakt tritt;
- eindeutig sein, d.h. genau eine Person bezeichnen und jede Person erfassen;
- fest an die Person gebunden sein, auch wenn ein Merkmal (z.B. der Name) ändert;
- nach dem Tod einer Person gesperrt werden, d.h. nicht neu vergeben werden;
- nicht-sprechend sein.

Die Vergabe soll in einem geregelten Verfahren über bereits bestehende Stellen erfolgen (z.B. Zivilstandsregister, Einwohnerregister, Sozialversicherungsregister), und zwar:

[3] Vgl. Eidgenössisches Departement des Innern (EDI), „Der eidgenössische Personenidentifikator – Projektskizze" (Bern, 31. Mai 2002).

- im Rahmen der sog. Erstvergabe (bei Einführung des Personenidentifikators);
- in einer ereignisgesteuerten laufenden Vergabe (insb. bei der Geburt, beim erstmaligen Aufenthalt in der Schweiz).

Primär erfasst werden soll die Wohnbevölkerung. Eine Ausdehnung auf weitere Personenkreise wird ins Auge gefasst (z.B. Auslandschweizerinnen und –schweizer mit Blick auf die elektronische Stimmabgabe).

Ein eidgenössischer Personenidentifikator kann als Primär-Schlüssel (so z.B. geplant für kantonale und kommunale Einwohnerregister) oder als Sekundär-Schlüssel (so eventuell im Bereich der AHV) dienen[4].

b. Erhoffter Nutzen

Als Motive für die Einführung eines koordinierten eidgenössischen Personenidentifikators werden vor allem genannt:[5]

Möglicher Nutzen für die Amtliche Statistik:

- Ausbau der Registerstatistik: Ein koordinierter Personenidentifikator ermöglicht eine Verknüpfung der in verschiedenen (eidgenössischen, kantonalen, kommunalen) Personenregistern vorhandenen Daten zu statistischen Zwecken und gilt daher als «Schlüsselelement für die Registerstatistik». Man verspricht sich davon eine erhebliche Verringerung des Erhebungsaufwands bei der Bevölkerung wie bei den Gemeinden.
- Verbesserung der Datenqualität.

Möglicher Nutzen für Registerführung und Datennutzer:

- Allgemein: Optimierung und Rationalisierung der Verwaltungsführung, Vereinfachung der Registerführung.
- Vereinfachung des Datenflusses zwischen Registern bzw. zwischen Behörden (z.B. zwischen dem Einwohnerregister des alten und des neuen Wohnortes, zwischen Zivilstandsämtern und Einwohnerkontrollen). In diesem Zusammenhang wird auch an die Öffnung neuer Kommunikationswege gedacht[6].

[4] Vgl. Eidgenössisches Departement des Innern (EDI), „Der eidgenössische Personenidentifikator – Projektskizze" (Bern, 31. Mai 2002), S. 7.
[5] Vgl. Eidgenössisches Departement des Innern (EDI), Aussprachepapier: Der eidgenössische Personenidentifikator (5. Juni 2002), S. 2.
[6] Z.B. im Verhältnis Zivilstandsregister – AHV-Register, Zivilstandsregister – Ausländerregister. Vgl. Eidgenössisches Departement des Innern (EDI), „Der eidgenössische Personenidentifikator – Projektskizze" (Bern, 31. Mai 2002), S. 5.

- Verbesserung der Datenqualität (da das weniger zuverlässige Abgleichen mit Hilfe von Name und Adresse entfällt).

Möglicher Nutzen für die Bürgerinnen und Bürger:

- Vereinfachungen beim Verkehr mit Behörden im Alltag (z.B. Anmeldung am neuen Wohnort ohne Vorsprache bei der Behörde oder Bestellen von Registerauszügen dank elektronischer Identifikation).

Maximal ist der genannte Nutzen dann, wenn grundsätzlich alle amtlichen Personenregister in ihren Personeneinträgen den eidgenössischen Personenidentifikator führen. In diesem Sinn sieht der verwaltungsinterne Vorentwurf (VE) für ein Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister vor, dass Bundesstellen in ihren Personenregistern den eidgenössischen Personenidentifikator zu führen haben (Art. 13 Abs. 1 VE).

Dementsprechend zieht man als mögliche Einsatzbereiche eines eidgenössischen Personenidentifikators in Betracht:

- Einsatz für *statistische* Zwecke;
- Einsatz für *administrative* Zwecke (Gesetzesvollzug, Datenaustausch zwischen Behörden bzw. Registern, Verkehr zwischen Bürger und Behörde). Die möglichen administrativen Einsatzbereiche lassen sich naturgemäss nicht abschliessend angeben.

Im Zentrum des Interesses steht der Einsatz eines eidgenössischen Personenidentifikators in Verwaltungsbereichen bzw. Registern, die erhebliche Teile der Bevölkerung erfassen und für eine elektronische Geschäftsabwicklung geeignet erscheinen[7].

c. Mögliche Gefahren

Man ist sich allgemein bewusst, dass die Einführung eines eidgenössischen Personenidentifikators aus der Sicht des Persönlichkeitsschutzes nicht unproblematisch ist[8]. Die vorgesehene Einfügung in eine grössere Zahl von Personenregistern begründet ein nicht unerhebliches Missbrauchspotenzial. Die Gefährdungen potenzieren sich durch den Einsatz elektronischer Kommunikations- und Informationssysteme[9].

[7] Vgl. Eidgenössisches Departement des Innern (EDI), „Der eidgenössische Personenidentifikator – Projektskizze" (Bern, 31. Mai 2002), S. 4.
[8] Vgl. etwa die Hinweise in: Eidgenössisches Departement des Innern (EDI), „Der eidgenössische Personenidentifikator – Projektskizze" (Bern, 31. Mai 2002). S. 11.
[9] Vgl. Rainer J. Schweizer, in: Die schweizerische Bundesverfassung – St. Galler Kommentar, St. Gallen/Zürich 2002, Art. 13, Rz. 52.

So lassen sich mit Hilfe eines registerübergreifenden Personenidentifikators und elektronischer Kommunikationstechniken personenbezogene Eintragungen verschiedener Register relativ leicht miteinander verknüpfen[10]. Mit der Zahl der Personenregister, die mittels eines Personenidentifikators erschlossen werden können, wächst auch die Gefahr der zweckwidrigen, missbräuchlichen Verwendung von Personendaten.

Die Gefahr erscheint dann besonders gross, wenn ein Personenidentifikator zusammen mit besonders schützenswerten Daten (vgl. Ziffer II.2.) zum Einsatz kommt. Dies wäre beispielsweise der Fall, wenn ein koordinierter Personenidentifikator auch im Zusammenhang

- mit der elektronischen Stimmabgabe,
- mit die Gesundheit betreffenden Daten oder
- mit Daten über strafrechtliche Verfolgungen und Sanktionen

zum Einsatz kommt bzw. Verknüpfungen mit entsprechenden Personendaten ermöglicht oder erleichtert.

Überdies ist die Erkennbarkeit der Datenbearbeitung nicht mehr ohne Weiteres gewährleistet.

- Personendaten können mit Hilfe eines anwendungsübergreifenden Schlüssels bei anderen Datensammlungen erhoben werden, ohne dass die betreffende Person davon Kenntnis erhält.
- Damit wird es auch schwieriger, die Richtigkeit der Daten zu prüfen und zu beurteilen. Zugleich droht die Gefahr, dass der verfassungsrechtliche Anspruch auf Berichtigung unrichtiger Daten (vgl. hinten II.2.) praktisch gesehen nicht mehr voll durchgreifen kann.
- Private könnten ein Interesse haben, den Personenidentifikator in Erfahrung zu bringen (z.B. private Versicherungsunternehmen vor Abschluss eines Versicherungsvertrages, als Bedingung).

Allgemein wächst mit Einführung eines koordinierten Personenidentifikators die Gefahr eines schleichenden Verlusts der Souveränität über die eigenen Daten[11], zumal hier die Möglichkeiten des «Selbstdatenschutzes»[12] von vornherein beschränkt sind.

[10] Zur Verknüpfungsproblematik vgl. Jean-Philippe Walter, La protection de la personnalité lors du traitement de données à des fins statistiques, Diss. Fribourg 1988, S. 419; Beat Rudin, in: Urs Maurer/Nedim Peter Vogt (Hrsg.), Kommentar zum schweizerischen Datenschutzgesetz, Basel 1995, Art. 36, Rz. 31 ff.

[11] Generell zu diesem Problem Bruno Baeriswyl, Vom eindimensionalen zum mehrdimensionalen Datenschutz – Tendenzen der Rechtsentwicklung, in: ders./Beat Rudin (Hrsg.), Perspektive Datenschutz, Zürich/Baden-Baden/Wien 2002, S. 58.

[12] Hansjürgen Garstka, Selbstdatenschutz, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Perspektive Datenschutz, Zürich/Baden-Baden/Wien 2002, S. 159.

Verfassungsrechtlich gesehen kann der Einsatz eines eidgenössischen Personenidentifikators namentlich mit dem grundrechtlichen Anspruch auf Achtung und Schutz der Privatsphäre und dem verfassungsrechtlich garantierten Schutz vor Datenmissbrauch (Art. 13 BV) sowie mit dem Grundrecht der persönlichen Freiheit (Art. 10 BV) kollidieren. Es ist anerkannt, dass Einführung und Verwendung eines eidgenössischen Personenidentifikators den einschlägigen verfassungsrechtlichen Anforderungen genügen muss, d.h. namentlich durch ein überwiegendes öffentliches Interesse gerechtfertigt und verhältnismässig sein muss[13].

3. Zur aktuellen Regelungssituation

Da es heute in der Schweiz keinen einheitlichen eidgenössischen Personenidentifikator gibt, fehlen entsprechende gesetzliche Regelungen.

Eine sachbereichsübergreifende Regelung für Personenidentifikatoren findet sich immerhin in Art. 25 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11). Im Einzelnen legt die Bestimmung, die sich auf Art. 36 DSG stützt, fest[14]:

- Es kommen nur *nichtsprechende* Nummern in Frage (Abs. 1).
- Eine Verwendung durch andere Organe des Bundes oder der Kantone sowie durch private Personen bedarf der *Genehmigung* durch das betroffene Bundesorgan (Abs. 2).
- Die Genehmigung setzt voraus, dass ein enger *Zusammenhang* zwischen der vorgesehenen und der ursprünglichen Verwendung besteht (Abs. 3).
- Für die Verwendung der AHV-Nummer gilt die AHVGesetzgebung (Abs. 4)[15].

[13] So auch die Projektskizze des Eidgenössischen Departements des Innern (EDI), „Der eidgenössische Personenidentifikator" (Bern, 31. Mai 2002), S. 10.
[14] Der genaue Wortlaut der Bestimmung ist folgender:
Art. 25 Persönliche Identifikationsnummer

Eine gewisse sachbereichsübergreifende Bedeutung kommt heute der eben erwähnten AHV-Nummer zu. Auf die AHV-Nummer bezieht sich eine ganze Reihe von Regelungen betreffend andere Zweige des Sozialversicherungssystems[16] sowie betreffend weitere Rechtsgebiete (insb. Armeeverwaltung)[17]. Die Datenschutzgesetzgebung vermochte dem «Wildwuchs» in Sachen Verwendung der AHV-Nummer nicht wirksam entgegenzutreten[18].

4. Fragestellung

In Anbetracht der heutigen Regelungslage ist man sich darin einig, dass die Einführung eines eidgenössischen Personenidentifikators auf jeden Fall einer umfangreicheren Anpassung der Gesetzgebung bedürfte (Erlass von Vorschriften über Bildung und Zuteilung des Personenidentifikators, Zuständigkeiten und Aufgaben von Behörden usw.).

Aus rechtlicher Sicht wirft die allfällige Einführung eines eidgenössischen Personenidentifikators verschiedene Fragen auf:

[15] Vgl. jetzt Art. 133 der Verordnung vom 31. Oktober 1947 über die Alters- und Hinterlassenenversicherung (AHVV; SR 831.101) in der Fassung vom 29. November 1995.
1 Das Bundesorgan, welches für die Verwaltung seiner Datensammlung eine persönliche Identifikationsnummer einführt, schafft eine nichtsprechende Nummer, die im eigenen Aufgabenbereich verwendet wird. Eine nichtsprechende Nummer ist jede eindeutige oder umkehrbar eindeutige Summe von Zeichen, die jeder Person, die in einer Datensammlung registriert ist, zugeteilt wird, und aus der keine Rückschlüsse auf die Person gezogen werden können.
2 Die Verwendung der persönlichen Identifikationsnummer durch andere Organe des Bundes oder der Kantone sowie durch private Personen muss vom betroffenen Bundesorgan genehmigt werden.
3 Die Genehmigung kann erteilt werden, wenn ein enger Zusammenhang zwischen der vorgesehenen und derjenigen Datenbearbeitung besteht, für welche die persönliche Identifikationsnummer geschaffen wurde.
4 Im übrigen wird die Verwendung der AHV-Nummer von der AHVGesetzgebung geregelt. Vgl. Beat Rudin (Anm. 10), Art. 36, Rz. 31 ff.

[16] Vgl etwa Art. 4 und 5 der Verordnung vom 28. November 1983 über die Informations- und Auszahlungssysteme der Arbeitslosenversicherung (SR 837.063.1), Art. 7 der Verordnung vom 14. Dezember 1992 über das Informationssystem für die Arbeitsvermittlung und Arbeitsmarktstatistik (V-AVAM; SR 823.114), Art. 4 der Verordnung vom 20. Dezember 1982 über die Heimarbeit (Heimarbeitsverordnung [HArGV]; SR 822.311), Verordnung vom 23. November 1994 über das Zentrale Ausländerregister (ZAR-Verordnung; SR 142.215).

[17] Vgl. z.B. Art. 48 und 54 der Strahlenschutzverordnung (StSV) vom 22. Juni 1994 (SR 814.501), Art. 38 der Verordnung vom 16. November 1994 über die Organisation der Armee (VOA; SR 513.11), Verordnung vom 19. Oktober 1994 über das Kontrollwesen im Zivilschutz (ZSKV) (SR 521.5), Anhang.

[18] Vgl. etwa die kritischen Bemerkungen bei Jean-Philippe Walter (Anm. 10), S. 419 f.; Beat Rudin (Anm. 10), Art. 36, Rz. 37.

- Unter gesetzgebungstechnischem Blickwinkel: Soll ein eigenes Gesetz erlassen werden oder sollen bestehende Regelungen angepasst werden?
- Unter dem Blickwinkel der Normstufe: Welche Bestimmungen gehören in ein Gesetz im formellen Sinn (Bundesgesetz), welche könne in Verordnungsform ergehen?
- Unter verfassungsrechtlichem Blickwinkel stehen zwei Fragenkomplexe im Vordergrund:

o die bundesstaatliche Kompetenzfrage,

o der verfassungsrechtliche Persönlichkeitsschutz.

Gegenstand der vorliegenden Untersuchung ist die Bedeutung des Persönlichkeitsschutzes. Nicht behandelt wird die bundesstaatliche Kompetenzfrage[19], was nicht heisst, dass die föderalistische Dimension ganz ohne Bedeutung wäre (vgl. Ziffer IV.3.b.).

Referenzmassstab ist der *verfassungsrechtliche* Persönlichkeitsschutz, nicht die dem Persönlichkeitsschutz dienende Datenschutzgesetzgebung (DSG und Begleitgesetzgebung). Die Datenschutzgesetzgebung wird aber punktuell heranzuziehen sein, namentlich soweit sie – als gesetzliche Konkretisierung verfassungsrechtlicher Vorgaben – Aufschluss über die Tragweite des verfassungsrechtlichen Persönlichkeitsschutzes gibt.

II. Der verfassungsrechtliche Persönlichkeitsschutz

1. Überblick

Die neue schweizerische Bundesverfassung enthält mehrere dem Persönlichkeitsschutz gewidmete Bestimmungen[20].

Im Vordergrund steht Art. 13 BV, der wie folgt lautet:

[19]19 Vgl. dazu eine im Zusammenhang mit dem Projekt Registerharmonisierung erarbeitete gutachterliche Stellungnahme des Bundesamtes für Justiz vom 16. Juli 2001.

[20] Vgl. zum verfassungsrechtlichen Persönlichkeitsschutz unter der neuen Bundesverfassung vgl. Jörg Paul Müller, Grundrechte in der Schweiz, 3. Aufl., Bern 1999, S. 7 ff.

Art. 13 Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Aus der hier vorab interessierenden datenschutzrechtlichen Sicht ist vor allem der zweite Absatz von Interesse.

Dem Gedanken des Persönlichkeitsschutz verpflichtet ist auch Art. 10 BV, dessen zweiter Absatz das Recht auf persönliche Freiheit gewährleistet. Diese Bestimmung führt das frühere ungeschriebene Grundrecht der persönlichen Freiheit nach, das unter der Herrschaft der Bundesverfassung von 1874 bei der Sicherstellung des verfassungsrechtlichen Persönlichkeitsschutzes eine zentrale Rolle spielte[21]. Die Bestimmung lautet wie folgt:

Art. 10 Recht auf Leben und auf persönliche Freiheit

[1] Jeder Mensch hat das Recht auf Leben. Die Todesstrafe ist verboten.

[2] Jeder Mensch hat das Recht auf persönliche Freiheit, insbesondere auf körperliche und geistige Unversehrtheit und auf Bewegungsfreiheit.

[3] Folter und jede andere Art grausamer, unmenschlicher oder erniedrigender Behandlung oder Bestrafung sind verboten.

Art. 10 Abs. 2 BV ist hier von Bedeutung, weil die Bestimmung (unter anderem) jeder Person die Freiheit garantiert, «eine bestimmte Situation nach eigener Einschätzung zu beurteilen und aufgrund dieser Einschätzung zu handeln[22]». Diese Freiheit der Selbstbestimmung ist nicht zuletzt dann gefährdet, wenn eine Person die Herrschaft über ihre Daten verliert. In diesem Sinn ordnete das deutsche Bundesverfassungsgericht in seinem «Volkszählungsurteil» vom 15. Dezember 1983 den grundrechtlichen Anspruch auf Datenschutz – unter der Bezeichnung «Recht auf informationelle Selbstbestimmung» – beim allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG) ein[23]. Nach diesem wegweisenden Urteil besitzt das Individuum einen verfassungsmässigen Anspruch darauf, grundsätzlich selber zu bestimmen, wer wann und zu welchem

[21] Vgl. BGE 125 I 257 (260); BGE 122 I 360 (362 f.); BGE 120 I 147 (149); BGE 113 Ia 1 (5); BGE 113 Ia 257 (263); Thomas W. Schrepfer, Datenschutz und Verfassung, Bern usw. 1985, S. 62 ff.; Walter Haller, Persönliche Freiheit (1987), in: Kommentar aBV, Rz. 82.
[22] So Jörg Paul Müller (Anm. 20), S. 30.
[23] BVerfGE 65, 1 (41 ff.).

Zweck ihn betreffende persönliche Daten erlangen, verarbeiten und nutzen darf, wobei das Individuum allerdings auch Einschränkungen seines Anspruch auf informationelle Selbstbestimmung hinzunehmen hat[24]. Das schweizerische Bundesgericht hat diesen Überlegungen in seine Grundrechtsjudikatur übernommen[25].

Das Verhältnis des (Art. 8 EMRK nachempfundenen[26]) Art. 13 BV zu Art. 10 Abs. 2 BV ist noch nicht restlos geklärt[27]. In der Rechtslehre wird regelmässig darauf hingewiesen, dass die beiden Bestimmungen «Parallelen» und «Überschneidungen» aufweisen[28]. Die Materialien der Verfassungsgebung geben keinen eindeutigen Aufschluss darüber, wie sich die Schutzbereiche der beiden Grundrechte zueinander verhalten.

In der Rechtslehre tendiert man zur Annahme, dass Schutzgehalte, die heute durch Art. 13 BV gewährleistet werden, nicht (mehr) unter den Schutz der persönlichen Freiheit (Art. 10 Abs. 2 BV) fallen[29]. In der Tat spricht einiges dafür, dass die «neuere», speziellere Grundrechtsbestimmung

(Art. 13 BV) vorrangig zu berücksichtigen ist und die «ältere», weniger spezifische Grundrechtsnorm mehr oder weniger verdrängt.

Ein Blick auf den Wortlaut des Art. 13 Abs. 2 BV lässt freilich eine etwas vorsichtigere Lesart ratsam erscheinen. Denn der datenschutzspezifische Art. 13 Abs. 2 BV ist, zumindest von seinem Wortlaut her, relativ eng gefasst. Ausdrücklich wird nur der «Missbrauch» von persönlichen Daten erfasst. Anerkannte Schutzgehalte wie das Recht auf Berichtigung, das Recht auf Löschung und das Recht auf Auskunft haben bei der Verfassungsreform nicht Eingang in den Normtext des Art. 13 BV gefunden – was denn auch in der Rechtslehre verschiedentlich kritisch vermerkt wurde[30].

[24] BVerfGE 65, 1 (43 f.).
[25] Vgl. insbesondere BGE 122 I 153 (162).
[26] Vgl. Stephan Breitenmoser, in: Die schweizerische Bundesverfassung – St. Galler Kommentar, St. Gallen/Zürich 2002, Art. 13, Rz. 3.
[27] In BGE 127 I 6 (10 ff.), der die Zulässigkeit der medikamentösen Zwangsbehandlung betraf, liess das Bundesgericht die Frage der Abgrenzung der Schutzbereiche von Art. 10 Abs. 2 BV und Art. 13 BV offen. – Vgl. nun immerhin das Urteil des Bundesgerichts vom 29. Mai 2002 (1P.648/2001), Erw. 3.2., wo Art. 13 Abs. 2 BV im Vordergrund steht.
[28] Vgl. z.B. Jörg Paul Müller (Anm. 20), S. 42 ff.; Rainer J. Schweizer (Anm. 28), Rz. 23; Stephan Breitenmoser (Anm. 26), Art. 13, Rz. 5.
[39] Vgl. z.B. Jörg Paul Müller (Anm. 20), S. 10.
[30] Vgl. z.B. Rainer J. Schweizer (Anm. 28), Rz. 29; ders. (Anm. 9), Art. 13, Rz. 41.

Da die Verfassungsreform den damals bestehenden verfassungsrechtlichen Persönlichkeitsschutz[31] nicht schmälern wollte, darf man davon ausgehen, dass die unter der Herrschaft der Bundesverfassung von 1874 anerkannten geschriebenen und ungeschriebenen Schutzgehalte – namentlich die Ansprüche auf Auskunft, Berichtigung und Löschung – mit der neuen Bundesverfassung weitergeführt werden[32].

Es ist wahrscheinlich, aber noch nicht hinreichend erhärtet, dass Rechtsprechung und Lehre grundsätzlich alle anerkannten datenschutzspezifischen Grundrechtsgehalte – d.h. nicht nur den Schutz vor eigentlichem Datenmissbrauch, sondern auch den Schutz vor sonstigen Benachteiligungen, die eine Person bei der Bearbeitung von Personendaten erleiden kann – künftig vornehmlich dem Art. 13 Abs. 2 BV zuordnen werden[33].

Angesichts des etwas «schmal» geratenen Wortlauts des (Art. 13 Abs. 2 BV) sollte man jedoch vorsichtigerweise Art. 13 Abs. 1 BV sowie das Grundrecht der persönlichen Freiheit (Art. 10 Abs. 2 BV) – als dem subsidiären Grundrecht im Bereich des verfassungsrechtlichen Persönlichkeitsschutzes – vorerst nicht ganz aus dem Blick verlieren und weiterhin als «Auffangnetz» für jene etablierten Schutzgehalte verwenden, welche Praxis und Lehre, aus welchen Gründen auch immer, künftig vielleicht nicht dem etwas eng formulierten Grundrecht auf Datenschutz (Art. 13 Abs. 2 BV) zuordnen werden[34].

Zusammenfassend kann man Art. 13 Abs. 2 BV durchaus als die hier einschlägige speziellere Grundrechtsnorm bezeichnen. Art. 13 Abs. 1 BV und Art. 10 Abs. 2 BV sollten jedoch nicht von vornherein beiseite gedrängt und für unbeachtlich erklärt werden, zumal das Bundesgericht das Sammeln, Bearbeiten und Aufbewahren auch in jüngerer Zeit immer wieder als Eingriffe in das Grundrecht der persönlichen Freiheit behandelt hat[35].

[31] Vgl. vorne Fussnote 21.
[32] Vgl. in diesem Sinn Botschaft des Bundesrates über eine neue Bundesverfassung vom 20. November 1996, BBl 1997 I 153.
[33] Vgl. Rainer J. Schweizer (Anm. 28), Rz. 29; Urteil des Bundesgerichts vom 29. Mai 2002 (1P.648/2001), Erw. 3.2.
[34] Vgl. auch Rainer J. Schweizer/Dean Kradolfer/Patrick Sutter, Das Verhältnis von datenschutzrechtlichen Persönlichkeitsrechten, Verfahrensgerechtigkeit und Amtsöffentlichkeit zueinander, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Perspektive Datenschutz, Zürich/Baden-Baden/Wien 2002, S. 237, wonach Art. 10 Abs. 2 BV auch im Zusammenhang mit dem Datenschutz weiterhin Bedeutung zukommt.
[35] Vgl. BGE 128 I 63 (69); BGE 125 I 257 (260). Vgl. auch BGE 122 I 360 (362 f.); BGE 120 I 147 (149); BGE 113 Ia 1 (5); BGE 113 Ia 257 (263).

Dafür spricht auch ein weiterer Gesichtspunkt. Im hier interessierenden Zusammenhang spielt, wie sich zeigen wird, nicht nur die sog. abwehrrechtliche Grundrechtsdimension (Anspruch des Individuums gegenüber dem Staat auf Unterlassung von Eingriffen) eine Rolle, sondern auch die objektiv-konstitutive Komponente und die mit ihr einhergehenden grundrechtlichen Schutzpflichten (vgl. Ziffer IV.). Solche Schutzpflichten, die dem Staat im Interesse der Grundrechtsverwirklichung ein positives Tun abverlangen, sind im Bereich der hergebrachten Grundrechte der persönlichen Freiheit und des Anspruchs auf Schutz der Privatsphäre grundsätzlich anerkannt[36].

Auch im Fall des neuartigen Art. 13 Abs. 2 BV liegt es nahe, aus der Grundrechtsbestimmung staatliche Schutzpflichten abzuleiten. Voraussetzungen und Grenzen lassen sich aber zur Zeit noch nicht hinreichend genau erkennen. Auch dies lässt es ratsam erscheinen, Art. 13 Abs. 1 BV und Art. 10 Abs. 2 BV nicht vorschnell aus dem Blick zu verlieren.

Somit kann festgehalten werden, dass der verfassungsrechtliche Persönlichkeitsschutz – oder, wie man neuerdings auch in der Schweiz gerne sagt: das Recht auf informationelle Selbstbestimmung[37] oder auf informationelle Integrität[38] – auch nach der Verfassungsreform datenschutzrechtliche Schutzgehalte umfasst. Die Bundesverfassung vermittelt dem Einzelnen den Anspruch, «grundsätzlich selber darüber zu bestimmen, wem und wann er persönliche Lebenssachverhalte, Gedanken, Empfindungen oder Emotionen offenbart[39]». Die Zuordnung zu den einschlägigen Grundrechtsbestimmungen kann zur Zeit noch nicht ganz eindeutig vorgenommen werden.

Bei dieser Ausgangslage kann man die hier interessierenden persönlichkeitsrelevanten Schutzgehalte vorerst unter dem sich etablierenden Oberbegriff des «verfassungsrechtlichen Persönlichkeitsschutzes[40]» einordnen. Man kann aber auch, ohne dass damit eine Differenz in der Sache verbunden wäre, die hier interessierenden

[36] Zur Schutzpflichtendimension vgl. etwa Jörg Paul Müller (Anm. 20), S. 18, 28; für Art. 8 EMRK, der Art. 13 Abs. 1 BV Pate stand, vgl. Robert Uerpmann, Höchstpersönliche Rechte und Diskriminierungsverbot, in: Dirk Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, Berlin 2002, S. 55.

[37] Vgl. z.B. Jörg Paul Müller (Anm. 20), S. 44; René Rhinow, Die Bundesverfassung 2000, Basel usw. 2000, S. 113; Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 45; Marc Buntschu, in: Urs Maurer/Nedim Peter Vogt (Hrsg.), Kommentar zum schweizerischen Datenschutzgesetz, Basel 1995, Art. 1, Rz. 14 ff. Vgl. auch BGE 122 I 153 (162).
– Kritisch zum Begriff Beat Rudin, Kollektives Gedächtnis und informationelle Integrität, in: AJP 1998, S. 248 f.

[38] Vgl. Beat Rudin (Anm. 37), S. 249.

[39] Jörg Paul Müller (Anm. 20), S. 45.

[40] Dazu vgl. z.B. Jörg Paul Müller (Anm. 20), S. 7 ff

Schutzgehalte bis auf Weiteres dem Art. 13 Abs. 2 BV zuordnen und von einem (relativ breiten) Grundrecht auf Datenschutz ausgehen, das nicht nur den eigentlichen «Missbrauch» erfasst. Im Folgenden wird der zweite Weg beschritten, entsprechend der sich abzeichnenden mehrheitlichen Tendenz in der neueren Rechtslehre[41].

2. Insbesondere: Der verfassungsrechtliche Anspruch auf Schutz vor Missbrauch persönlicher Daten (Art. 13 Abs. 2 BV)

Gemäss Art. 13 Abs. 2 BV hat jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Der hiermit garantierte «grundrechtliche Datenschutz[42]» erstreckt sich auf grundsätzlich jede staatliche Bearbeitung von Angaben, die einen Bezug zur Privatsphäre einer Person aufweisen (Erheben, Sammeln, Verarbeiten, Aufbewahren, Weitergeben)[43], bietet somit in allgemeiner Weise Schutz gegenüber dem datenbearbeitenden Staat[44]. Ein Umgang mit solchen Daten ist nur zulässig, wenn die allgemeinen Voraussetzungen für die Beschränkungen von Grundrechten (Art. 36 BV) erfüllt sind, d.h. die Bearbeitung notwendig ist, zweckgebunden erfolgt und verhältnismässig ist[45].

Die Schutzgehalte des Art. 13 Abs. 2 BV im Einzelnen haben in der noch jungen Praxis und Lehre zur neuen Bundesverfassung noch keine ganz klaren Konturen gewonnen. Immerhin kann man – in Fortführung bewährter bisheriger Rechtsprechung und Lehre – festhalten, dass der nunmehr auch auf Verfassungsebene verankerte Datenschutz namentlich folgende Elemente umfasst[46]:

- Grundsatz der rechtmässigen Beschaffung;
- Grundsatz der Bearbeitung nach Treu und Glauben;
- Grundsatz der Offenheit und Transparenz der Bearbeitung («Erkennbarkeit»);
- Grundsatz der Zweckbindung der Bearbeitung;
- Grundsatz der Verhältnismässigkeit der Bearbeitung (inkl. Verbot des Sammelns auf Vorrat);

[41] Vgl. z.B. Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 29. In diese Richtung neuerdings auch das Bundesgericht in seinem Urteil vom 29. Mai 2002 (1P.648/2001), Erw. 3.2.
[42] Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 40. Vgl. auch Jörg Paul Müller (Anm. 20), S. 44 ff.
[43] Vgl. Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 40 (mit Nachweisen).
[44] Vgl. z.B. René Rhinow (Anm. 37), S. 113; Jörg Paul Müller (Anm. 20), S. 45 f.
[45] Vgl. z.B. Jörg Paul Müller (Anm. 20), S. 45 f.; Botschaft des Bundesrates über eine neue Bundesverfassung vom 20.
November 1996, BBl 1997 I 153.
[46] Vgl. die Aufzählung bei Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 43 (mit weiteren Hinweisen).
– Zu den gesetzlichen Konkretisierungen vgl. Art. 4 ff. DSG.

- Grundsatz der Richtigkeit der Datenbearbeitung;
- Grundsatz der Wahrung der Datensicherheit;
- Grundsatz der Beschränkung der Datenweitergabe ins Ausland, wenn kein gleichwertiger Persönlichkeits- bzw. Datenschutz besteht.

Diese Grundsätze sind bei der Auslegung und Konkretisierung des Verfassungsbegriffs «Missbrauch» (von persönlichen Daten), mit welchem die neue Bundesverfassung heute den Schutzgehalt des Grundrechts auf Datenschutz (Art. 13 Abs. 2 BV) umschreibt, zu berücksichtigen.

Entgegen dem, was der Wortlaut vermuten lässt, bietet die Verfassung nicht erst gegen eigentlichen Datenmissbrauch Schutz. Der grundrechtliche Schutz greift vielmehr – im Sinne der genannten Grundsätze – bereits im Vorfeld ein, will auch präventiv wirken. Dem Gedanken der Prävention verpflichtet sind namentlich drei Instrumente, welche die Verfassung im Interesse des Persönlichkeitsschutzes dem Individuum zur Verfügung stellt[47]:

- Anspruch auf Berichtigung falscher Daten;
- Anspruch auf Löschung von ungeeigneten, unnötigen («überflüssigen») Daten;
- Recht auf Auskunft bzw. Einsicht – als «Grundpfeiler des Datenschutzrechts[48]».

Art. 13 Abs. 2 BV nennt zwar diese Instrumente nicht ausdrücklich. Man darf jedoch davon ausgehen, dass diese unter der alten Bundesverfassung anerkannten Positionen auch unter der neuen Bundesverfassung weiterhin verfassungsrechtlich geschützt sind[49].

Die genannten verfassungsrechtlich fundierten Datenschutzgrundsätze gelten nicht absolut. Sie können unter gewissen Voraussetzungen – insbesondere: Vorliegen eines gewichtigen öffentlichen Interesses, Wahrung der Verhältnismässigkeit – relativiert werden. So ist beispielsweise anerkannt, dass man unter bestimmten Umständen vom Grundsatz der Erkennbarkeit der Beschaffung abgehen kann (z.B. verdeckte Überwachung des Fernmeldeverkehrs im Fall schwerwiegender Straftaten[50]).

[47] Vgl. z.B. René Rhinow (Anm. 37), S. 113. Vgl. auch Botschaft des Bundesrates über eine neue Bundesverfassung vom 20. November 1996, BBl 1997 I 153.
[48] Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 45.
[49] Vgl. Ulrich Häfelin/Walter Haller, Schweizerisches Bundesstaatsrecht, 5. Aufl., Zürich 2001, N. 388 f.; Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 44 ff. – Gemäss Schweizer (a.a.O., Rz. 46) kommt ein Anspruch auf Rechtsschutz hinzu (zur Geltendmachung und Durchsetzung der Ansprüche auf Auskunft, Berichtigung, Vernichtung usw.).
[50] Vgl. etwa BGE 109 Ia 273 ff.

Im Unterschied zur Datenschutzgesetzgebung des Bundes erwähnt die Bundesverfassung die Kategorie der besonders schützenswerten Daten nicht. Als besonders schützenswert gelten gemäss Art. 3 Bst. c. DSG Daten über:

1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
3. Massnahmen der sozialen Hilfe,
4. administrative oder strafrechtliche Verfolgungen und Sanktionen.

Den besonders schützenswerten Daten stellt das Datenschutzgesetz die sog. Persönlichkeitsprofile gleich, d.h. die «Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt» (Art. 3 Bst. d. DSG).

Diese auf Gesetzesebene herausgehobenen Kategorien können auch unter verfassungsrechtlichem Blickwinkel eine spezielle Bedeutung erlangen. So gelten bei der Bearbeitung von besonders schützenswerten Daten bzw. Persönlichkeitsprofilen regelmässig erhöhte Anforderungen hinsichtlich der gesetzlichen Grundlage, des öffentlichen Interesses und der Verhältnismässigkeit bzw. der damit verbundenen Interessenabwägungen[51]

3. Weitere Verfassungsnormen und Regelungen auf internationaler Ebene (Hinweise)

Der Vollständigkeit halber sei hier darauf hingewiesen, dass neben den bereits erörterten Grundrechten (Art. 13 und Art. 10 BV) auch weitere Verfassungsnormen dem Schutz der Persönlichkeit dienen, so namentlich Art. 7 BV (Schutz der Menschenwürde), Art. 8 BV (Rechtsgleichheit), Art. 29 BV (Recht auf Akteneinsicht als Teilgehalt des Anspruchs auf rechtliches Gehör[52]), Art. 119 BV (Schutz genetischer Daten).

Relevant ist sodann auch der neuartige Art. 35 BV. Diese Bestimmung verlangt, dass die Grundrechte in der ganzen Rechtsordnung zur Geltung kommen, und auferlegt es den Behörden, dafür zu sorgen, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden.

[51] Vgl. Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 41 und 49.
[52] Zu Abgrenzung und Unterschieden vgl. z.B. Jörg Paul Müller (Anm. 20), S. 49.

Nach heutigem Stand von Rechtsprechung und Lehre darf man davon ausgehen, dass die Grundrechte der neuen Bundesverfassung mindestens den gleichen Schutz bieten wie die einschlägigen Garantien internationaler Übereinkommen zum Schutz der Menschenrechte und Grundfreiheiten[53].

Dementsprechend können sich die folgenden Überlegungen auf den grundrechtlich gewährleisteten Persönlichkeitsschutz gemäss Bundesverfassung konzentrieren. Erwähnt sei immerhin Folgendes:

Im Rahmen des Europarates wird der grundrechtliche Persönlichkeitsschutz namentlich durch Art. 8 EMRK[54] sowie durch das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten gewährleistet, das für die Schweiz am 1. Februar 1998 in Kraft trat[55]. Verschiedene Empfehlungen des Ministerkomitees behandeln Fragen des Datenschutzes, auch im Zusammenhang mit persönlichen Identifikationsnummern (z.B. im Sozialversicherungsbereich)[56]. Speziell mit Fragen des Einsatzes von Personenidentifikatoren befasst sich eine 1991 im Schoss des Europarates entstandene Studie[57].

Im Rahmen der Europäischen Union hat das Anliegen des Schutzes personenbezogener Daten Eingang gefunden in die – rechtlich vorerst nicht verbindliche – Charta der Grundrechte der Europäischen Union (vgl. Art. 8)[58]. Die EG-Datenschutz-Richtlinie von 1995 überlässt es in ihrem Art. 8 Abs. 7 – in Anbetracht sehr unterschiedlicher Verwaltungskulturen und Datenschutztraditionen – den Mitgliedstaaten festzulegen, unter welchen Bedingungen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung Gegenstand einer Datenverarbeitung sein dürfen[59].

[53] Vgl. in diesem Sinn z.B. BGE 128 I 63 (69).
[54] Zu Art. 8 EMRK vgl. etwa Luzius Wildhaber/Stephan Breitenmoser, in: Internationaler Kommentar zur EMRK, Köln usw. 1994 ff., Kommentar zu Art. 8 EMRK; Jochen Abr. Frowein/Wolfgang Peukert, EMRK-Kommentar, 2. Aufl., Kehl usw. 1996, S. 337 ff.; Robert Uerpmann (Anm. 36), S. 47 ff.
[55] Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SR 0.235.1). Vgl. Rainer J. Schweizer, Datenschutz in der Schweiz und in Europa – Auswirkungen des europäischen Datenschutzrechts auf die Schweiz, in: Astrid Epiney/Marianne Freiermuth (Hrsg.), Datenschutz in der Schweiz und in Europa, Fribourg 1999, S. 25 ff.
[56] Vgl. z.B. Ziffer 5.1 der Empfehlung R (86) 1 des Ministerkomitees des Europarates zum Schutz personenbezogener Daten, die für Zwecke der sozialen Sicherheit verwendet werden.
[57] Comité d'experts sur la protection des données (CJ-PD), Les numéros personnels d'identification: leur mise en oeuvre, leur utilisation et la protection des données.
[58] Amtsblatt der Europäischen Gemeinschaften Nr. C 364/1 vom 18.12.2000.
[59] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Die Datenschutz-Richtlinie erging gestützt auf den heutigen Art. 95 (ex-Art. 100a) EGV. Vgl. Ulrich Dammann/ Spiros Simitis, EG-Datenschutzrichtlinie: Kommentar, Baden-Baden 1997, S. 173 f.

4. Fazit

Der verfassungsrechtliche Persönlichkeitsschutz umfasst neben dem in Art. 13 Abs. 2 BV ausdrücklich genannten Anspruch auf Schutz vor Missbrauch personenbezogener Daten eine ganze Reihe von anerkannten – im Verfassungstext nicht direkt angesprochenen – Schutzgehalten. Für den Zweck dieser Untersuchung ist es nicht entscheidend,

- ob man diese Schutzgehalte der datenschutzspezifischen Grundrechtsbestimmung (Art. 13 Abs. 2 BV) zuordnet oder den allgemeineren bzw. althergebrachten Grundrechtspositionen (Anspruch auf Schutz der Privatsphäre, Art. 13 Abs. 1 BV; persönliche Freiheit, jetzt Art. 10 Abs. 2 BV) und
- wie man die Grenzen zwischen Art. 13 Abs. 2, Art. 13 Abs. 1 und Art. 10 Art. 2 BV im Einzelnen zieht.

Festzuhalten ist im Weiteren, dass der verfassungsrechtliche Persönlichkeitsschutz sich nicht in der klassischen abwehrrechtlichen Grundrechtsdimension erschöpft. Der Staat und seine Organe sind darüber hinaus generell dazu verpflichtet, die Grundrechte – und somit prinzipiell auch das Grundrecht auf Datenschutz oder informationelle Selbstbestimmung – in der ganzen Rechtsordnung zur Geltung zu bringen (Art. 35 Abs. 1 BV).

III. Einführung eines Personenidentifikators als zulässiger Grundrechtseingriff?

1. Problemkreise

Für die allfällige Einführung und Verbreitung eines koordinierten eidgenössischen Personenidentifikator sind unterschiedliche Szenarien denkbar. Für den Zweck der vorliegenden Untersuchung werden folgende Vorgänge unterschieden:

(1) Vergabe des Personenidentifikators

Hier geht es um die Zuordnung einer persönlichen Zeichenfolge an alle zu erfassenden Personen («Durchnummerierung» der schweizerischen Bevölkerung) in Form einer Erstvergabe des Personenidentifikators und in Form der späteren laufenden Vergabe.

(2) Aufnahme des Personenidentifikators in Amtliche Register

Hier geht es um die Bezeichnung der Register, in denen ein koordinierter eidgenössischer Personenidentifikator geführt wird (Festlegen des Einsatzbereichs).

Der Vorentwurf für ein Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister sieht Folgendes vor:

- Der eidgenössische Personenidentifikator soll in allen kantonalen und kommunalen Einwohnerregistern zum Einsatz kommen (im Sinn einer Vorgabe des Bundes; vgl. Art. 6 VE).
- Im Weiteren sollen alle Bundesstellen verpflichtet werden, in ihren Personenregistern den einheitlichen Personenidentifikator zu führen (wiederum im Sinne einer zwingenden gesetzlichen Vorgabe; vgl. Art. 13 VE).
- Sodann sollen weitere staatliche Stellen (z.B. kantonale oder kommunale Stellen) ermächtigt werden können, den eidgenössischen Personenidentifikator für den Vollzug gesetzlicher Aufgaben zu nutzen (im Sinne eines Zur-Verfügung-Stellens; Art. 14 VE).

(3) *Anderweitige Nutzung des Personenidentifikators*

In Betracht gezogen wird neben der Nutzung für statistische Zwecke auch eine Nutzung für weitere Zwecke (Vollzug gesetzlicher Aufgaben). Aus der Sicht des Persönlichkeitsschutzes geht es hier um vielfältige Fragen des Datenbearbeitens: Beschaffen (Erheben), Aufbewahren, Verwenden, Bekanntgeben (Einsichtgewähren; Weitergeben an Dritte, z.B. andere Behörden oder Private; Veröffentlichen) usw.

Von besonderem Interesse ist dabei, dass mit Hilfe eines einheitlichen Personenidentifikators die Verknüpfung von Daten verschiedener Datensammlungen erleichtert wird (Problem der «Verknüpfbarkeit» und des daraus resultierenden Gefährdungspotenzials).

Die folgenden Untersuchungsschritte orientieren sich an dieser Gliederung, wobei es nicht darum gehen wird, flächendeckend alle erdenklichen Fragen aufzuwerfen und zu behandeln, sondern vielmehr, die neuralgischen Punkte herauszuarbeiten.

2. Kriterien der verfassungsrechtlichen Prüfung im Überblick

In der neuerer Rechtsprechung und Rechtslehre geht man davon aus, dass die Zulässigkeit von staatlichen Eingriffen in das Grundrecht auf Datenschutz bzw. das Recht auf informationelle Selbstbestimmung anhand der Kriterien des Art. 36 BV zu beurteilen sind[60].

[60] In diesem Sinn etwa BGE 128 I 63 (69) (Datenbearbeitung als Eingriff in das Grundrecht der persönlichen Freiheit, so dass die Kriterien des Art. 36 BV erfüllt sein müssen); Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 41; Eidgenössisches Departement des Innern (EDI), „Der eidgenössische Personenidentifikator – Projektskizze" (Bern, 31. Mai 2002), S. 10. Vgl. auch Art. 8 Abs. 2 EMRK sowie BVerfGE 65, 1 (44).

Zu prüfen ist mithin, ob die staatliche Massnahme eine genügende gesetzliche Grundlage hat, durch ein überwiegendes öffentliches Interesse gerechtfertigt und verhältnismässig ist und den unantastbaren Kerngehalt des Grundrechts wahrt. Bei schwerwiegenden Eingriffen – so unter Umständen im Zusammenhang mit besonders schützenswerten Personendaten – muss die Rechtsgrundlage in einem Gesetz im formellen Sinn enthalten sein[61].

Eine solche Überprüfung ist freilich nur am Platz, wenn die fragliche staatliche Massnahme den grundrechtlich geschützten Bereich tangiert. Dieser geschützte Bereich wird durch die vorne genannten Ansprüche und Grundsätze näher bestimmt (vgl. Ziffer II.2.): Grundsatz der rechtmässigen Beschaffung; der Bearbeitung nach Treu und Glauben; der Offenheit und Transparenz der Bearbeitung («Erkennbarkeit»); der Zweckbindung der Bearbeitung; der Verhältnismässigkeit der Bearbeitung; der Richtigkeit der Datenbearbeitung; der Wahrung der Datensicherheit; der Beschränkung der Datenweitergabe ins Ausland; Anspruch auf Einsicht, Berichtigung und Löschung.

Diese Teilgehalte des Grundrechts auf Datenschutz werden nicht in allen vorne skizzierten Problemkreisen gleichermassen relevant sein.

Im Zentrum der nachstehenden Überlegungen werden die *Erfordernisse des öffentlichen Interesses* und *der Verhältnismässigkeit* stehen. Letzteres wird vom Bundesgericht wie folgt umschrieben:

«Das verfassungsmässige Gebot der Verhältnismässigkeit verlangt, dass staatliche Hoheitsakte für das Erreichen eines im übergeordneten öffentlichen Interesse liegenden Zieles geeignet, notwendig und für den Betroffenen zumutbar sein müssen (...). Erforderlich ist eine vernünftige Zweck-Mittel-Relation (...)[62].»

Nicht näher geprüft wird im Folgenden die Wahrung des Kerngehalts – dies in der (vorläufigen) Annahme, dass man mit den in Betracht gezogenen Massnahmen aus heutiger Sicht nicht in die Nähe eines allfälligen unantastbaren Grundrechtskerns vordringen wird (dessen Konturen im Fall des Grundrechts auf Datenschutz, Art. 13 Abs. 2 BV, heute noch nicht genau absehbar sind).

Nicht im Einzelnen untersucht wird vorerst auch die Frage der Stufe der erforderlichen Rechtsgrundlagen (Gesetz oder Verordnung?) und die Frage der näheren Ausgestaltung (Normbestimmtheit).

[61] Vgl. Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 41. – Vgl. auch Art. 17 Abs. 2 DSG.
[62] BGE 128 I 92 (95).

3. Zulässigkeit der Vergabe eines Personenidentifikators aus grundrechtlicher Sicht

Für die Klärung der Frage, inwiefern die «Durchnummerierung» der Bevölkerung (Erstvergabe und laufende Vergabe eines Personenidentifikators) unter dem Aspekt des verfassungsrechtlichen Persönlichkeitsschutzes problematisch sein könnte, ist die rechtliche Qualifizierung des Personenidentifikators (aus grundrechtlicher Sicht) von Bedeutung.

Bei der Einführung eines Personenidentifikators wird eine Ziffernfolge unauflöslich mit einer bestimmten Person verknüpft, wobei jeweils eine sichere Identifikation der Person nötig ist. Mit der Vergabe eines Personenidentifikators entsteht ein personenbezogenes Datum. Die Vergabe ist somit eine datenschutzrechtlich relevante Bearbeitung von Personendaten. Die Eigenart des Personenidentifikators besteht darin, dass es sich nicht um ein natürliches, sondern um ein behördlich geschaffenes, gewissermassen «künstliches» Datum handelt.

Aus der Sicht des verfassungsrechtlichen Persönlichkeitsschutzes stellt sich die Frage, ob bereits die Vergabe einer persönlichen Identifikationsnummer als solche einen Grundrechtseingriff bedeutet – mit der Folge, dass die Vergabe nur zulässig ist, wenn sie den Anforderungen des Art. 36 BV genügt, d.h. sich namentlich auf eine hinreichende rechtliche Grundlage stützen kann, durch ein öffentliches Interesse gerechtfertigt und verhältnismässig ist.

Diese Frage hat in Rechtsprechung und Rechtslehre bisher so weit ersichtlich kaum Aufmerksamkeit erlangt.

Wenn man mit der neueren Rechtsprechung und Lehre von der Annahme ausgeht, dass grundsätzlich jeder Umgang mit personenbezogenen Daten den Schutzbereich des Grundrechts der persönlichen Freiheit bzw. des Grundrechts auf Datenschutz (Art. 13 Abs. 2 BV) bzw. des Rechts auf informationelle Selbstbestimmung berührt[63], so ist die Frage zu bejahen[64]: Auch die Vergabe eines Personenidentifikators berührt den grundrechtlichen Schutzbereich. Unter den Bedingungen der automatisierten Datenverarbeitung gibt es kein «belangloses» Datum mehr[65].

[63] In diesem Sinn z.B. BGE 128 I 63 (69); BGE 125 I 257 (260); Jörg Paul Müller (Anm. 20), S. 45.
[64] Wenn man den Vorgang allein unter dem Blickwinkel des (allgemeinen und subsidiären) Persönlichkeitsschutzes gemäss Art. 10 Abs. 2 BV betrachtet, könnten unter Umständen Zweifel am Vorliegen eines Grundrechtseingriffs aufkommen, weil ja die persönliche Freiheit nicht alle Aspekte der Persönlichkeit schützt, sondern nur die elementaren Erscheinungsformen der Persönlichkeitsentfaltung (vgl. z.B. Jörg Paul Müller, Anm. 20, S. 43 f.). Das Bundesgericht hat indes bisher im Bereich der Datenbearbeitung stets ein weites Verständnis des grundrechtlichen Schutzbereichs zugrunde gelegt. Vgl. z.B. BGE 128 I 63 (69).
[65] Vgl. BVerfGE 65, 1 (45).

Allerdings handelt es sich – jedenfalls im Fall eines nichtsprechenden Identifikators[66] – um einen Eingriff, der nicht schwer wiegt. Ein Personenidentifikator für sich allein gehört nicht zu den «besonders schützenswerten Personendaten» oder den sog. Persönlichkeitsprofilen, solange die «Durchnummerierung» der Bevölkerung, darauf beschränkt bleibt, jeder Person eine bestimmte, nichtsprechende Ziffernfolge zuzuordnen.

Eine Rechtfertigung eines solchen Eingriffs erscheint unter dem Aspekt des öffentlichen Interesses (z.B. Einsparungen und Qualitätssteigerung bei der Statistik) wie unter dem Aspekt der Verhältnismässigkeit aus heutiger Sicht prinzipiell möglich.

Problematisch wird die Vergabe erst in Verbindung mit weiteren Vorgängen wie Einfügen in ein Register, Erschliessbarkeit weiterer, unter Umständen auch besonders schützenswerter Personendaten. Darauf wird noch einzugehen sein.

Unter den vorne genannten Grundsätzen des Datenschutzes verdienen hier der Grundsatz der Offenheit und Transparenz und der Grundsatz der Zweckbindung Aufmerksamkeit.

Aus dem Transparenzgrundsatz ergibt sich das Postulat, dass der behördlich geschaffene Personenidentifikator der betreffenden Person grundsätzlich nicht vorenthalten werden darf, sofern eine Geheimhaltung gegenüber dem Träger nicht durch überwiegende öffentliche Interessen gerechtfertigt sowie verhältnismässig ist. Aus dem Grundsatz der Zweckbindung kann man ableiten, dass die Schaffung eines Personenidentifikators einem bestimmten, definierten Zweck (z.B. für Zwecke der Statistik) zu dienen hat und nicht gewissermassen auf Vorrat erfolgen soll. Ein solcher definierter Zweck ist gegeben, wenn – wie vorgesehen – ein koordinierter Personenidentifikator für statistische Zwecke geschaffen werden soll.

Die (gleichzeitige oder spätere) Nutzung für allfällige weitere Zwecke bedeutet eine Abweichung vom Grundsatz der Zweckbindung. Eine solche Lockerung erscheint aus verfassungsrechtlicher Sicht nicht von vornherein ausgeschlossen[67], sofern die Voraussetzungen für eine Beschränkung des Grundrechts auf Datenschutz erfüllt sind. Darauf wird zurückzukommen sein (vgl. Ziffer 4.).

[66] Anders verhielte es sich bei einem sprechenden Identifikator, der Aufschluss über besonders schützenswerte Personendaten (z.B. die Religionszugehörigkeit usw.) gibt.
[67] Zur Möglichkeit einer Lockerung der Zweckbindung im besonders gelagerten Bereich der Statistik vgl. das Volkszählungsurteil des deutschen Bundesverfassungsgerichts, BVerfGE 65, 1 (47 ff.). Zur Möglichkeit einer Lockerung der Zweckbindung im Zusammenhang mit der Archivierung vgl. Beat Rudin (Anm. 37), S. 251 ff. – Kritisch zur allgemeinen Tendenz einer schleichenden Lockerung der Zweckbindung Bruno Baeriswyl (Anm. 11), S. 57.

Zusammenfassend kann man festhalten, dass es sich bei der Vergabe des Personenidentifikators um einen datenschutzrechtlich relevanten Vorgang handelt, der nach heutigem Stand von Rechtsprechung und Lehre einen Grundrechtseingriff bedeutet, jedoch nicht besonders schwer wiegt und grundsätzlich rechtfertigungsfähig erscheint, sofern die üblichen Schutzvorkehren greifen.

4. Zulässigkeit des Einfügens eines Personenidentifikators in amtliche Register aus grundrechtlicher Sicht

a. Einfügen für Zwecke der Statistik

Von den verschiedenen Teilgehalten des Grundrechts auf Datenschutz stehen hier die Grundsätze der rechtmässigen Beschaffung, der Transparenz, der Zweckbindung und der Verhältnismässigkeit im Vordergrund.

Der Grundsatz der rechtmässigen, d.h. rechtlich hinreichend abgestützten Beschaffung (des Personenidentifikators) ist gewahrt, wenn – wie vorgesehen – registerführende Stellen ausdrücklich per Gesetz zur Führung des eidgenössischen Personenidentifikators verpflichtet werden (kantonale und kommunale Einwohnerregister, Bundesstellen) oder aber ausdrücklich dazu ermächtigt werden (weitere kantonale Stellen). Bei Vorliegen derartiger Rechtsgrundlagen dürfte das Einfügen des Personenidentifikators in Register zu statistischen Zwecken auch unter dem Blickwinkel der Offenheit und Transparenz grundsätzlich statthaft sein[68].

Eine andere Frage ist, inwieweit Verwaltungsbehörden befugt sein sollen, von Bürgerinnen und Bürgern, die mit ihnen in Kontakt treten, die Angabe des Personenidentifikators zu verlangen. Unter dem Aspekt der Rechtmässigkeit der Datenbeschaffung ist eine entsprechende Rechtsgrundlage zu fordern.

Einer genaueren Betrachtung bedarf das Einfügen und Führen eines koordinierten Personenidentifikators in eidgenössischen, kantonalen und kommunalen Personenregistern unter dem Aspekt des Zweckbindungsgrundsatzes, welche «Schutz gegen Zweckentfremdung[69]» bietet und gewöhnlich durch entsprechende gesetzliche Weitergabe- und Verwertungsverbote gesichert wird.

[68] Vgl. immerhin zur Problematik indirekter Erhebungen Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 50.

[69] So das deutsche Bundesverfassungsgericht in seinem Volkszählungsurteil: BVerfGE 65, 1 (46). Das Bundesverfassungsgericht spricht dabei auch von einem „Grundsatz der Trennung von Statistik und Vollzug": BVerfGE 65, 1 (61).

Aus verfassungsrechtlicher Sicht ergeben sich dann keine spezifischen Probleme, wenn ein für statistische Zwecke geschaffener Personenidentifikator tatsächlich allein für statistische Zwecke genutzt wird. Zwar werden bei der Durchführung statistischer Erhebungen mitunter auch personenbezogene Daten erhoben, die zu den besonders schützenswerten gehören bzw. der Erstellung von Persönlichkeitsprofilen dienen können. Da die Statistik nicht auf Individuen bezogen ist, sondern auf die Gewinnung von aggregierten und anonymisierten Erkenntnissen[70], erscheint ein Einsatz von Personenidentifikatoren für rein statistische Zwecke aus grundrechtlicher Sicht grundsätzlich rechtfertigungsfähig, sofern eine rechtzeitige Anonymisierung gewährleistet ist.

b. Ermöglichung des Einsatzes für weitere Zwecke

Heikel erscheinen dagegen aus verfassungsrechtlicher Sicht Konstellationen der folgenden Art (die sich nicht scharf voneinander abgrenzen lassen):

- Nutzung eines ursprünglich für statistische Zwecke geschaffenen Personenidentifikators für weitere Zwecke (Einsatz für die Erfüllung anderer als statistischer Aufgaben);
- Schaffung eines Personenidentifikators für noch unbestimmte Zwecke.

Entsprechende Vorgänge geraten mit dem im Grundrecht auf Datenschutz (Art. 13 Abs. 2 BV) verankerten Grundsatz der Zweckbindung in Konflikt. Eine Relativierung dieses Grundsatz ist, wie gesehen, nicht unter allen Umständen ausgeschlossen. Eine solche Relativierung setzt jedoch – neben einer hinreichenden gesetzlichen Grundlage und der Wahrung des Grundrechtskerngehalts – die Rechtfertigung durch ein überwiegendes öffentliches Interesse und die Wahrung der Verhältnismässigkeit voraus.

c. Öffentliches Interesse für eine Lockerung der Zweckbindung?

Als Motive für eine Ausdehnung des Einsatzbereichs eines koordinierten Personenidentifikators über statistische Zwecke hinaus werden etwa genannt (vgl. auch vorne Ziffer I.2.b.):

- Rationalisierung und Kosteneinsparungen bei der Verwaltungsführung (insb. bei der Registerführung),
- Vereinfachung und Optimierung des Verkehrs (Datenfluss) zwischen Behörden bzw. Registern und mit den Bürgerinnen und Bürgern,

[70] Zu den Besonderheiten der Statistik aus datenschutzrechtlicher Sicht vgl. Jean-Philippe Walter (Anm. 10); Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 50; sowie das Volkszählungsurteil des deutschen Bundesverfassungsgerichts, BVerf- GE 65, 1 (47 ff.).

- Verbesserung der Datenqualität und der Zuverlässigkeit von Registern.

Grundsätzlich handelt es sich bei diesen Interessen um legitime öffentliche Interessen. Dies gilt gemäss Rechtsprechung des Bundesgerichts namentlich auch für das Interesse an einem nicht übermässigen Verwaltungsaufwand[71].

In der gemäss Art. 36 Abs. 2 BV durchzuführenden Interessenabwägung (vgl. auch Art. 5 Abs. 2 BV) sind diese Gesichtspunkte den grundrechtlich geschützten Interessen der Bürgerinnen und Bürger gegenüberzustellen.

Diese Abwägung kann sinnvoll nur in Kenntnis der jeweiligen näheren Umstände vorgenommen werden. Pauschale Hinweise auf mögliche Erleichterungen und Verbesserungen genügen nicht.

Im Rahmen der vorliegenden gutachterlichen Abklärung kann keine abschliessende Beurteilung abgegeben werden. Immerhin kann man aus heutiger Sicht festhalten, dass Interessen der genannten Art nicht ohne Weiteres genügen, um gewichtigere Grundrechtseingriffe zu rechtfertigen. Weiter kann festgehalten werden, dass eine kontextbezogene Abwägung – in Kenntnis der jeweiligen konkreten öffentlichen Interessen und Rahmenbedingungen – erforderlich ist. Diese Interessenabwägung muss überdies durch eine zur grundrechtlichen Abwägung demokratisch hinreichend legitimierte Stelle vorgenommen werden. Als unzulässig erscheint unter dem Aspekt des verfassungsrechtlichen Persönlichkeitsschutzes eine Pauschal-Freigabe (z.B. mit dem vorerst alleinigen Ziel, «Goodwill» für die Einführung eines koordinierten Personenidentifikators zu schaffen).

Auf die Problematik einer Lockerung des Zweckbindungsgrundsatzes wird noch einmal einzugehen sein, wenn die aus dem verfassungsrechtlichen Persönlichkeitsschutz fliessenden staatlichen Schutzpflichten näher beleuchtet werden (vgl. Ziffer IV.).

d. Verhältnismässigkeit einer Lockerung der Zweckbindung?

Unter dem Aspekt der Verhältnismässigkeit interessiert die Frage, ob der Einsatz eines koordinierten Personenidentifikators «für das Erreichen eines im übergeordneten öffentlichen Interesse liegenden Zieles geeignet, notwendig und für den Betroffenen zumutbar» ist[72]. Aus dieser allgemeinen Umschreibung, die auch bei der Klärung der hier interessierenden Fragen zugrunde zu legen ist, geht hervor, dass die Prüfung der Verhältnismässigkeit nicht «abstrakt» vorgenommen werden kann. Man kann einer

[71] Vgl. z.B. BGE 101 Ia 341 (344).
[72] BGE 128 I 92 (95).

Massnahme nur in Bezug auf einen näher bestimmten Zweck Verhältnismässigkeit attestieren.

- Die Eignung kann nur bejaht werden, wenn die fragliche Massnahme zur Erreichung eines mehr oder weniger *definierten Ziels* taugt.
- Die Erforderlichkeit kann nur bejaht werden, wenn mit Bezug auf einen *näher bestimmten Zweck* keine andere, ebenso gut geeignete, aber weniger eingreifende Alternative zur Verfügung steht.
- Die Zumutbarkeit bzw. die Vernünftigkeit der Zweck-Mittel- Relation kann nur beurteilt werden auf Grund eine *Abwägung*, die auch die *Zweckbestimmung* der Massnahme einbezieht.

Für den hier interessierenden Zusammenhang ergibt sich aus diesen Überlegungen Folgendes:

Bei der Beurteilung der Verhältnismässigkeit ist ein Vorgehen geboten, das nach einzelnen Zielsetzungen und Einsatzbereichen differenziert. Es ist mithin getrennt – d.h. jeweils mit Blick auf eine näher bestimmte Zielsetzung – zu prüfen und auszuweisen, dass das besagte Ziel (die Legitimität des Ziels einmal unterstellt)

- mit dem Einsatz eines Personenidentifikators erreicht werden kann (Eignungsnachweis);
- nicht mit anderen, unter dem Blickwinkel der Eignung grundsätzlich gleichwertigen, jedoch unter dem Blickwinkel des verfassungsrechtlichen Persönlichkeitsschutzes weniger einschneidenden Mitteln erreicht werden kann (Erforderlichkeitsnachweis);
- in einer vernünftigen Relation zum eingesetzten Mittel steht (Zumutbarkeitsnachweis).

Der Eignungsnachweis dürfte für Zielsetzungen wie Kosteneinsparung, Verwaltungsrationalisierung, Verbesserung der Datenqualität in der Regel nicht besonders schwer fallen; dies um so mehr, als das Bundesgericht an die grundrechtliche Eignungsprüfung im Allgemeinen keine besonders hohen Anforderungen stellt. Der Erforderlichkeitsnachweis hingegen dürfte nicht immer leicht zu erbringen sein. Denn die in Betracht fallenden Ziele – wie Rationalisierung, Kosteneinsparungen, Optimierung des Datenflusses zwischen Behörden bzw. Registern, Vereinfachung des Verkehrs mit den Bürgerinnen und Bürgern, Verbesserung der Datenqualität und der Zuverlässigkeit von Registern – lassen sich gewöhnlich auch mit Hilfe anderer Instrumente erreichen.

Im hier interessierenden Zusammenhang spielt eine entscheidende Rolle, welche Massnahmen man unter dem Blickwinkel der Eignung als grundsätzlich gleichwertig einstuft. Konkret: Wie ist im Rahmen der Verhältnismässigkeitsprüfung eine Massnahme einzuordnen und zu bewerten, die zwar weniger einschneidend, jedoch teurer ist? Diese Frage ist nicht abstrakt zu beantworten, sondern mit Blick auf den konkreten Einsatzbereich und unter Berücksichtigung von Überlegungen zur Zumutbarkeit.

Im Rahmen des Zumutbarkeitsnachweises ist namentlich das einem koordinierten Personenidentifikator innewohnende Gefährdungspotenzial zu berücksichtigen (das grösser ist, wenn besonders schützenswerte Daten im Spiel sind). Neben dem zu erwartenden Nutzen sind daher auch die mit dem Einsatz eines koordinierten Personenidentifikators verbundenen *Gefahren* (für verfassungsrechtlich geschützte Interessen des Individuums) in die Abwägung einzubeziehen. Ein besonderes Gewicht kommt solchen Gefahren in der Interessenabwägung dann zu, wenn der Eintritt der Gefahr nicht eine bloss entfernte Möglichkeit ist und wenn es um besonders gewichtige Individualinteressen geht (z.B. um besonders schützenswerte Personendaten).

Eine potenzielle Gefahr für das Individuum und sein verfassungsrechtlich geschütztes Persönlichkeitsrecht resultiert aus der Tatsache, dass personenbezogene Daten, die an verschiedensten Orten aufbewahrt werden, mit Hilfe eines koordinierten Personenidentifikators verknüpfbar werden. Vereinfachend lässt sich sagen, dass die Gefahr um so grösser ist, je weiter verbreitet der koordinierte Personenidentifikator ist. Wie schwer die Gefahr wiegt, lässt sich auch hier nicht abstrakt sagen. Die Antwort hängt nicht zuletzt davon ab, welche sichernden Massnahmen ergriffen werden und wie wirksam diese sind.

e. Fazit

Zusammenfassend kann man im jetzigen Zeitpunkt Folgendes festhalten: Es ist nicht von vornherein ausgeschlossen, dass eine Ausdehnung des Einsatzbereichs eines vorab für statistische Zwecke geschaffenen Personenidentifikators im öffentlichen Interesse liegen kann und als verhältnismässig eingestuft werden kann und dass die damit verbundene Lockerung der Zweckbindung unter grundrechtlichem Blickwinkel als gerechtfertigt erscheinen kann.

Eine derartige Schlussfolgerung darf aber nicht das Ergebnis einer Pauschalbeurteilung sein. Sie muss sich vielmehr auf eine sorgfältige Interessenabwägung und Verhältnismässigkeitsprüfung abstützen können anhand der konkreten Gegebenheiten im geplanten Einsatzbereich.

Bei dieser Ausgangslage erscheint es verfassungsrechtlich höchst problematisch, den Einsatz eines koordinierten eidgenössischen Personenidentifikators gewissermassen pauschal für nicht-statistische Verwaltungszwecke freizugeben.

5. Anderweitige Nutzung des Personenidentifikators aus grundrechtlicher Sicht (Hinweise)

Weitere grundrechtlich relevante Fragestellungen treten zu Tage, wenn man die Einführung eines koordinierten eidgenössischen Personenidentifikators unter dem Aspekt allfälliger künftiger Möglichkeiten des Einsatzes im Behördenalltag näher betrachtet. Unter den verschiedenen Teilgehalten des Grundrechts auf Datenschutz stehen auch hier die Grundsätze der rechtmässigen Beschaffung, der Transparenz, der Zweckbindung und der Verhältnismässigkeit im Vordergrund.

Der Rechtmässigkeitsgrundsatz ist, wie bereits erörtert, gewahrt, wenn registerführende Stellen ausdrücklich zur Führung des eidgenössischen Personenidentifikators verpflichtet bzw. ermächtigt werden. Darüber hinaus stellt sich die Frage, unter welchen Voraussetzungen weitere Verwaltungsstellen befugt sind, sich den koordinierten Personenidentifikator zu beschaffen, insbesondere befugt sind, von Bürgerinnen und Bürgern, die mit ihnen in Kontakt treten (beispielsweise wenn sie Einsicht in amtliche Dokumente nehmen wollen oder wenn sie sich um eine Stelle bewerben), zu verlangen, dass sie ihren Personenidentifikator angeben.

Angesichts der potenziellen Gefahren für das verfassungsrechtlich geschützte Persönlichkeitsrecht, die jede Weiterverbreitung des Personenidentifikators in sich birgt, ist zu fordern, dass eine Erhebung auf diesem Weg nur erfolgen darf, wenn eine hinreichend bestimmte Rechtsgrundlage dies vorsieht.

Aus der Sicht des verfassungsrechtlichen Persönlichkeitsschutzes ist darüber hinaus zu fordern, dass eine derartige Rechtsgrundlage nur bei Vorliegen eines hinreichenden öffentlichen Interesses und unter Wahrung der Verhältnismässigkeit – d.h. nicht auf «Vorrat» – geschaffen wird.

Unter dem Aspekt der Offenheit und Transparenz ist zu postulieren, dass für die Bürgerinnen und Bürger erkennbar ist, welche Behörden den koordinierten Personenidentifikatoren führen dürfen.

Neben der Erhebung wirft auch eine allfällige Weitergabe des Personenidentifikators verfassungsrechtliche Fragen auf. Die latente Gefahr von verfassungsrechtlich relevanten Persönlichkeitsverletzungen wird nicht nur durch das Einfügen eines koordinierten Personenidentifikators in verschiedene Register (vgl. Ziffer 4.) erhöht, sondern unter Umständen auch durch die Weiterverbreitung im Einzelfall, so z.B. bei einer Weitergabe:

- von Behörde zu Behörde,
- von Behörden an Private,
- von Privaten an andere Private (nicht zuletzt: durch den «Träger» des Personenidentifikators an andere Private).

Zwar handelt es sich nicht bei all diesen Vorgängen um eigentliche Grundrechtseingriffe, da das Grundrecht auf Datenschutz keine unmittelbare Drittwirkung im Verhältnis zwischen Privaten erlangt. Gleichwohl sind solche Vorgänge unter dem Blickwinkel des verfassungsrechtlichen Persönlichkeitsschutzes nicht irrelevant (vgl. Ziffer IV.), da die Bundesverfassung den Staat dazu verpflichtet (Art. 35 Abs. 1 BV), die Grundrechte – somit auch das Grundrecht auf Datenschutz – in der ganzen Rechtsordnung – mithin auch im Verhältnis zwischen Privaten – zur Geltung zu bringen (vgl. auch Art. 35 Abs. 3 BV).

Eine dem Gedanken des verfassungsrechtlichen Persönlichkeitsschutzes verpflichtete gesetzliche Regelung der Weitergabe ist daher geboten. Sie erscheint auch deshalb geboten, weil mit der Weitergabe – auch jener im Einzelfall – die Gefahr steigt, dass der Grundsatz der Zweckbindung unterlaufen wird (zumal dann, wenn letztlich faktisch die Empfänger mehr oder weniger selbst über Einsatzzweck und Einsatzbereich befinden).

Im geltenden Recht versucht Art. 25 VDSG, dieser Gefahrenlage entgegenzuwirken: Danach muss die Verwendung von persönlichen Identifikationsnummern durch andere (eidgenössische oder kantonale) Behörden sowie durch private Personen vom «ausgebenden» Bundesorgan genehmigt werden (Abs. 2). Diese Genehmigung setzt voraus, dass ein enger Zusammenhang besteht zwischen der vorgesehenen Datenbearbeitung und jener Datenbearbeitung, für welche die persönliche Identifikationsnummer geschaffen wurde.

Bereits mit Blick auf den Einsatz der heute bekannten Personenidentifikatoren gewährleistet diese Regelung freilich keinen adäquaten Schutz der einschlägigen Verfassungsgehalte, einerseits weil die Regelung nicht alle Identifikatoren erfasst (die AHV-Gesetzgebung bleibt ausgeklammert; vgl. Art. 25 Abs. 4 DSG), andererseits weil sich eine blosse Verordnungsbestimmung gegen gegenteilige Regelungen der Gesetzesstufe und gegen späteres Verordnungsrecht nicht durchzusetzen vermag.

Im Fall der Einführung eines koordinierten eidgenössischen Personenidentifikators muss diesen verfassungsrechtlichen Gehalten bereits bei der Schaffung und Ausgestaltung der formell-gesetzlichen Rechtsgrundlagen in geeigneter Weise Rechnung getragen werden.

Die vorstehenden Überlegungen lassen erkennen, dass die Problematik der Einführung eines koordinierten eidgenössischen Personenidentifikators sich nicht in der abwehrrechtlichen Grundrechtsfunktion erschöpft, die bisher im Zentrum stand. Vielmehr ist zumeist auch die Frage nach flankierenden Schutzmassnahmen (bzw. nach staatlichen Schutzpflichten) angesprochen. Dieser Eindruck erhärtet sich, wenn man die neuralgischen Punkte im Überblick betrachtet.

6. Zwischenergebnis: neuralgische Punkte

Auf Grund der bisherigen Ausführungen lassen sich einige neuralgische Punkte herausschälen:

- Die Schaffung und Vergabe eines koordinierten eidgenössischen Personenidentifikator als solche bewirkt aus der Sicht des verfassungsrechtlichen Persönlichkeitsschutzes nur einen vergleichsweise geringfügigen Grundrechtseingriff. Das Hauptproblem liegt bei der latenten Gefahr von Missbräuchen, wobei die Missbrauchsgefahren im Einzelnen schwer abzuschätzen sind, solange die späteren Verwendungen nicht ohne Weiteres überblickbar sind.

- Schon die Existenz eines koordinierten Personenidentifikators erhöht das Gefährdungspotenzial, da eine Verknüpfung von personenbezogenen Daten erleichtert wird. Dieses Gefährdungspotenzial wächst mit zunehmender Verbreitung des koordinierten Personenidentifikators.

- Der Grundsatz der Transparenz verlangt im Prinzip, dass die persönliche Identifikationsnummer gegenüber dem Träger der Nummer offengelegt wird. Mit der allgemeinen Kenntnis des Identifikators steigt aber auch die Wahrscheinlichkeit, dass sich Dritte (z.B. private Versicherungsunternehmen) über den Träger Zugang zu verschaffen versuchen (und dabei auch Erfolg haben).

- Das Einfügen eines koordinierten Personenidentifikators in eine Vielzahl von Personenregistern fördert (zumindest in der Tendenz) die – aus der Sicht des verfassungsrechtlichen Persönlichkeitsschutzes verpönte – Vermischung von Zwecksetzungen. Eine Lockerung des Zweckbindungsgrundsatzes ist nicht von vornherein ausgeschlossen, aber nur unter qualifizierten Voraussetzungen (Art. 36 BV) zulässig.

- Wenn die Einsatzzwecke bekannt und definiert sind, lässt sich eine Beurteilung unter dem Aspekt des öffentlichen Interesses und der Verhältnismässigkeit durchführen. Bei «offener» Zwecksetzung bzw. pauschaler Freigabe versagen die hergebrachten verfassungsrechtlichen Prüfkriterien.

- Der latenten Erhöhung des Gefährdungspotenzials ist mit der hergebrachten abwehrrechtlichen Dimension des Grundrechts auf Datenschutz – und mit den vorab auf klassische Grundrechtseingriffe zugeschnittenen Erfordernissen des überwiegenden öffentlichen Interesses und der Verhältnismässigkeit – nicht ohne Weiteres beizukommen, wie sich am Beispiel der Erhebung durch bzw. der Weitergabe an Private zeigt.

- Insgesamt besteht die Gefahr, dass ein koordinierter Personenidentifikator bei einer grosszügigen Freigabe nach und nach für nicht im vornherein bestimmte Zwecke zum Einsatz kommt. Was in einer Anfangsphase – wegen der vorerst möglicherweise geringen Verbreitung – noch als (relativ) unproblematisch erscheint, kann mit fortschreitender Zeit – und fortschreitender Verbreitung – problematisch werden.

In Anbetracht dieser neuralgischen Punkte erscheint es geboten, der Gefahr eines «Ausuferns» durch geeignete Massnahmen entgegenzuwirken.

Dass es sich dabei nicht um ein blosses rechtspolitisches Postulat handelt, sondern um ein verfassungsrechtlich abgestütztes Gebot, zeigen die folgenden Ausführungen (vgl. Ziffer IV.), in welchen die Tragweite des verfassungsrechtlichen Persönlichkeitsschutzes unter dem Blickwinkel der konstitutiv-institutionellen Grundrechtskomponente (Grundrecht als objektive Grundsatznorm) erörtert wird.

IV. Folgerungen aus der konstitutiv-institutionellen Tragweite des verfassungsrechtlichen Persönlichkeitsschutzes

1. Verfassungsrechtliche Pflicht, die Grundrechte in der gesamten Rechtsordnung zur Geltung zu bringen (Art. 35 BV)

Nach dem schon seit einiger Zeit vorherrschenden schweizerischen Grundrechtsverständnis erschöpft sich die Funktion der Grundrechte nicht darin, dem staatlichen Handeln Schranken zu ziehen und die Bürgerinnen und Bürger gegen staatliche Eingriffe zu schützen (Abwehrfunktion). Die Grundrechte haben darüber hinaus auch die Bedeutung von *fundamentalen Ordnungsprinzipien*, welche als objektive Grundsatznormen die gesamte Rechtsordnung durchdringen und eine programmatische Schicht aufweisen, die auf Verwirklichung durch schützende («positive») staatliche Massnahmen drängt[73]. Im Rahmen der Totalrevision der Bundesverfassung fand dieses Grundverständnis Eingang in den Verfassungstext. Art. 35 Abs. 1 BV bestimmt:

[73] Vgl. z.B. Jörg Paul Müller, Allgemeine Bemerkungen zu den Grundrechten, in: Daniel Thürer u.a. (Hrsg.), Verfassungsrecht der Schweiz, Zürich 2001, Rz. 29 ff.; Ulrich Häfelin/Walter Haller(Anm. 49), N. 256 ff.; für Art. 13 BV Stephan Breitenmoser (Anm. 26), Art. 13, Rz. 6.

Art. 35 Verwirklichung der Grundrechte

[1] Die Grundrechte müssen in der ganzen Rechtsordnung zur Geltung kommen. (...)

Wie aus Art. 35 Abs. 2 BV hervorgeht, sind alle Träger staatlicher Aufgaben zur Verwirklichung dieses Grundsatzes aufgerufen:

[2] Wer staatliche Aufgaben wahrnimmt, ist an die Grundrechte gebunden und verpflichtet, zu ihrer Verwirklichung beizutragen.

Den Behörden (Gesetzgeber, Verwaltung, Gerichte) obliegt es überdies dafür zu sorgen, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden (Art. 35 Abs. 3 BV):

[3] Die Behörden sorgen dafür, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden.

Die Bundesverfassung erteilt hier den staatlichen Organen einen allgemein formulierten Auftrag, sich aktiv und unter Einsatz «alle(r) geeigneten Mittel[74]» für die Verwirklichung der Grundrechte einzusetzen. Neben die traditionelle Verpflichtung, übermässige Grundrechtseingriffe zu unterlassen, tritt eine Verpflichtung, die Verwirklichung der Grundrechte zu fördern.

Die Bundesverfassung äussert sich nicht ausdrücklich zur Frage, welche Mittel dabei zum Einsatz kommen sollen. Sie gibt den Adressaten des Art. 35 BV in erster Linie ein Ziel vor; die Wahl der Mittel bleibt im Wesentlichen den Verpflichteten überlassen.

In der Verfassungsrechtslehre ist heute allgemein anerkannt, dass die Grundrechte auch jenseits ihrer Funktion als Abwehrpositionen *Schutzwirkungen* entfalten und dem Gesetzgeber und den weiteren Staatsorganen unter Umständen eigentliche Handlungsverpflichtungen auferlegen können (z.B. Gesetzgebungsaufträge).

In der schweizerischen Rechtslehre spricht man in diesem Zusammenhang neuerdings öfters von «staatlichen Schutzpflichten[75]», von «positiven Schutzpflichten[76]» des Staates, von «objektiven Schutz- und Leistungspflichten[77]» oder von «grundrechtlichen Schutzpflichten[78]» . Das Bundesgericht hat diesen Ansatz in einer kürzlich ergangenen Entscheidung aufgegriffen:

[74] So die Botschaft des Bundesrates über eine neue Bundesverfassung vom 20. November 1996, BBl 1997 I 192.
[75] So z.B. Jörg Paul Müller (Anm. 20), S. 28.
[76] So z.B. Alexander Ruch, Informationsgesellschaft als Risikogesellschaft: Rechtliche, soziale und politische Konzepte, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Perspektive Datenschutz, Zürich/Baden-Baden/Wien 2002, S. 105.
[77] So z.B. Stephan Breitenmoser (Anm. 26), Art. 13, Rz. 6.
[78] So z.B. Markus Schefer, Die Kerngehalte von Grundrechten, Bern 2001, S. 235. – Vgl. auch Jörg Paul Müller (Anm. 74), Rz. 36 ff.; verfassungsvergleichend Michael Holoubek, Grundrechtliche Gewährleistungspflichten, Wien/New York 1997, S. 15 ff.; Markus Schefer (Anm. 78), S. 238 ff.

«Nach neuerer Auffassung haben Grundrechte nicht nur eine abwehrende Funktion gegen Beeinträchtigungen durch den Staat, sondern begründen auch eine staatliche Schutzpflicht gegen Gefährdungen, die von Dritten verursacht werden[79].»

Der Begriff Schutzpflichten wird heute in der Schweiz im Allgemeinen eher unspezifisch als eine Art «Sammelbegriff» verwendet[80], den man bei näherer Analyse noch weiter unterteilen kann[81]:

- Grundrechtsgewährleistung in Form von grundrechtlichen Schutzpflichten,
- Grundrechtsgewährleistung in Form von Vorkehren im Bereich von Organisation und Verfahren,
- Grundrechtsgewährleistung im Zusammenhang mit institutionellen Garantien,
- Grundrechtsgewährleistung durch Einräumung von Teilhaberechten bzw. Leistungsansprüchen.

In der Schweiz sind derartige (aus dogmatischer Sicht sehr nützliche) Unterscheidungen bisher noch nicht heimisch geworden. Auf den Grad der dogmatischen Ausdifferenzierung und die noch ungefestigte Terminologie kommt es indessen nicht an. Für die Zwecke der vorliegenden Untersuchung ist entscheidend, dass man in der Schweiz mittlerweile die Existenz von aus den Grundrechten fliessenden staatlichen Schutzpflichten im Grundsatz anerkennt. Wichtig ist weiter, dass solche grundrechtlichen Schutzpflichten nicht erst durch Verletzungen aktualisiert werden, sondern schon durch *Gefährdungen* des geschützten Rechtsgutes[82].

2. Aus dem verfassungsrechtlichen Persönlichkeitsschutz fliessende grundrechtliche Schutzpflichten

Zu prüfen bleibt, ob und inwieweit solche grundrechtlichen Schutzpflichten auch im hier interessierenden Bereich des verfassungsrechtlichen Persönlichkeitsschutzes bestehen. Zu Recht wird in der Rechtslehre betont, dass die objektiven, konstitutiv-institutionellen Schutzwirkungen nicht bei allen Grundrechten schematisch gleich bestehe, dass deren Tragweite vielmehr für jedes Grundrecht einzeln zu untersuchen sei[83].

[79] BGE 126 II 300 (314).
[80] Markus Schefer (Anm. 78), S. 236.
[81] Zu diesen Erscheinungsformen auf rechtsvergleichender Grundlage eingehend Michael Holoubek (Anm. 78), S. 75 ff. 82 In diesem Sinn BGE 126 II 300 (314); Markus Schefer (Anm. 78), S. 255.
[83] In diesem Sinn BGE 126 II 300 (314); Markus Schefer (Anm. 78) S. 255.

Heute ist allgemein anerkannt, dass aus dem grundrechtlichen Anspruch auf Schutz der Privatsphäre, wie er heute in Art. 13 Abs. 1 BV bzw. in der Parallelbestimmung der EMRK verankert ist (Art. 8 EMRK), gewisse Schutzpflichten resultieren[84]. Schutzpflichten ergeben sich ferner auch aus dem – früher ungeschriebenen, heute in Art. 10 Abs. 2 BV verankerten – Grundrecht der persönlichen Freiheit[85].

Inwieweit dies auch für das in Art. 13 Abs. 2 BV verankerte Grundrecht auf Datenschutz gilt, wurde bisher noch kaum erörtert. Angesichts des Wortlauts des Art. 13 Abs. 2 BV – wo von einem «Anspruch auf Schutz vor Missbrauch» die Rede ist – spricht vieles dafür, dass auch aus diesem Grundrecht Schutzpflichten fliessen, die zu erfüllen dem Gesetzgeber, allenfalls weiteren Staatsorganen obliegt. Diese Annahme liegt um so näher, als etliche der Grundsätze, die heute bei der Umschreibung des Schutzgehalts von Art. 13 Abs. 2 BV genannt werden (vgl. Ziffer II.2.), nicht sinnvoll verwirklicht werden können, ohne dass der Staat auch gewisse positive Massnahmen zu ihrem Schutz trifft[86]. Erwähnt seien hier etwa der Grundsatz der Wahrung der Datensicherheit und der Grundsatz der Datenrichtigkeit, welche nur durch technische und gesetzliche Vorkehren wirksam umgesetzt werden können. Dazu zählen aber auch der Grundsatz der Transparenz und der Grundsatz der Zweckbindung, die sich nicht ohne gesetzliche Leitplanken verwirklichen lassen (Offenlegungspflichten, Weitergabeverbote u.ä.). Datenschutz erfordert ein Tätigwerden des Gesetzgebers[87]. Sicherheitsregeln müssen statuiert, Zweck und Umfang der Datenbearbeitung müssen festgelegt, Zugriffsberechtigungen und Verantwortlichkeiten geregelt werden[88]. Man kann durchaus sagen, dass die aktuelle Datenschutzgesetzgebung in weiten Teilen ein Mittel ist, um grundrechtliche Schutzpflichten, die aus dem verfassungsrechtlichen Persönlichkeitsschutz fliessen, zu erfüllen. In diesem Sinn bestimmt der Zweckartikel des Datenschutzgesetzes des Bundes:

[84] In diesem Sinn z.B. Jörg Paul Müller, Zur sog. subjektiv- und objektivrechtlichen Bedeutung der Grundrechte, in: Der Staat 1990, S. 39. Vgl. auch Markus Schefer (Anm. 78), S. 246.

[84] Vgl. BGE 126 II 300 (314); Stephan Breitenmoser (Anm. 26), Art. 13, Rz. 7; Rainer J. Schweizer (Anm. 28), Rz. 32; Robert Uerpmann (Anm. 36), S. 55. – Vgl. auch die Empfehlung R (86) 1 des Ministerkomitees des Europarates zum Schutz personenbezogener Daten, die für Zwecke der sozialen Sicherheit verwendet werden: Gemäss Ziffer 5.1 soll die Verwendung einer einheitlichen, einzigen Sozialversicherungsnummer durch im innerstaatlichen Recht vorgesehene Schutzmassnahmen begleitet werden.

[85] Vgl. z.B. Ulrich Häfelin/Walter Haller (Anm. 49), N. 361 f.; BGE 126 II 300 (314).

[86] Zur Schutzpflichtendimension des Rechts auf informationelle Selbstbestimmung aus der Sicht des deutschen Rechts vgl. BVerfGE 65, 1 (45 ff.).

[87] Zur Notwendigkeit gesetzlicher Regelungen vgl. z.B. Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 49.

[88] Vgl. Rainer J. Schweizer (Anm. 9), Art. 13, Rz. 49.

Art. 1 Zweck

Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.

Insoweit kann gerade im Bereich des Datenschutzes mit gutem Grund von grundrechtlichen Schutzpflichten die Rede sein, wobei in erster Linie der Gesetzgeber in der Pflicht steht.

Im hier interessierenden Zusammenhang kommt ein Weiteres hinzu: Es ist der Staat selbst, der durch die Einführung eines koordinierten Personenidentifikators die vorne geschilderten Gefahren bzw. Gefährdungspotenziale schaffen würde. Der Staat steht daher hier in einer gesteigerten Verantwortung. Es trifft ihn die Pflicht, die nötigen gesetzlichen Leitplanken zu setzen und sonstigen Schutzvorkehren zu ergreifen, um die von ihm geschaffene Gefahr soweit möglich zu bannen.

Im Zusammenhang mit der geplanten Einführung eines koordinierten Personenidentifikators besteht somit gewissermassen ein doppelter Grund, das Bestehen grundrechtlicher Schutzpflichten zu bejahen:

- einerseits wegen Art. 13 Abs. 2 BV in Verbindung mit Art. 35 BV,
- andererseits wegen des vom Staat geschaffenen, mithin von ihm zu verantwortenden und einzudämmenden Gefahrenpotenzials.

Zusammenfassend kann man festhalten, dass im hier interessierenden Bereich grundrechtlich fundierte staatliche Schutzpflichten bestehen – und zwar nicht nur im Sinn einer Pflicht zum Schutz gegen «Missbrauch» (im engeren Sinn), wie der Wortlaut des Art. 13 Abs. 2 BV bei oberflächlicher Lektüre denken lassen könnte, sondern grundsätzlich auch im Sinn einer Pflicht zum Schutz gegen sonstige Gefährdungen und Beeinträchtigungen des verfassungsrechtlichen Persönlichkeitsrechts.

Welche Folgerungen ergeben sich aus der Bejahung einer aus dem verfassungsrechtlichen Persönlichkeitsschutz fliessenden grundrechtlichen Schutzpflicht?

3. Mögliche Instrumente zur Erfüllung grundrechtlicher Schutzpflichten

a. Möglichkeiten und inhärente Grenzen der verfassungsrechtlichen Analyse

Die neue Bundesverfassung lässt – sowohl in Art. 13 Abs. 2 BV als auch in Art. 35 BV – offen, in welcher Weise der Staat durch positive Massnahmen zum Schutz des verfassungsrechtlichen Persönlichkeitsrechts beizutragen hat.

Dies hat mit der rechtlichen Struktur der hier interessierenden Grundrechtsdimension zu tun: Vereinfachend kann man sagen, dass grundrechtliche Schutzpflichten (bzw. die Grundrechte als objektive Grundsatznormen) in erster Linie ein *Ziel vorgeben*, es aber im Wesentlichen den zuständigen Organen überlassen, die Instrumente zu bestimmen. Es obliegt vorab dem Gesetzgeber festzulegen, welche Instrumente – unter den geeigneten, wirksamen Instrumenten – zum Einsatz kommen sollen. Dabei ist ihm ein erheblicher Prognose-, Beurteilungs- und Gestaltungsspielraum zuzugestehen.

Bei dieser Ausgangslage ist es nur begrenzt möglich, konkrete Aussagen aus verfassungsrechtlich fundierten staatlichen Schutzpflichten (hier: aus dem verfassungsrechtlichen Persönlichkeitsschutz) abzuleiten:

- Es ist möglich, Aussagen über das «Ob» zu machen, nämlich ob aus verfassungsrechtlicher Sicht Handlungsbedarf zu bejahen ist oder nicht (z.B. ob es geboten ist oder nicht, gesetzliche Massnahmen zu treffen, ob aus einer grundrechtlich begründeten Schutzpflicht ein Gesetzgebungsauftrag resultiert oder nicht).
- Es ist nicht möglich, abschliessende Aussagen über das «Wie» zu machen. (Andernfalls würde der Verfassungsinterpret den Gestaltungs-, Beurteilungs- und Prognosespielraum aushöhlen, den die Verfassung dem Gesetzgeber bzw. allfälligen anderen angesprochenen Organen belässt.)
- Immerhin ist es möglich, zu skizzieren, welche Arten von Instrumenten in Betracht kommen könnten.
- Und es ist in der Regel möglich, zu beurteilen, ob bestimmte ins Auge gefasste Instrumente oder Regelungen zur Verwirklichung des durch die Verfassung gesetzten Schutzziels taugen oder nicht, den verfassungsrechtlichen Anforderungen genügen oder nicht.

b. Aussagen mit Blick auf die Einführung eines eidgenössischen Personenidentifikators

Im Hinblick auf die allfällige Einführung eines einheitlichen eidgenössischen Personenidentifikators lässt sich aus heutiger Sicht Folgendes festhalten:

Angesichts des anerkannten Gefährdungspotenzials ist Handlungsbedarf zu bejahen. Die Einführung eines koordinierten eidgenössischen Personenidentifikators darf, in Anbetracht der im verfassungsrechtlichen Persönlichkeitsrecht verankerten Schutzanliegen, nicht ohne flankierende Schutzmassnahmen erfolgen, die dafür sorgen, dass die geschilderten Gefahren soweit möglich gebannt werden. Ein Handlungsbedarf ist um so mehr zu bejahen, als es der Staat selbst ist, der durch Einführung eines Personenidentifikators die fraglichen Gefahren bzw. Gefährdungspotenziale schafft.

Da es sich um einen Personenidentifikator handelt, den der Bund einführen will, ist mit «Staat» hier in erster Linie der Bund angesprochen. Zwar stehen auch die Kantone und Gemeinden durchaus in der Pflicht, denn Art. 35 BV spricht alle staatlichen Ebenen an. Der Bund als Urheber steht jedoch in einer gesteigerten Verantwortung, der er sich nicht einfach durch «Weiterdelegation» an die Kantone oder Gemeinden und deren Organe (Gesetzgeber, andere Behörden) entziehen darf.

Als Instrumente fallen grundsätzlich in Betracht:

- juristische Instrumente (gesetzliche Gebote und Verbote, allenfalls durch Sanktionen verstärkt; Administrativmassnahmen wie Bewilligungen, Kontrollen usw.);
- organisatorische Vorkehren (Grundrechtsgewährleistung durch Organisation und Verfahren, vgl. vorne Ziffer IV.1.);
- technische Vorkehren (auf die im Rahmen dieser verfassungsrechtlichen Analyse nicht näher eingetreten wird).

Die vom Staat ergriffenen organisatorischen und technischen Vorkehren bedürfen einer rechtlichen Grundlage (vgl. Art. 5 BV) und weisen insofern ebenfalls eine rechtliche Komponente auf.

In der Projektskizze des Eidgenössischen Departements des Innern (EDI) wird die Notwendigkeit von *gesetzlichen Leitplanken*, wenn auch in recht allgemeiner Weise, anerkannt. Genannt werden folgende Regelungsthemen[89]:

- Festlegung der Bedingungen der Erhebung, Speicherung, Verbreitung und Benützung des einheitlichen eidgenössischen Personenidentifikators; solche Regelungen müssen «exakt und eingrenzend sein».
- Beschränkung des Kreises der Stellen, die Zugang zu einem solchen Personenidentifikator erhält, auf das Notwendige.
- Genaue rechtliche Umschreibung der Verwendung und Verbreitung des Personenidentifikators.

[89] Vgl. Eidgenössisches Departement des Innern (EDI), „Der eidgenössische Personenidentifikator – Projektskizze" (Bern, 31. Mai 2002), S. 11.

Aus der Sicht des verfassungsrechtlichen Persönlichkeitsschutzes und der daraus fliessenden staatlichen Schutzpflicht bzw. Grundrechtsverantwortung ist es nur folgerichtig, solche Leitplanken zu fordern. Entscheidend ist aber nicht das abstrakte Anerkennen der Notwendigkeit gesetzlicher Leitplanken, sondern das Umsetzen in ein wirksames Massnahmendispositiv. In dieser Hinsicht muss (angesichts der Erfahrungen im Zusammenhang mit der AHV-Nummer) vor allem darauf geachtet werden, dass adäquate Antworten auf die Gefahr der schleichenden Ausbreitung und des drohenden «Ausuferns» eines einmal eingeführten koordinierten Personenidentifikators gefunden werden.

Wie gezeigt, ist es aus der Sicht des verfassungsrechtlichen Persönlichkeitsschutzes unabdingbar, dass eine kontextbezogene Abwägung, in Kenntnis der jeweiligen konkreten öffentlichen Interessen und Rahmenbedingungen, vorgenommen wird, und zwar durch eine zur grundrechtlichen Abwägung demokratisch hinreichend legitimierte Stelle.

Verfassungsrechtlich höchst problematisch wäre es aus dieser Sicht namentlich,

- wenn ein Gesetz des Bundes die Verwendung des koordinierten Personenidentifikators *in pauschaler Weise* (für nicht näher bezeichnete Stellen) *zwingend vorschreibt*[90], ohne sich weiter darum zu kümmern, für welche weiteren Administrativzwecke der Personenidentifikator dadurch verfügbar wird;
- wenn ein Gesetz (des Bundes) die Verwendung des koordinierten Personenidentifikators *pauschal ermöglicht*, z.B. ohne weitere Voraussetzungen kantonalen oder kommunalen Verwaltungsstellen zur Verfügung stellt[91].

Derartige Regelungen würden das Gebot der Interessenabwägung unterlaufen. Angesichts des skizzierten Gefährdungspotenzials darf der Bund «seinen» eidgenössischen Personenidentifikator nicht ohne Weiteres für kantonale oder private Stellen verfügbar machen. Eine solche «Überlassung» ist vielmehr nur dann zulässig, wenn der Persönlichkeitsschutz hinreichend und wirksam gewährleistet ist.

[90] In diese Richtung scheint der Vorentwurf für ein Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister zu gehen. Vgl. Art. 13 Abs. 1 VE.
[91] Der Vorentwurf für ein Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister sieht eine Pauschalermächtigung zu Gunsten der Kantone und Gemeinden vor (vgl. Art. 14 VE). Diese Ermächtigung wird immerhin insoweit relativiert, als der Einsatz nur in Frage kommt, „sofern dies die massgebenden Bundesgesetze" vorsehen; darüber hinaus wird auch eine gesetzliche Grundlage im kantonalen Recht gefordert.

Zusammenfassend kann man sagen: Zufolge der aus dem verfassungsrechtlichen Persönlichkeitsschutz fliessenden grundrechtlichen Schutzpflichten (Art. 13 Abs. 2 BV in Verbindung mit Art. 35 BV) muss der Bund dafür sorgen, dass es nicht zu einer unkontrollierten Ausbreitung des eidgenössischen Personenidentifikators kommt.

Wie lässt sich eine kontrollierte Ausbreitung gewährleisten?

Eine erste Möglichkeit besteht darin, dass der Gesetzgeber selbst, auf der Stufe des formellen Gesetzes, abschliessend darüber bestimmt, welche Stelle für welche Zwecke den eidgenössischen Personenidentifikator nutzen darf. Eine solche Lösung hätte den Nachteil einer gewissen Schwerfälligkeit.

Eine mögliche Alternative könnte darin bestehen, dass man die Kontrolle über die Ausbreitung durch eine Art «Zulassungssystem» zu gewährleisten versucht: Nur Stellen, die bestimmte gesetzlich festgelegte Anforderungen erfüllen, werden – nach entsprechender Prüfung – ermächtigt, den eidgenössischen Personenidentifikator einzusetzen. Dies wäre ein Anwendungsfall für eine Grundrechtsgewährleistung durch verfahrensmässige und organisatorische Vorkehren (vgl. Ziffer IV.1.).

Die Idee eines «Zulassungsverfahrens» ist dem geltenden Recht nicht fremd. Gemäss Art. 36 Abs. 4 Bst. c. DSG kann der Bundesrat näher bestimmen, «wie die Mittel zur Identifikation von Personen verwendet werden dürfen». In Ausführung dieser Ermächtigung hat der Bundesrat in Art. 25 VDSG die folgende, bereits vorne beschriebene Regelung getroffen (vgl. Ziffer I.3.):

- Die Verwendung eines (anwendungsspezifischen) Personenidentifikators durch andere Organe des Bundes oder der Kantone sowie durch private Personen muss vom betroffenen Bundesorgan genehmigt werden (Art. 25 Abs. 2 VDSG).
- Die Genehmigung kann (d.h. darf, aber muss nicht ohne Weiteres) erteilt werden, wenn ein enger Zusammenhang zwischen der vorgesehenen Verwendung und der Verwendung, für welche die persönliche Identifikationsnummer geschaffen wurde, besteht.

Das für anwendungsspezifische Personenidentifikatoren geschaffene Genehmigungssystem, das lediglich auf Verordnungsstufe geregelt ist, vermag im Fall der Einführung eines einheitlichen eidgenössischen Personenidentifikators unter verschiedenen Gesichtswinkeln nicht zu genügen. Die Grundidee könnte aber als Modell dienen.

Falls man zur Gewährleistung des Grundrechts auf Datenschutz die Schaffung eines derartigen «Zulassungssystems» in Betracht zieht, stellt sich die Folgefrage, wer nach welchen Kriterien entscheiden soll. Aus der Verfassung lässt sich naturgemäss keine abschliessende Antwort ableiten. Mit Blick auf das zur Entscheidung berufene Organ kann man immerhin festhalten, dass es sich nicht um eine involvierte Stelle handeln

sollte, die selbst an einer möglichst weiten Verbreitung des koordinierten Personenidentifikators interessiert ist. Zu denken ist vielmehr an eine möglichst unabhängige Stelle mit hinreichender Distanz zum Geschehen.

V. Ergebnis

Die wichtigsten Erkenntnisse der vorliegenden Untersuchung können wie folgt zusammengefasst werden:

Der namentlich in Art. 13 BV verankerte verfassungsrechtliche Persönlichkeitsschutz erfasst grundsätzlich jede staatliche Bearbeitung von Personendaten, somit auch die Schaffung eines eidgenössischen Personenidentifikators. Die Verfassung bietet, entgegen dem zu engen Wortlaut des Art. 13 Abs. 2 BV, nicht nur Schutz gegen eigentlichen Missbrauch personenbezogener Daten, sondern grundsätzlich auch Schutz vor sonstigen Benachteiligungen, die eine Person bei der Bearbeitung von Personendaten erleiden kann.

Aus dem im Grundrecht auf Datenschutz verankerten Grundsatz der Zweckbindung kann man ableiten, dass die Schaffung eines Personenidentifikators einem bestimmten, definierten Zweck zu dienen hat. Die (gleichzeitige oder spätere) Nutzung für allfällige weitere Zwecke bedeutet eine Abweichung vom Grundsatz der Zweckbindung.

Eine Lockerung des Grundsatzes der Zweckbindung bewirkt eine Einschränkung des verfassungsrechtlich geschützten Grundrechts auf Datenschutz. Eine solche Einschränkung erscheint aus verfassungsrechtlicher Sicht nicht von vornherein ausgeschlossen. Sie ist jedoch nur zulässig, wenn sie auf einer hinreichenden gesetzlichen Grundlage beruht, sich durch ein überwiegendes öffentliches Interesse rechtfertigen lässt und verhältnismässig (d.h. geeignet, erforderlich und zumutbar) ist.

Bei der Beurteilung der Verhältnismässigkeit ist ein Vorgehen geboten, das nach einzelnen Zielsetzungen und Einsatzbereichen differenziert. Es ist mithin getrennt – d.h. jeweils mit Blick auf eine näher bestimmte Zielsetzung – zu prüfen und auszuweisen, dass das besagte Ziel (die Legitimität des Ziels einmal unterstellt):

- mit dem Einsatz eines Personenidentifikators erreicht werden kann (Eignungsnachweis);
- nicht mit anderen, unter dem Blickwinkel der Eignung grundsätzlich gleichwertigen, jedoch unter dem Blickwinkel des verfassungsrechtlichen Persönlichkeitsschutzes weniger einschneidenden Mitteln erreicht werden kann (Erforderlichkeitsnachweis);
- in einer vernünftigen Relation zum eingesetzten Mittel steht (Zumutbarkeitsnachweis).

Der verfassungsrechtliche Persönlichkeitsschutz erschöpft sich nicht in der klassischen abwehrrechtlichen Grundrechtsdimension. Der Staat und seine Organe sind darüber hinaus generell dazu verpflichtet, die Grundrechte – und somit prinzipiell auch das Grundrecht auf Datenschutz oder informationelle Selbstbestimmung – in der ganzen Rechtsordnung zur Geltung zu bringen (Art. 35 Abs. 1 BV).

Heute ist allgemein anerkannt, dass aus Art. 13 Abs. 1 BV und Art. 10 Abs. 2 BV solche grundrechtlichen Schutzpflichten fliessen. Inwieweit dies auch für das in Art. 13 Abs. 2 BV verankerte Grundrecht auf Datenschutz gilt, wurde bisher noch kaum erörtert. Es spricht vieles dafür, dass auch aus diesem Grundrecht Schutzpflichten fliessen.

Grundrechtliche Schutzpflichten geben in erster Linie ein Ziel vor, überlassen es aber im Wesentlichen den zuständigen Organen, vorab dem Gesetzgeber, die Instrumente zu bestimmen. Dem Gesetzgeber kommt dabei ein erheblicher Prognose-, Beurteilungs- und Gestaltungsspielraum zu.

In Anbetracht des Gefährdungspotenzials und der im verfassungsrechtlichen Persönlichkeitsrecht verankerten Schutzanliegen darf die Einführung eines koordinierten eidgenössischen Personenidentifikators nicht ohne flankierende Schutzmassnahmen erfolgen. Eine staatliche Schutzpflicht ist um so mehr zu bejahen, als es der Staat (Bund) selbst ist, der durch Einführung eines Personenidentifikators die fraglichen Gefahren bzw. Gefährdungspotenziale schafft. Der Bund als Urheber steht dabei in einer gesteigerten Verantwortung, der er sich nicht einfach durch «Weiterdelegation» an die Kantone oder Gemeinden und deren Organe (Gesetzgeber, andere Behörden) entziehen darf.

Wegen der aus dem verfassungsrechtlichen Persönlichkeitsschutz fliessenden grundrechtlichen Schutzpflichten (Art. 13 Abs. 2 BV in Verbindung mit Art. 35 BV) muss der Bund dafür sorgen, dass es nicht zu einer unkontrollierten Ausbreitung des eidgenössischen Personenidentifikators kommt. Eine allfällige Lockerung der Zweckbindung (soweit sie sich im konkreten Fall als verfassungsrechtlich zulässig erweist) löst, wegen der damit verbundenen Gefährdungen entsprechende grundrechtliche Schutzpflichten aus.

Eine erste Möglichkeit, die Kontrolle über die Ausbreitung sicherzustellen, besteht darin, dass der Gesetzgeber selbst (auf der Stufe des formellen Gesetzes) abschliessend darüber bestimmt, welche Stelle für welche Zwecke den eidgenössischen Personenidentifikator nutzen darf. Eine andere Möglichkeit besteht darin, die Kontrolle über die Ausbreitung des Personenidentifikators durch eine Art «Zulassungssystem» zu gewährleisten.

Prof. Dr. Giovanni Biaggini

13.8 Entscheid der EDSK in Sachen Mietrecht

Siehe Anhang 13.8 im französischem Teil.

13.9 Entscheid der EDSK in Sachen Drogentests in der Lehre

Nr. 12/01 Urteil vom 29. August 2003

mitwirkend: Prof. Dr. R.J. Schweizer (Präsident), Frau Dr. R. Sauter, Frau T. Mona; Fürsprecher M. Sterchi (Sekretär)

In Sachen

Eidgenössischer Datenschutzbeauftragter,

Feldeggweg 1, 3003 Bern

Weiterziehungskläger

gegen

F. Hofmann-La Roche AG,

Grenzacherstr. 124, 4070 Basel

vertreten durch

Dr. Benedikt A. Suter, Advokat, Postfach 430, 4010 Basel

Weiterziehungsbeklagte

betreffend Empfehlung des EDSB vom 22. Februar 2001 in Sachen Drogentests in der Lehre bei der F. Hoffmann-La Roche AG

hat sich ergeben:

A. 1999 wurde der Eidgenössische Datenschutzbeauftragte (EDSB) von verschiedenen Seiten auf Drogentests aufmerksam gemacht, die bei der Firma Hoffmann-La Roche AG (im folgenden «Roche») durchgeführt werden.

Mit Schreiben vom 22. Dezember 1999 gelangte der EDSB an Roche und verlangte von ihr die Beantwortung von Fragen im Zusammenhang mit der Rechtmässigkeit der Drogentests. Insbesondere wollte er sich über Zweck, Freiwilligkeit, Testbedingungen, gesetzliche Grundlage und die Folgen einer Verweigerung solcher Tests erkundigen.

Mit Schreiben vom 17. Januar 2000 (Beilage Nr. 2 zur Weiterziehung = WB 2) nahm Roche zu den durch den EDSB gestellten Fragen Stellung. Roche erläuterte ihr Kon-

zept der «drogenfreien Lehre» und wies insbesondere auf die Freiwilligkeit der Tests und die Einhaltung des Arztgeheimnisses durch die internen Betriebsärzte hin. Zusammenfassend präsentiert sich das Konzept wie folgt:

Ziel von Roche ist es, den ihr anvertrauten Lehrtöchtern und Lehrlingen eine solide und ganzheitliche Ausbildung zu vermitteln. Sicherheit und Gesundheitsschutz an allen Arbeitsplätzen sowie Schutz von Mensch, Umgebung und Umwelt werden als vorrangige Anliegen bezeichnet. Das Schwergewicht aller Aktivitäten und Massnahmen zur Gewährleistung von Sicherheit und Umweltschutz legt Roche auf die Prävention. Die Firma stellt fest, dass Unfälle meist durch menschliches Versagen bedingt sind, und dass Mitarbeiterinnen und Mitarbeiter mit Suchtproblemen ein erhöhtes Risiko darstellen, weil Drogen in ihrer Wirkung nicht voraussehbar sind. Somit sind ein frühzeitiges Erkennen einer Suchtentwicklung bei Mitarbeiterinnen und Mitarbeitern sowie die Einleitung entsprechender Hilfsmassnahmen sehr wichtig (vgl. Informationsschreiben an Interessentinnen und Interessenten einer Lehre bei Roche, Beilage Nr. 3a zur Stellungnahme vom 17.12.2001 = AB 3a). Roche bekennt sich deshalb aus Gründen des Gesundheitsschutzes und des Wohlergehens junger Menschen sowie im Hinblick auf die Arbeitssicherheit zu einer drogenfreien Lehrzeit. (vgl. Broschüre «Probleme in der Lehre - was nun?» = AB 1, sowie das Informationsschreiben AB 3a).

Mit dem 1997 eingeführten Konzept «Ohne Drogen in und durch die Lehre» bekennt sich Roche nach eigenen Worten «zur sozialen Verantwortung gegenüber Jugendlichen, Eltern und Gesellschaft». Teil dieses Konzeptes ist das Drogenscreening. Dieses soll die Früherfassung einer potentiellen Sucht- und Missbrauchs-Entwicklung ermöglichen. Es ermögliche einerseits die Sicherheitsaspekte bei der Arbeit abzuklären und andererseits, wo nötig, die in einem Frühstadium noch am erfolgversprechendsten Therapiemassnahmen einzuleiten.

Im Brief an die Interessentinnen und Interessenten einer Berufslehre wird über das Konzept der drogenfreien Lehre sowie das Drogenscreening informiert. Roche weist darauf hin, dass, wer sich um eine Lehrstelle bewerbe, Tests auf gängige weiche und harte Drogen zu verschiedenen Zeitpunkten akzeptiere. Ebenso wird auf die Konsequenzen positiver Tests - auf harte und weiche Drogen - hingewiesen.

Lehrstellen-Bewerberinnen und -Bewerber müssen einen Fragebogen bezüglich ihres Gesundheitszustandes ausfüllen (AB 4). Die Aufnahme in die Lehrstelle erfolgt unter Vorbehalt ärztlicher Untersuchung und Drogenscreening. Wer positiv auf weiche Drogen getestet wird, kann bei fachlicher Qualifikation die Lehre dennoch antreten. Wer positiv auf harte Drogen getestet wird, kann zu diesem Zeitpunkt nicht in die Lehre aufgenommen werden. Bei Lehrbeginn und anschliessend stichprobenweise (zweimal pro Jahr) während der Lehre werden weitere Drogentests durchgeführt.

B. Am 30. März 2000 empfahl der EDSB Roche, auf die Drogentests und die entsprechende Datenbearbeitung zu verzichten. Die Empfehlung wurde im wesentlichen mit der Unverhältnismässigkeit und der fehlenden Zweckmässigkeit der systematischen und präventiven Erhebung von Gesundheitsdaten durch den Arbeitgeber, der Unfreiwilligkeit der Drogentests und dem fehlenden überwiegenden Sicherheitsinteresse begründet.

Am 30. Mai 2000 fand eine Besprechung zwischen dem EDSB und Roche statt, wo Roche ihren Standpunkt nochmals erläuterte und den EDSB ersuchte, seine Empfehlung zurückzuziehen. Der EDSB schob in der Folge die Weiterziehung der Empfehlung an die EDSK bis zum Abschluss der Arbeiten einer eigens eingesetzten «groupe de réflexion» auf.

Mit Schreiben vom 31. Mai 2000 (WB 11), in dem die wesentlichen Punkte der Diskussion festgehalten wurden, gelangte Roche nochmals an den EDSB.

Die genannte Arbeitsgruppe (EDSB in Zusammenarbeit mit der Schweizerischen Fachstelle für Alkohol- und andere Drogenprobleme, dem Staatssekretariat für Wirtschaft, dem Bundesamt für Gesundheit und dem Bundesamt für Justiz) publizierte am 16. Februar 2001 einen «Bericht über Drogentests in der Lehre» (WB 16). Der Bericht kommt u.a. zu folgenden Schlüssen:

- Generelle Drogentests bei allen Auszubildenden eines Betriebes sind nicht zulässig.
- Der Schutz der Privatsphäre überwiegt in den allermeisten Fällen einen möglichen Nutzen für den Betrieb oder die Betroffenen.
- Drogentests sind deshalb nur unter ganz bestimmten Bedingungen - einem überwiegenden Sicherheitsinteresse und der Einwilligung der Betroffenen - zulässig.

Die Drogentests selber werden als nur beschränkt zuverlässig bezeichnet.

Roche wurde von der Arbeitsgruppe im Rahmen von Hearings angehört, macht aber geltend, dass ihre Argumente sowie die eingereichten Dokumente nur ungenügend gewürdigt worden seien. Sie bestreitet im übrigen die Relevanz des Berichtes.

Unter Berücksichtigung der Ergebnisses dieses Berichtes erliess der EDSB am 22. Februar 2001 eine neue, überarbeitete Empfehlung. Unter anderem führte er darin aus, dass die ärztliche Massnahme der Urinanalyse einen Eingriff in die Persönlichkeit der untersuchten Person darstelle und das Bestehen eines überwiegenden Rechtfertigungsgrundes voraussetze. Nur ein gegenüber dem Persönlichkeitsschutz überwiegendes Sicherheitsinteresse, verbunden mit der Einwilligung des Lehrlings, könne einen Drogentest rechtfertigen. Ein solches überwiegendes Sicherheitsinteresse könne

durch Roche nicht belegt werden. Roche wurde durch den EDSB nochmals aufgefordert,

1. die Drogentests unverzüglich einzustellen;
2. die in Zusammenhang mit den Drogentests erhobenen Gesundheitsdaten zu vernichten;
3. den Vollzug der Empfehlung innert 15 Tagen seit Erhalt zu melden.
4.

C. Mit Schreiben vom 2. April 2001 (WB 18) lehnte Roche diese Empfehlung des EDSB in grundsätzlichen Hinsicht wiederum ab und zeigte sich nicht bereit, die präventiven Drogentests im Rahmen des gesamtheitlichen Drogenschutzkonzeptes für Lehrlinge einzustellen. Die Sicherheitsrelevanz, verbunden mit den Interessen der Eltern und der Lehrlinge, stelle einen Rechtfertigungsgrund für die Durchführung der fraglichen Drogentests dar. Hingegen war Roche bereit, der Empfehlung des EDSB insoweit Rechnung zu tragen, als künftig vor jedem Drogentest jeweils eine neue schriftliche Einwilligung des Lehrlings eingeholt wird.

D. Am 14. August 2001 nahm der Datenschutzbeauftragte zwecks Abklärung des Bestehens eines überwiegenden Sicherheitsinteresses bei einigen Lehrkategorien einen Augenschein bei Roche vor. Roche hielt im Anschluss an diesen Besuch in einem Schreiben vom 20. August 2001 (WB 24) fest, dass ihre Ausführungen vom 2. April 2001 nach wie vor gelten und bat den EDSB, ihr mitzuteilen, ob er nach Prüfung der Sicherheitsaspekte an der Empfehlung vom 22. Februar 2001 festhalte.

E. In der Folge gelangte der EDSB mit Datum vom 18. September 2001, in Weiterziehung seiner Empfehlung vom 22. Februar 2001, mit dem Begehren an die Eidgenössische Datenschutzkommission (EDSK), es sei Roche aufzufordern, die Drogentests bei Lehrlingen und die damit zusammenhängenden Datenbearbeitungen einzustellen. Auf die Begründung wird weiter unten im Rahmen der Erwägungen einzugehen sein.

F. In der Stellungnahme zur Weiterziehungsschrift vom 17. Dezember 2001 beantragte Roche, es sei festzustellen, dass die F. Hoffmann-La Roche AG mit ihrem Konzept der «drogenfreien Lehre» und der Durchführung der damit verbundenen Drogenscreenings bei Lehrlingen nicht gegen die Bestimmungen des Datenschutzgesetzes verstösst, und es sei das Urteil in anonymisierter Form mitzuteilen unter Kostenfolge zu Lasten EDSB.

G. Zur Klärung strittiger Sach- und Rechtsfragen wurde von der EDSK am 20. März 2003 eine mündliche Verhandlung durchgeführt. Die dabei zu klärenden Fragenkomplexe wurden den Parteien vorgängig schriftlich zugestellt. Der EDSB reichte daraufhin mit Schreiben vom 3. Februar 2003 eine von ihm angeforderte Stellungnahme des Schweizerischen Gewerkschaftsbundes (SGB) vom 23. Januar 2003 ein, die Auskunft über die Haltung des SGB zu Drogentests im Ausbildungs- und Arbeitsverhältnis gibt. Diese Stellungnahme wurde in Wert und Unwert zu den Akten erkannt. Im Hinblick auf die Verhandlung wurde ferner beim Kaufmännischen Verband Schweiz (KV) die Broschüre «Lehre & Drogen» angefordert und den Parteien zugestellt.

Auf die anlässlich der mündlichen Verhandlungen von den Zeugen gemachten Ausführungen wird ebenfalls nachfolgend im Rahmen der Erwägungen, soweit erforderlich, eingegangen.

H. Sowohl Weiterziehungskläger als auch Weiterziehungsbeklagte hielten nach durch-geführtem Beweisverfahren an ihren Stellungnahmen fest.

I. Im Nachgang zur Verhandlung forderte die EDSK mit Verfügung vom 30. April 2003 eine Stellungnahme des EDSB in Bezug auf seine Position des bei der Emil Frey AG prakti-zierten Drogenkonzeptes ein. Mit Schreiben vom 13. Mai 2003 nahm der EDSB dazu Stel-lung und erläuterte die Unterschiede der bei beiden Firmen praktizierten Drogenkonzepte zusammenfassend wie folgt:

- Die Emil Frey AG führe weder präventive systematische Drogenscreenings noch Einzel-tests durch,
- Im Einzelfall sei ein Drogentest im Rahmen eines medizinischen Eignungstests möglich, wenn der vom Unternehmen unabhängige Behandlungsarzt dies aus arbeitsmedizini-schen Gründen für nötig erachte und der Lehrling seine Einwilligung gegeben habe. Der Entscheid, ob ein Test durchgeführt wird, liege beim Arzt und beim Lehrling und nicht bei der E. Frey AG.
- Der behandelnde Arzt melde lediglich die Eignung für die Arbeitsstelle

Die Weiterziehungsbeklagte weist mit Schreiben vom 10. Juni 2003, bezugnehmend auf die Stellungnahme des EDSB, auf die Ähnlichkeiten der Konzepte von Roche und Emil Frey AG hin. Darüber hinaus wird weiterhin das Vorliegen eines Systemfehlers bestritten. Im übrigen hält Roche an allen ihren bisherigen Stellungnahmen fest.

Die Eidgenössische Datenschutzkommission zieht in Erwägung:

1. Roche bestreitet zunächst das Vorliegen einer datenschutzrechtlichen Frage. Ebenso bestreitet sie das Vorliegen eines Systemfehlers und damit die Zuständigkeit des EDSB und seine Legitimation zur Weiterziehung. Vielmehr handle es sich um eine arbeits-vertragliche und berufsbildungsrechtliche Frage.

a) Anwendbarkeit des Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1):

aa) Das DSG gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen und Bundesorgane (Art. 2 Abs. 1 DSG). Als Personendaten gelten dabei alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG). Unter «Bearbeiten» ist jeder Umgang mit Personendaten zu verstehen, dabei insbesondere das Beschaffen, Aufbewahren, Archivieren oder Vernichten von Daten (Art. 3 lit. e DSG).

bb) Jugendliche, die sich bei Roche für eine Lehrstelle bewerben, haben u.a. einen Fragebogen auszufüllen, auf welchem sie verschiedene Fragen betreffend ihres Gesundheitszustandes zu beantworten, aber auch Auskunft zu Sucht-gewohnheiten zu geben haben. Der Betriebsarzt, zu dessen Handen der Frage-bogen ausgefüllt wird, nimmt daraufhin eine Beurteilung über die Geeignetheit eines Bewerbers oder einer Bewerberin zum Antritt der Lehrstelle vor.

cc) Die so erhobenen Angaben über die Stellenbewerberinnen und -bewerber sind unzweifelhaft Daten im Sinne des DSG. Die meisten dieser Daten fallen sogar unter die Kategorie der «besonders schützenswerten Personendaten», wie unten ausgeführt werden wird. Als solche werden u.a. Daten über die Gesundheit oder die Intimsphäre bezeichnet (vgl. Art. 3 lit. c Ziff. 2); sie geniessen einen privile-gierten Schutz. Die während der Lehrzeit im Rahmen der stichprobenweise durch-geführten Drogentests anfallenden Testergebnisse sind, da Angabe (nämlich «positiv» oder «negativ») über die getestete Person, ebenfalls als Daten bzw. als «besonders schützenswerte Daten» zu qualifizieren.

dd) Roche macht in Bezug auf den Fragebogen geltend, bei diesem handle es sich um ein Dokument, welches der schulärztliche Dienst des Kt. Basel-Stadt zur Verfügung stelle und auf dessen Gestaltung sie somit keinen Einfluss habe.

Es stellt sich somit die Frage, ob es sich bei diesem Fragebogen um ein Dokument handelt, welches ausserhalb des Geltungsbereichs des DSG liegt, weil es dem massgebenden Recht des Kt. Basel-Stadt untersteht, und deshalb der Beurteilung durch die EDSK entzogen ist.

Wie oben ausgeführt, ist dieser Fragebogen Bestandteil des Anstellungsverfah-rens bei Roche. Seine Verwendung erfolgt im vorliegenden Zusammenhang somit nicht in Erfüllung kantonaler öffentlichrechtlicher Aufgaben, sondern er bildet Grundlage für den Vertragsschluss und daher Bestandteil eines privatrechtlichen Verfahrens. Zudem wurde er von Roche erweitert und ergänzt; er kann also als eigenes, selbständiges Formular von Roche betrachtet werden und unterliegt damit auch den Bestimmungen des DSG.

Das DSG ist demnach sowohl auf die Frage der Erhebung der Testergebnisse als auch auf die Benutzung des Fragebogens zur Beurteilung der Bewerberinnen und Bewerber anzuwenden.

b) Zuständigkeit des EDSB/Legitimation zur Weiterziehung

aa) Im Zusammenhang mit Datenbearbeitungen im Privatrechtsbereich klärt der EDSB von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn (Art.29 Abs. 1 DSG):

- lit a) Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler);
- lit. b) Datensammlungen registriert werden müssen;
- lit. c) Bekanntgaben ins Ausland gemeldet werden müssen.

Im vorliegenden Fall kommt einzig lit. a) in Betracht (vgl. die Voraussetzungen für die Registrierung von Datensammlungen und die Meldung von Bekanntgaben ins Ausland in Art. 11 resp. 6 DSG).

bb) In der Lehre wird als zusammenfassende Bezeichnung für die Eignung der Verletzung einer grösseren Anzahl von Personen in ihrer Persönlichkeit der Begriff «Systemfehler» verwendet (vgl. R. Bründler, Kommentar zum schweizerischen Datenschutzgesetz, Basel/Frankfurt a.M. 1995, N. 3 zu Art. 29). In ihrer bisherigen Rechtsprechung (erstmals Nr. 1/95; EDSB gegen Schweiz. Verband der Immobilien-Treuhänder u.a.; Urteile vom 15. Dez.1995/ 21. Nov. 1996, VPB 62 (1998) Nr. 42 A/B S. 350 ff.) hat die EDSK die Empfehlungsbefugnis des EDSB weit interpre-tiert und also nicht nur auf die Fehler von Informationssystemen der EDV beschränkt beurteilt. Von einem Systemfehler im Sinne der genannten Bestim-mung ist auch dann zu sprechen, wenn das System der 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.

cc) Im vorliegenden Fall sind von der vom EDSB beanstandeten Bearbeitung jährlich rund 100 Auszubildende betroffen; insgesamt werden bei Roche gleichzeitig immer rund 300 Lehrlinge und Lehrtöchter ausgebildet. Von diesen Auszubildenden werden vor Lehrstellenantritt und während der Lehrzeit regelmässig besonders schützenswerte Daten erhoben. Diese Anzahl erfüllt durchaus das Tatbestandselement der «grösseren Anzahl» i.S. von Art. 29 Abs. 1 lit. a DSG.

dd) Die Kompetenz des EDSB, eine Empfehlung abzugeben, ist somit gegeben. Da Roche die Empfehlung des EDSB ablehnt, ist er berechtigt, diese der EDSK zum Entscheid vorzulegen (Art. 29 Abs. 4 DSG). Die genannte Bestimmung setzt dem EDSB keine Frist für die Weiterziehung. Diese ist auch an keine weiteren formellen Voraussetzungen gebunden.

Auf die Weiterziehung an die EDSK ist somit einzutreten.

2. a) Kognition der EDSK

Die EDSK entscheidet als erstinstanzliche Schiedskommission (Art. 33 Abs. 1 lit.a DSG). Das Verfahren richtet sich nach dem Bundesgesetz über das Verwaltungs-verfahren vom 20. Dezember 1968 (VwVG; SR 172.021). Ihre Kognition ist durch keine gesetzlichen Bestimmungen eingeschränkt und damit umfassend. Der Über-prüfung durch die EDSK unterliegt die vom EDSB abgegebene Empfehlung. Sie kann diese entweder bestätigen und damit für den Adressaten verbindlich werden lassen, abändern oder ganz oder teilweise aufheben bzw. als unverbindlich erklären.

b) Streitgegenstand

Der EDSB beanstandet sowohl den von Roche zur Befragung der Lehrstellen-bewerberinnen und -bewerber für die Erhebung von Gesundheitsdaten benutzten Fragebogen (Erw. 3) als auch die bei Roche durchgeführten Screenings (Erw. 2) und die damit verbundenen Datenerhebungen. Explizit zum Gegenstand der Empfehlung vom 22. Februar 2003 werden jedoch nur die Drogentests gemacht.

c) Passivlegitimation:

Weiter stellt sich die Frage, wer – die Weiterziehungsbeklagte oder der Betriebs-arzt – als Bearbeiter der durch Fragebogen und Screenings erhobenen Daten zu gelten hat und somit materiell Adressat der Empfehlung des EDSB ist.

aa) Gemäss Art. 328b des Schweizerischen Obligationenrechts vom 30. März 1911 (OR; SR 220) gelten die Bestimmungen des DSG auch für Arbeitsverhält-nisse (BGE 120 II 119). Roche betont indessen, dass einzig der Betriebsarzt die detaillierten Antworten der Fragebogen und die Testergebnisse kenne respektive bearbeite, und dass die bei seiner Tätigkeit anfallenden Informationen bereits durch das

Arztgeheimnis geschützt seien. Seine Tätigkeit erfolge zudem weisungsungebunden.

bb) Dadurch, dass die Untersuchungen und Tests auf Veranlassung von Roche und zum einen im Hinblick auf den Abschluss eines Lehrvertrags mit der betroffe-nen Person, zum andern zur Durchsetzung ihres Konzeptes der drogenfreien Lehre erfolgen, kann die Tätigkeit des Betriebsarztes nicht unabhängig von der Unternehmenspolitik von Roche beurteilt werden. Der Betriebsarzt, bei Roche in einem Anstellungsverhältnis beschäftigt, bearbeitet die Daten damit letztlich als Hilfsperson von Roche. Der EDSB hat deshalb zu Recht die Empfehlung an das verantwortliche Unternehmen Roche und nicht an den Betriebsarzt (der im Laufe der Zeit auch wechseln kann) gerichtet. In Bezug auf die vorliegende Weiterziehung ergibt sich daraus auch ihre Passivlegitimation.

3. Materielle Prüfung der Empfehlung vom 22. Februar 2001

Es ist zu prüfen, ob die durch Roche im Rahmen der Abklärung der Eignung zum Antritt einer Lehrstelle und während des Lehrverhältnisses durchgeführten Urintests und dabei erfolgenden Datenerhebungen die Persönlichkeit der Auszubildenden widerrechtlich verletzen.

a) Persönlichkeitsverletzung

aa) Geschützt ist die Persönlichkeit in umfassender Weise. Danach hat der Arbeitgeber im Arbeitsverhältnis die Persönlichkeit des Arbeitnehmers zu schützen und zu achten. Grundsätzlich ist jede Beeinträchtigung der Persönlichkeit als Verletzung derselben i.S. von Art. 28 ZGB anzusehen. Wegen der absoluten Natur des geschützten Rechtsgutes gilt sodann jede Verletzung als widerrechtlich (vgl. Pedrazzini / Oberholzer, Grundriss des Personenrechts, 4. Aufl. 1993, S. 129). Die Frage der Zulässigkeit der Bearbeitung von Personendaten entscheidet sich denn auch nach dem Kriterium der Widerrechtlichkeit (M. Hünig, DSG-Kommentar, N 11 zu Art. 12 DSG). Das DSG verlangt deshalb für jede Form der privaten Datenbearbei-tung, soll diese rechtmässig sein, ausdrücklich einen Rechtfertigungsgrund.

In Konkretisierung von Art. 28 ZGB enthalten zudem Art 328 ff. OR spezifische Bestimmungen zum Schutz der Persönlichkeit des Arbeitnehmers. Der Arbeitgeber hat namentlich alle Eingriffe in die Persönlichkeit des Arbeitnehmers zu unterlassen, die nicht durch den Arbeitsvertrag gerechtfertigt sind. Zu den Persönlichkeitsrechten gehören insb. Leben und Gesundheit, körperliche und geistige Integrität, persönliche und berufliche Ehre, Stellung und Ansehen im Betrieb, *Geheim- und Privatsphäre*, Freiheit der persönlichen Meinungsäusserung und Freiheit der gewerkschaftlichen Organisation (vgl. BSK OR I-Rehbinder/Portmann, 3. Aufl. 2003, N 4 zu Art. 328 OR)

Vom Arbeitgeber dürfen gemäss Art. 328b OR Daten über den Arbeitnehmer nur bearbeitet werden, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Im übrigen wird diesbezüg-lich ausdrücklich auf die Bestimmungen des DSG verwiesen.

bb) In Umsetzung ihres Konzeptes «drogenfrei durch die Lehre» erhebt Roche im Rahmen des Anstellungsverfahrens mittels eines Fragebogens Daten über den Gesundheitszustand. Vor Antritt der Lehre und später während der Lehrzeit werden Urintests durchgeführt, deren Ergebnisse ebenfalls Angaben und damit Daten über die getesteten Personen liefern. Durch das Ausfüllen des Fragebogens und das Absolvieren der Drogentests werden somit besonders schützenswerte Daten im Sinne von Art. 3 lit. c Ziff. 2 (vgl. hierzu U. Belser, DSG-Kommentar, N. 13 zu Art. 3 DSG) über die Bewerberinnen und Bewerber erhoben. Sie müssen Auskunft geben über Gesundheitszustand, persönliche Lebensgewohnheiten und Schwächen. Dies sind Angaben, die der Intimsphäre einer Person zuzurechnen sind. Die systematische Erhebung dieser Daten ergibt eben nicht nur ein Bild über den Gesundheitszustand des Auszubildenden und damit allenfalls über seine Arbeitsfähigkeit. Vielmehr werden damit auch Rückschlüsse über private Lebensgewohnheiten möglich.

b) Widerrechtlichkeit

Eine Verletzung der Persönlichkeit ist dann widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, ein überwiegendes privates oder öffentliches Interesse oder eine besondere gesetzliche Vorschrift gerechtfertigt ist (Art. 13 Abs. 1 DSG).

Roche führt verschiedene Gründe an, die den Eingriff in die Persönlichkeit der Auszubildenden ihrer Ansicht nach rechtfertigen.

aa) Sicherheitsaspekt:

Dass aus Gründen der Arbeitssicherheit ein Verbot des Konsums von Drogen erlassen wird, würde Sinn machen. Es leuchtet ein, dass in einem Betrieb wie jenem von Roche, wo mit chemischen Substanzen gearbeitet wird, an die Gewährleistung der Sicherheit höchste Ansprüche gestellt werden müssen. Unfälle, die auf mangelnde Sicherheit zurückzuführen sind, gefährden nicht nur Arbeitnehmerinnen und Arbeitnehmer, sondern auch die Umwelt oder die Bevölkerung in einem weiteren Umfeld. Aufgrund der vorliegenden Akten und der durchgeführten Anhörung der Sachverständigen und Zeugen von Roche ergibt sich indessen der Schluss, dass aus Sicht von Roche nicht die Sicherheit im Vordergrund stand, als es darum ging, die Scree-nings einzuführen. Ihr Grundlagen findet diese Massnahme vielmehr im ganzheitli-chen Ausbildungskonzept von Roche (welches eine drogenfreie Lehre umfasst), im Präven-

tionsgedanken und in der fürsorgerischen Pflicht des Arbeitgebers (siehe auch die Aussagen in der Roche-Broschüre «Probleme in der Lehre, was nun?»). Drogen-screenings werden dabei als Massnahme der sogenannt sekundären Prävention und Früherkennung von Suchtmittelproblemen genannt (vgl. Stellungnahme zur Weiter-ziehungsschrift, S. 2). Als Zeichen des Erfolgs dieses Ausbildungskonzeptes werden u.a. der Rückgang der Lehrabbrüche, das Wegfallen von Drogenproblemen in den Wohnheimen oder das Wegfallen von Beschwerden von Eltern angeführt.

Es ist durchaus einzuräumen, dass der Konsum von Drogen Auswirkungen auf die Arbeitsfähigkeit und damit die Arbeitssicherheit haben könnte. Drogenkonsumenten werden in der Broschüre der IGBCE (deutsche Gewerkschaft Bergbau Chemie Energie, S. 4; AB 5) als «Sicherheitsrisiko» bezeichnet. Diesem Papier ist zu entnehmen, dass «*betriebliche Regelungen gefunden werden müssen, Drogenkonsum bei allen Mitarbeitern auszuschliessen, die Tätigkeiten mit Eigen-, Fremd- und Umweltgefährdung ausüben*» (S. 2). Und weiter: «*Damit dürfen Vorgesetzte niemanden weiter beschäftigen, der für sich oder Dritte aufgrund von Drogenkonsum eine Gefährdung darstellt*» (S. 20). Es wird in diesem Zusammenhang ein Drogenscreening für alle Mitarbeitenden, die in diese Kategorien fallen, empfohlen.

Dass ein Bedürfnis und eine Notwendigkeit bestehen kann, «sicherheitsgefährdende» Arbeitnehmerinnen und -nehmer zu erkennen und (allenfalls) vorübergehend von ihrer Tätigkeit zu befreien, erscheint einleuchtend. Insoweit könnten allenfalls über-wiegende private Interessen, die sich aus den Schutz- und Fürsorgepflichten des Arbeitgebers gegenüber den übrigen Arbeitnehmern, aber auch überwiegende öffent-liche Interessen (Schutz vor möglicher Gefährdung Dritter oder der Umwelt) im Sinne von Art. 13 Abs. 1 DSG durchaus erkannt werden.

Vor diesem Hintergrund könnte ein Drogenscreening als Massnahme zur Erkennung von «Sicherheitsrisiken» grundsätzlich geeignet sein. Damit ist jedoch nicht gesagt, dass sie – jedenfalls in der praktizierten Form – auch verhältnismässig ist. Wenn nämlich Roche mit der Begründung der Gewährleistung der Arbeitssicherheit das Drogenscreening a) auf sämtliche Auszubildenden, also z.B. auch jene, die nicht einer erhöht sicherheitssensitiven (z.B. rein administrativen) Tätigkeit nachgehen, und andererseits b) ausschliesslich auf eine Gruppe von Arbeitnehmenden, eben die in der Lehre stehenden, und nicht auf sämtliche in sicherheitsrelevanten Bereichen tätigen Mitarbeiterinnen und Mitarbeiter anwendet, so ist dies zumindest inkonse-quent. Des weiteren wird der Konsum von Alkohol, der ebenfalls ein ernsthaftes Problem und Sicherheitsrisiko darstellen kann (s. «Alkohol, Drogen, Medikamente - was tun bei Problemen am Arbeitsplatz?», hrsg. vom werksärztlichen Dienst der Degussa-Hüls AG, AB 15 b) nicht getestet. Wird als Rechtfertigungsgrund für Screenings der Sicherheitsaspekt herangezogen, dann müssten solche also auch den Konsum von Alkohol umfas-

sen. Dies geschieht bei Roche nicht. Somit kann festge-stellt werden, dass durch die praktizierte und Gegenstand der Empfehlung bildende Datenbearbeitung einerseits das angestrebte Ziel (Gewährleistung der Sicherheit) nicht einwandfrei erreicht und andererseits über dieses Ziel hinaus geschossen wird. Dadurch verletzt die Datenbearbeitung den Grundsatz der Verhältnismässigkeit, und der Sicherheitsaspekt kann nicht als Rechtfertigungsgrund ins Feld geführt werden.

bb) Drogenfreie Lehre und damit zusammenhängende Begründung

Roche führt im weiteren als Begründung für die Durchführung der Drogenscreenings bei den Auszubildenden an, Ziel sei es, eine drogenfreie Lehrzeit zu erreichen. Roche verfolgt dieses Ziel im Bestreben, den ihr anvertrauten Auszubildenden eine solide und ganzheitliche Ausbildung zu vermitteln. Damit handle sie im Rahmen der Fürsorgepflicht des Arbeitgebers und berücksichtige zudem einen Wunsch vieler Eltern. In der Broschüre «Probleme in der Lehre - was nun», bezeichnet sich Roche denn auch als mitverantwortlich für das Wohlergehen der ihr anvertrauten Lehrtöchter und Lehrlinge. Deren Probleme und Sorgen sollen erkannt werden und beim Auftreten von Schwierigkeiten soll geholfen werden. Die Drogenscreenings werden dabei als ein «taugliches Mittel für eine präventive Früherkennung potentieller Suchtentwicklung» bezeichnet (siehe «Probleme in der Lehre - was nun, S. 13; AB1).

Das von Roche verfolgte Ziel, ihren Auszubildenden eine drogenfreie Lehrzeit zu ermöglichen, soll hier vorerst nicht beurteilt werden. So achtenswert dieses Ziel auch ist, so stellt sich indessen die Frage nach der Verhältnismässigkeit der Massnahmen zur Erreichung dieses Ziels. Diese laufen darauf hinaus, die Fürsorgepflicht des Arbeitgebers auch auf das Privatleben der Auszubildenden auszudehnen; denn es ist davon auszugehen, dass z.B. gerade Cannabis vor allem ausserhalb der Arbeitszei-ten konsumiert wird. Eine derartige Erweiterung des arbeitsrechtlichen Schutz-bereichs über die Belange des Arbeitsplatzes hinaus ist jedoch dem schweizerischen Recht fremd. Gemäss Art. 328 Abs. 2 OR hat der Arbeitgeber 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 angemes-sen sind, soweit es mit Rücksicht auf das einzelne Arbeitsverhältnis und die Natur der Arbeitsleistung ihm billigerweise zugemutet werden kann (die Erwähnung des Haus-haltes betrifft dabei einzig den Fall der Hausgemeinschaft). Die Lehre sieht in dieser Bestimmung vorwiegend eine *Begrenzung* der Schutzpflichten des Arbeitgebers und keineswegs eine Grundlage für deren Ausdehnung in die Privatsphäre der Ange-stellten (vgl. OR-Rehbinder/Portmann, a.a.O., N. 9 f.).

Zwar wird in diesem Zusammenhang von Roche die Zustimmung der Eltern der Auszubildenden angeführt. Dieser Wunsch kann aber nicht den Anspruch der jugendlichen, zum Teil auch volljährigen, Auszubildenden auf Schutz ihrer Persönlichkeit überwiegen (vgl. auch Art. 11 BV). Über die Geeignetheit der Tests als Massnahme zur Erreichung des Ziels der drogenfreie Lehre sind zudem Zweifel anzubringen. Im Rahmen von Fachkreisen wird die präventive und pädagogische Wirkung solcher Tests eher in Frage gestellt (siehe Aussagen Dr. Richard Müller und Mario Antonelli an der Verhandlung vom 20. März 2003). Ebenso wird die Aussagekraft eines Test-ergebnisses in Bezug auf die Arbeitsfähigkeit in Frage gestellt.

Systematische Screenings, mithin Tests, die sich nicht an einer auffälligen Verhaltensänderung des Lehrlings orientieren, welche allenfalls auf den Konsum illegaler Drogen zurückzuführen sein könnte, sind dazu weder als erforderlich, noch geeignet, noch als angemessen zu beurteilen, worauf unten noch näher einzugehen sein wird. Die von Roche praktizierte Datenbearbeitung ist in Bezug auf das Arbeitsverhältnis als unverhältnismässig und damit als widerrechtliche Verletzung der Persönlichkeit der Auszubildenden zu beurteilen.

cc) Einwilligung der Auszubildenden

Roche macht geltend, dass für die Durchführung der Tests die schriftliche Einwilligung der Auszubildenden und deren Eltern vorliege. Um den Anliegen des EDSB nachzukommen, werde ausserdem seit Lehrbeginn 2001 vor jedem durchzuführen-den Test eine schriftliche Einwilligung des Lehrlings oder der Lehrtocher eingeholt.

Damit eine Einwilligung zur Datenerhebung als Rechtfertigungsgrund gemäss Art. 13 Abs. 1 DSG in Betracht gezogen werden kann, muss gewährleistet sein, dass sie ihrerseits vor Art. 27 Abs. 2 ZGB standhält. Hierzu ist erforderlich, dass sie freiwillig und in Kenntnis ihrer rechtlichen Tragweite erfolgt (*consentement «libre et éclairé»*; s. H. Deschenaux/P. H. Steinauer, Personnes physiques et tutelle, 4. éd. 2001, N 588). Bei der Beurteilung ist auf die tatsächliche Situation im Einzelfall abzustellen (M. Hünig; DSG-Kommentar, N 4 zu Art. 13 DSG). Insbesondere ist zu untersuchen, wie weit diese Einwilligungen vorliegend freiwillig erfolgen.

Roche zeigt auf, dass sie alle Interessentinnen und Interessenten, die sich für eine Lehrstelle bei Roche bewerben, vorgängig ausführlich über das Konzept der drogenfreien Lehre informiert (vgl. dazu die entsprechenden Schreiben an die Interessentinnen und Interessenten einer Lehrstelle bei Roche). Bereits während der Schnupperlehre wird dieses Thema angesprochen. Im Rahmen der Beantwortung der Fragen auf dem Fragebogen wird ebenfalls nochmals auf die Drogentests hingewiesen; die Bestätigung, dass von diesem Konzept Kenntnis genommen wurde, wird mit der Unterschrift des Auszubildenden und - bei Minderjährigen - dessen Eltern oder Erzie-

hungsberechtigten gegeben. Auf diesem Fragebogen werden die Bewerberinnen und Bewerber auch darauf hingewiesen, dass positive Testresultate der Lehrlingsleitung mitgeteilt werden können. Eine Testverweigerung während der Lehre stellt nach Ansicht von Roche somit einen Verstoss gegen die vereinbarten Abmachungen dar (vgl. WB 2).

Niemand ist theoretisch gezwungen, sich um eine Lehrstelle bei Roche zu bewerben und diese anschliessend anzutreten. Roche weist zudem darauf hin, dass die Firma im Raume Basel keine Monopolstellung innehabe, es den Jugendlichen vielmehr freistehe, sich um eine Lehrstelle bei einem anderen chemischen Betrieb zu bewerben. Wer sich hingegen bei Roche bewerbe, wisse um das Konzept der drogenfreien Lehre und sei bereit, dieses - mit den entsprechenden Konsequenzen - mitzutragen. Diese Argumentation greift zu kurz. Gerade in einer Zeit, in der es für junge Leute schwierig ist, einen Ausbildungsplatz zu finden, sind sie wohl bereit, Konzessionen einzugehen, wenn es darum geht, eine geeignete oder allenfalls sogar die «Wunsch»- Lehrstelle zu finden. Wenn man allenfalls noch von Freiwilligkeit sprechen könnte, sich vor Antritt der Lehrstelle einem Screening zu unterziehen, dann gilt dies jedoch sicher nicht mehr in Bezug auf die Screenings, die während der Lehrzeit durchgeführt werden. Die Auszubildenden sind sich wohl bewusst, dass ein Ablehnen eines solchen Tests als Verstoss gegen die vertraglich getroffene Vereinbarung angesehen und wohl auch entsprechende Konsequenzen nach sich ziehen würde. Die jeweils abzugebende Einwilligung ist somit nicht als wirklich freiwillig zu betrachten und genügt deshalb nicht als Rechtfertigungsgrund für die Durchführung der Tests und die damit verbundenen Datenerhebungen sowie die daraus resultierende Verletzung der Persönlichkeit.

4. Fazit

Obschon die Absicht von Roche, den von ihr ausgebildeten Jugendlichen eine drogenfreie Lehrzeit zu ermöglichen, grundsätzlich positiv zu würdigen ist, kommt die EDSK zum Schluss, dass die durchgeführten systematischen Screenings und damit verbunde-nen Datenerhebungen als unverhältnismässig zu qualifizieren sind. Auch ist die Geeig-netheit der von Roche getroffenen Massnahmen zur Erreichung des genannten Ziels in Frage zu stellen, werden doch in Fachkreisen Zweifel an der Zuverlässigkeit der Tests angebracht.

Da zudem keine überwiegenden privaten oder öffentlichen Interessen oder gar gesetzli-che Bestimmungen als stichhaltige Rechtfertigungsgründe für die flächendeckenden Tests vorliegen und da auch die von den Auszubildenden abgegebene Einwilligung als ungenügend bezeichnet werden muss, stellt die durch Roche durchgeführte Datenerhe-bung eine widerrechtliche Persönlichkeitsverletzung im Sinne von Art. 12 DSG dar.

Nicht in Frage gestellt wird damit die Kompetenz von Roche, zu verlangen, dass sämtliche Arbeitnehmerinnen und Arbeitnehmer ihre Tätigkeit frei von Einfluss und Nachwir-kungen - irgendeiner Art - von Drogen und Suchtmitteln zu erledigen haben. Sollte ein begründeter Verdacht aufkommen, dass eine Arbeitnehmerin oder ein Arbeitnehmer ein Drogenproblem hat, etwa aufgrund des Nachlassens der Leistungsfähigkeit oder sonsti-gen auffälligen Verhaltens, kann ein Drogentest – im Rahmen eines umfassenden Konzeptes – deshalb notwendig werden. Differenzierte Konzepte, die ein Handeln auf Anlass hin vorsehen, sind deshalb als mit dem Datenschutzgesetz vereinbar zu erklären.

Desgleichen ist auch der Fragebogen, der zur erstmaligen Erhebung von Angaben über den Gesundheitszustand der sich Bewerbenden benutzt wird, als unverhältnismässig zu beurteilen. Eine Überarbeitung sämtlicher Fragen im Hinblick auf den Verhältnismässig-keitsgrundsatz erscheint angezeigt. Sie ist jedoch nicht Gegenstand der vom EDSB abgegebenen Empfehlung, so dass sie auch nicht im Rahmen der vorliegenden Weiterziehung in verbindlicher Weise angeordnet werden kann.

5. Gemäss Art. 26 der Verordnung über Organisation und Verfahren eidgenössischer Rekurs- und Schiedskommissionen vom 3.2.1993 (VOVRS; SR 173.31) richten sich die Verfahrenskosten nach Art. 63 VwVG und, mit Ausnahme von Art. 6 Abs. 2, nach der Verordnung über Kosten und Entschädigungen im Verwaltungsverfahren vom 10.9.1969 (VKEV; SR 172.041.0).

a) Die Kosten des Weiterziehungsverfahrens sind gemäss Art. 63 Abs. 1 VwVG der unterliegenden Partei aufzuerlegen. Unterliegt diese nur teilweise, werden die Verfahrenskosten ermässigt. Für die Kostenliquidation ist davon auszugehen, dass der EDSB und die Weiterziehungsbeklagte je als teilweise unterliegende Parteien zu betrachten sind. Die Empfehlung des EDSB wird in ihrer Argumentation im Wesent-lichen bestätigt und in ihrem Kerngehalt beibehalten, jedoch als zu weitgehend erachtet und Drogentests bei Arbeitnehmerinnen und Arbeitnehmern im Einzelfall und bei begründeten Verdachtsmomenten als zulässig erklärt. Dies lässt eine Aufteilung der Kosten im Verhältnis von zwei Drittel zu Lasten der Weiterziehungsbeklagten und ein Drittel zu Lasten des Bundes als angemessen erscheinen.

Unter Zugrundelegung des Gebührenrahmens gemäss Art. 2 VKEV werden die Spruchgebühr auf Fr. 4'000.— und die Schreibgebühr gemäss Art. 3 VKEV auf Fr. 200.—, festgelegt; zuzüglich Barauslagen von Fr. 410.— (Zeugenentschädi-gung) und Fr. 190.— (pauschal) für Kopien werden somit die Verfahrenskosten auf total Fr. 4'800.— festgesetzt.

b) Gemäss Art. 64 Abs. 1 VwVG kann die Beschwerdeinstanz der ganz oder teilweise obsiegenden Partei von Amtes wegen oder auf Begehren eine Entschädigung für ihr erwachsene notwendige und verhältnismässig hohe Kosten zusprechen. Als solche Kosten fallen gemäss Art. 8 Abs. 2 lit. a VKEV namentlich die Kosten anwaltlicher Vertretung in Betracht. Die Bestimmungen über die Anwaltskosten im Tarif des Bundesgerichts über die Entschädigungen an die Gegenpartei vom 9.11.1978 (SR 173.119.1) finden sinngemäss Anwendung

Der Anwalt der Weiterziehungsbeklagten hat unter dem 19. März 2003 eine Kostennote eingereicht, mit welcher unter Hinweis auf einen detailliert ausgewiesenen Aufwand von 194.4 Stunden und gestützt auf Art. 4, 6 und insb. 7 des erwähnten Tarifs ein Anwaltshonorar von Fr. 52'500.— zuzüglich Auslagen und Mehrwertsteuer geltend gemacht wird.

Obschon für die Weiterziehungsbeklagte unzweifelhaft auch wirtschaftliche Interessen mit betroffen sind, weist das vorliegende datenschutzrechtliche Verfahren nicht einen ziffernmässig bestimmten Streitwert auf, sondern gilt als Verfahren ohne Vermögensinteresse. Für solche beträgt das Anwaltshonorar gemäss Art. 6 Abs. 2 des bundesgerichtlichen Tarifs in der Regel Fr. 500.— bis 15'000.—. Der Umfang des vorliegenden Verfahrens rechtfertigt ohne Zweifel die Anwendung von Art. 7 Abs. 1 des Tarifs, wonach bei aussergewöhnlich viel Aufwand verursachenden Streitsachen über diese Ansätze hinausgegangen werden kann. Diese Bestimmung nennt keinen Maximalzuschlag. Den Intentionen des Gesetzgebers am nächsten kommen dürfte eine analoge Anwendung von Art. 153a Abs. 3 (Fassung vom 4.10.1991) des Bundesgesetzes über die Organisation der Bundesrechtspflege vom 16.12.1943 (OG; SR 173.110), wonach das Gericht bei der Bemessung der Gerichtsgebühr über die Höchstbeträge hinausgehen kann, wenn besondere Gründe es rechtfertigen, jedoch höchstens bis zum doppelten Betrag. Dies ergäbe ein Maximalhonorar von Fr. 30'000.—. Gemäss Art. 8 Abs. 3 VKEV vermindert sich dieser Höchstbetrag indessen in Verfahren vor der EDSK um einen Viertel, mithin auf Fr. 22'500.—. Auf diesen Betrag ist das Anwaltshonorar deshalb festzusetzen. Zuzüglich der geltend gemachten Auslagen und Mehrwertsteuer ergibt sich ein Betrag von (gerundet) Fr. 24'750.—.

Bei bloss teilweisem Obsiegen rechtfertigt es sich, die Entschädigung nach Massgabe des Verfahrenausgangs zu kürzen, vorliegend mithin auf einen Drittel der vollen Entschädigung, so dass die Parteientschädigung in Anwendung der oben dargelegten Grundsätze auf Fr. 8'250.— festzusetzen ist.

Aus diesen Gründen wird erkannt:

1. Die Firma Roche hat ihr Konzept dahingehend anzupassen, dass Drogentests nur auf begründeten Verdacht hin im Einzelfall und nur bei Vorliegen einer auf diesen Einzelfall bezogenen Einwilligung vorgenommen werden.

   Sämtliche bisher im Rahmen des Konzeptes der drogenfreien Lehre erhobenen Daten sind zu vernichten, soweit im Einzelfall kein begründeter Verdacht Anlass für einen Test war.

2. Die Verfahrenskosten des Weiterziehungsverfahrens werden auf Fr. 4'800.— bestimmt und zu 2/3, ausmachend Fr. 3'200.—, der Weiterziehungsbeklagten auferlegt. Das rest-liche Drittel der Verfahrenskosten trägt der Bund.

3. Der Weiterziehungsbeklagten wird eine Parteientschädigung von Fr. 8'250.— ausgerich-tet. Diese ist im Umfang der ihr auferlegten Verfahrenskosten mit denselben zu verrech-nen, auszahlbar durch die Bundeskasse somit Fr. 5'050.—.

5. Zu eröffnen: den Parteien

NAMENS DER EIDG. DATENSCHUTZKOMMISSION

Der Präsident: Der Sekretär:

Rechtsmittelbelehrung

Dieser Entscheid kann binnen 30 Tagen seit der Eröffnung gemäss Art. 97 ff. OG mit Verwaltungsgerichtsbeschwerde beim Schweizerischen Bundesgericht angefochten werden. Die Frist kann nicht erstreckt werden. Die Beschwerdeschrift ist, mit Unterschrift versehen, unter Beilage dieses Entscheides, in dreifacher Ausfertigung dem Bundesgericht, Mon Repos, 1000 Lausanne 14, zuzustellen.

13.10 Empfehlungen des EDSB

13.10.1 Empfehlung EDSB – Orange Entlassungsliste

Empfehlung

gemäss

Art. 29 Abs. 3 des Bundesgesetzes

über den Datenschutz vom 19. Juni 1992

in Sachen

Planungstool Top Orange Switzerland (TOP OCH)

I. Der Eidg. Datenschutzbeauftragte stellt fest:

1. Mit Schreiben vom 19. Juni 2003 erstattet die Gewerkschaft Kommunikation (Gewerkschaft) Anzeige gegen Orange Communications SA, Lausanne (Orange), wegen Erstellung der Datensammlung Top Orange Switzerland (TOP OCH). TOP OCH enthält nach Auffassung der Gewerkschaft unverhältnismässige und zweckwidrige Daten über das Verhalten und die Privatsphäre der Angestellten von Orange, welche ohne Wissen der betroffenen Personen gesammelt worden sind und hat als Entscheidungsgrundlage für eine Massenentlassung gedient. Die Gewerkschaft rügt weiter, das Auskunftsrecht sei nicht gewährleistet worden. Sie ersucht den Eidg. Datenschutzbeauftragten, die Rechtmässigkeit von TOP OCH zu überprüfen, dabei den Systemfehler festzustellen und die Gewährleistung des Auskunftsrechtes sowie die Zerstörung der Datensammlung zu empfehlen.

2. Ende Juni 2003 kontaktiert der Eidg. Datenschutzbeauftragte die Firma Orange, um den Sachverhalt im Sinne von Art. 29 des Datenschutzgesetzes näher abzuklären. Orange wird ersucht, Fragen im Zusammenhang mit dem Zweck von TOP OCH, den Zugriffsrechten und dem Auskunftsrecht zu beantworten.

3. In ihrer Antwort vom 30. Juli 2003 erläutert Orange zuerst die Situation rund um den Abbau eines Teils des Arbeitnehmerbestandes. Sie macht geltend, das Planungstool TOP OCH habe nicht als Entscheidungsgrundlage für die Entlassungen gedient, präzisiert aber dennoch, dass die Liste den Zweck hatte, alle Daten, die für die ordnungsgemässe Durchführung des Arbeitsverhältnisses bzw. der anstehenden/abzuwickelnden Restrukturierungsmassnahmen und Kündigungen zu be-

achten sind, komprimiert zusammenzufassen. In die Liste haben Einträge aus den Personaldossiers Eingang gefunden, welche z. T. mit persönlichen, für die Abwicklung der Restrukturierung notwendigen Informationen angereichert wurden. Orange gibt zu, dass einzelfallweise auch subjektive Wertungen in die Liste Eingang gefunden haben. Es habe jedoch zwischen den Einträgen und den Entlassungsentscheiden kein Kausalzusammenhang bestanden. Vor dem Aussprechen von Kündigungen habe Orange gesetzliche Schutzvorschriften zugunsten von schwangeren Frauen, Militärdienstleistende und Kranke beachtet. Der Eintrag betreffend Mitgliedschaft bei der Gewerkschaft war einzig ein Planungstool, um sicherzustellen, dass nach der Entlassung der Servicelevel in verschiedenen Abteilungen aufrechterhalten werden konnte. Auf eine Offenlegung der Liste hätte Orange darum verzichtet, weil es sich dabei um eine Notiz gehandelt hat, welche zu rein persönlichen Zwecken bzw. zur Personalplanung erstellt und Dritten nicht bekannt gegeben worden sei.

4. In ihrer Stellungnahme vom 3. Oktober 2003 erwidert die Gewerkschaft, es bestehe ein Kausalzusammenhang zwischen den Einträgen ins TOP OCH und den Entlassungen von Angestellten, die sich gewerkschaftlich organisiert haben bzw. am Streik mitgewirkt haben. Es verstosse zudem gegen Treu und Glauben, ein dem Personal nicht bekanntes Qualifikationssystem anzuwenden. An TOP OCH seien ausserdem mehrere Personen beteiligt gewesen, sodass nicht von einer persönlichen Notiz gesprochen werden könne.

5. Mit Schreiben vom 14. Oktober 2003 ersucht der Eidg. Datenschutzbeauftragte Orange, den Zusammenhang zwischen den Einträgen im TOP OCH und den Kündigungen nochmals zu erläutern.

6. Am 14. November 2003 nimmt Orange SA zu dieser Frage nochmals Stellung. Dabei wird betont, dass der Zweck der Personalübersicht TOP OCH nicht war, eine Sammlung von möglichen Kündigungsgründen zu erstellen, sondern Informationen übersichtlich und komprimiert bereitzustellen, um die beschlossenen Restrukturierungsmassnahmen im Einzelfall ordnungsgemäss durchzuführen. Bei der Personalliste handle es sich um eine Übersicht für die zentrale Personalabteilung, die im Hinblick auf die Reorganisation aufzeigen sollte, bei welchen Angestellten besondere Rücksicht notwendig war. Es werden im übrigen Bedenken über die Berechtigung des Eidg. Datenschutzbeauftragten geäussert, die Stellungnahme von Orange vom 30. Juli 2003 an die Gewerkschaft Kommunikation ohne ihr Wissen zur Einsichtnahme und Kommentierung zuzustellen. Nach Meinung von Orange SA ist das Untersuchungsverfahren vor dem Eidg. Datenschutzbeauftragten nicht kontradiktorisch ausgestaltet.

II. Der Eidg. Datenschutzbeauftragte zieht in Erwägung:

1. Der Eidg. Datenschutzbeauftragte klärt von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn u. a. Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler, Art. 29 Abs. 1 lit. a DSG). Er kann dabei Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen. Er kann auch Personen vernehmen (Inhaber von Datensammlungen, betroffene Personen, Dritte). Er kann ein *kontradiktorisches Verfahren* durchführen und insbesondere die Meinungen der Parteien vergleichen. Er ist dabei an die allgemeinen Verfahrensregeln, insbesondere an das Gleichbehandlungsgebot gemäss Art. 29 Abs. 1 Bundesverfassung, gebunden. Die Parteien haben im Verfahren vor dem Eidg. Datenschutzbeauftragten Anspruch auf rechtliches Gehör (Art. 29 Abs. 2 Bundesverfassung, BV, SR 101). Danach können die Unterlagen den Parteien vorgelegt werden.

2. Als Datensammlung gilt nach der gesetzlichen Definition (Art. 3 Bst. g Datenschutzgesetz, DSG, SR 235.1) jeder Bestand von Personendaten (Liste, Ordner, Aktenablage, elektronischer Datenträger, usw.), der so aufgebaut ist, dass Informationen über eine bestimmte Person mit einem vernünftigen Aufwand gefunden werden können. Entscheidend ist nach dieser Definition einerseits, dass der Datenbestand Informationen über mehr als eine Person enthält und andererseits ist es die Erschliessbarkeit der Informationen nach betroffenen Personen (U. Belser in Maurer/Vogt [Hrsg.] Kommentar zum Schweizerischen Datenschutzgesetz, Art. 3 N 28). Die Daten sind im Top OCH so aufgebaut, dass sie offenkundig nach betroffenen Personen erschliessbar sind. Das Planungstool Top OCH stellt somit eine *Datensammlung* im Sinne von Art. 3 lit. g DSG dar. Ausserdem waren ausgewählte Mitarbeiter innerhalb der Firma (insb. innerhalb der Personalabteilung) auf TOP OCH zugriffsberechtigt. Es handelt sich folglich nicht um eine Notiz, die zu rein persönlichen Zwecken erstellt und Dritten nicht bekannt gegeben wurde bzw. wird (vgl. Art. 2 Abs. 2 lit. a. DSG), wie Orange behauptet. Die auf Art. 2 Abs. 2 lit. a DSG gestützte Begründung, wonach das DSG auf Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt, nicht anwendbar ist, scheitert auch daran, dass die entsprechende Ausnahme nur für natürliche Personen gilt. Die Liste TOP OCH hätte als Datensammlung beim Eidg. Datenschutzbeauftragten angemeldet werden müssen, da sie besonders schützenswerte Personendaten beinhaltet und die betroffenen Personen keine Kenntnis davon hatten (Art. 11 Abs. 3 DSG).

3. Datenbearbeitungen müssen nach Treu und Glauben erfolgen (Art. 4 Abs. 2 DSG). Aus diesem Prinzip ist die Anforderung abzuleiten, dass eine Datenbearbeitung für die betroffene Person transparent erfolgen muss. Dies bedeutet, dass eine Datenbeschaffung und jede weitere Datenbearbeitung grundsätzlich für die betroffene Person erkennbar sein muss (*vorherige Information* der betroffenen Personen, vgl. dazu U. Maurer, Kommentar zum Schweiz. Datenschutzgesetz, a. a. O., Art. 4 N9). Eine Verletzung dieses Grundsatzes liegt etwa vor, wenn Daten ohne Wissen der betroffenen Person bearbeitet werden. Dies gilt auch für die Bearbeitung von Personendaten zu Zwecken der Personalplanung. Orange begründet die fehlende Information über die Existenz von TOP OCH damit, dass es sich dabei um eine Zusammenstellung von Personendaten aus dem Personaldossier handelt, das dem Auskunftsrecht bereits unterliegt, welche mit weiteren persönlichen Notizen angereichert wurde. Zudem stützt sie ihre Begründung auf den Leitfaden des Eidg. Datenschutzbeauftragten über den Datenschutz im Arbeitsbereich ab, wonach Notizen, die zu rein persönlichen Zwecken bzw. zur Personalplanung erstellt worden sind und Dritten nicht bekannt gegeben werden, nicht offen gelegt werden müssen. In diesem Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich (http://www.edsb.ch/d/doku/leitfaeden/arbeit/arbeit.pdf, insb. S. 19) ist von Einschränkung bzw. Verweigerung des Auskunftsrechts, nicht aber von fehlender vorheriger Information über eine bestimmte Datenbearbeitung die Rede. Gestützt auf Art. 4 Abs. 2 DSG und den daraus resultierenden Transparenzgrundsatz muss grundsätzlich jede Datenbearbeitung bekannt gegeben werden. Eine Abweichung von Art. 4 Abs. 2 DSG ist gemäss Art. 12 Abs. 2 lit. a DSG insbesondere möglich, wenn überwiegende private oder öffentliche Interessen des Datenbearbeiters dies rechtfertigen. Die Tatsache, dass die im TOP OCH bearbeiteten Daten teilweise bereits im Personaldossier vorhanden waren und das Recht auf Auskunft über den Inhalt des Personaldossiers bestand, vermag die fehlende Information über TOP OCH nicht zu rechtfertigen. Dies umso weniger, als zugegebenermassen die Datensammlung mit weiteren persönlichen Notizen angereichert wurde. Orange SA hätte spätestens ab offizieller Information über die Massenentlassung das Bestehen der Liste an die Mitarbeiter kommunizieren müssen, damit Letztere das Auskunftsrecht hätten ausüben können.

4. Top OCH stellt eine eigenständige, von den Personaldossiers getrennte und mit spezifischen Zugriffsrechten versehene Datensammlung dar. Gemäss Art. 8 Abs. 1, 2 und 5 DSG kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden (*Auskunftsrecht*). Der Inhaber der Datensammlung muss ihr u. a. alle über sie in der Datensammlung vorhandenen Daten mitteilen. Die Auskunft ist in der Regel schriftlich, in Form eines

Ausdrucks oder einer Fotokopie sowie kostenlos zu erteilen. Art. 9 Abs. 3 DSG legt fest, dass Private als Inhaber einer Datensammlung die Auskunft verweigern, einschränken oder aufschieben können, soweit eigene überwiegende Interessen es erfordern und sie die Personendaten nicht an Dritte bekannt geben. Art. 9 Abs. 4 DSG verpflichtet den Inhaber der Datensammlung anzugeben, aus welchem Grund er die Auskunft verweigert, einschränkt oder aufschiebt. Für die Anforderung an diese Begründung ist massgebend, dass sie einerseits dem Betroffenen ermöglichen muss, die Zulässigkeit und Stichhaltigkeit der Beschränkung zu überprüfen, andererseits den Richter befähigen muss, die wesentlichen Entscheidungsgründe des Inhabers der Datensammlung für die Nichtgewährung der Auskunft nachvollziehen zu können.

Das Gesetz verwendet sowohl für die allgemeinen (Art. 9 Abs. 1 Bst. b DSG) wie für die besonderen Einschränkungsgründe (Art. 9 Abs. 2 Bst. a DSG und Art. 9 Abs. 3 DSG) den Begriff der «überwiegenden (Geheimhaltungs-) Interessen». Damit wird deutlich, dass irgendein privates oder öffentliches Geheimhaltungsinteresse - welches in den meisten Fällen vorliegen dürfte – den Auskunftsanspruch noch nicht zu verdrängen vermag. Das Auskunftsrecht wird nur dann und nur insoweit durch Geheimhaltungsinteressen eingeschränkt, als diese das Interesse an der Auskunft in concreto überwiegen. Die einander entgegenstehenden Interessen an der Akteneinsicht einerseits und an deren Verweigerung andererseits sind im Einzelfall sorgfältig gegeneinander abzuwägen (A. Dubach, Kommentar zum Schweizerischen Datenschutzgesetz, a. a. O., Art. 9 N 6, 9 und 10). Wie bereits im vorherigen Paragraph festgehalten, hat Orange es im ersten Schriftenwechsel versäumt, einen genügenden Rechtfertigungsgrund für die Verweigerung des Auskunftsrechtes anzugeben. Im Schreiben vom 14. November 2003 beruft sich Orange auf ein Urteil des Arbeitsgerichtes Zürich vom 19. September 2003, wonach eine Offenlegungspflicht von Orange hinsichtlich der zusammenfassenden Personalliste in Anwendung von Art. 9 Abs. 3 DSG verneint wurde, da es sich bei der Personalliste um eine Übersicht für die zentrale Personalabteilung handelte, die im Hinblick auf die Reorganisation aufzeigen sollte, bei welchen Angestellten besondere Rücksicht notwendig war. In solchen Planungsunterlagen - so das Gericht – müsse dem einzelnen Angestellten keine Einsicht gewährt werden, da neben den firmeninternen Reorganisationsinformationen auch der Datenschutz anderer betroffenen Angestellten verletzt werden könnte. Dem kann erwidert werden, dass die Personendaten anderer Angestellten auf der Liste durch einfache Massnahmen problemlos hätten verheimlicht werden können. Die Frage, ob firmeninterne Reorganisationsinformationen aufgrund überwiegender Interessen im Sinne von Art. 9 Abs. 3 DSG geheimgehalten werden dürfen, kann offen bleiben. Spätestens ab Zeitpunkt der offiziellen Information über die Massenentlassung hätte aber das Auskunftsrecht gewährleistet

werden müssen, da keine weiteren überwiegenden Interessen der Firma an die Verweigerung, Einschränkung oder Aufschiebung des Auskunftsrechtes mehr bestanden und die Mitarbeiter das Recht hatten, zu erfahren, ob sie auf der Entlassungsliste figurierten.

5. In § 2 («Vorbemerkung») Ihres Schreibens vom 30. Juli 2003 hält Orange fest, «das Planungstool diente zu keiner Zeit als Entscheidungsgrundlage für irgendwelche Entlassungen». In § 2.2 Ihres Schreibens hält Orange jedoch weiter fest, Top OCH hatte den Zweck, alle Daten, die für die ordnungsgemässe Durchführung des Arbeitsverhältnisses bzw. der anstehenden/abzuwickelnden Restrukturierungsmassnahmen und Kündigungen zu beachten sind, komprimiert zusammenzufassen. Auch im Schreiben vom 14. November 2003 ist Orange der Auffassung, dass die fragliche Liste nicht als Entscheidungsgrundlage für die Auswahl der zu entlassenden Mitarbeiter diente, sondern eine übersichtliche und komprimierte Bereitstellung von Informationen darstellte, um die beschlossenen Restrukturierungsmassnahmen im Einzelfall ordnungsgemäss durchzuführen. Was das konkret bedeutet, ist unklar. Orange führt zwar einige Beispiele auf, welche belegen sollen, dass die Kündigungen nicht im Zusammenhang mit den gesammelten Daten stehen. Ihre Aussagen über den Zweck der Liste lässt aber keinen Zweifel zu, dass *TOP OCH als Entscheidungsgrundlage für die Massenentlassungen* gedient hat oder gedient haben kann.

6. Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind (Art. 328b erster Satz OR). Diese Bestimmung übernimmt und hebt das *Verhältnismässigkeits- und Zweckmässigkeitsprinzip* von Art. 4 Abs. 2 und 3 DSG im Arbeitsbereich hervor. Die Bearbeitung von Daten über Leistung, Verhalten, Krankheit oder Schwangerschaft ist demzufolge zulässig, sofern Letztere objektiv sind und die Voraussetzungen von Art. 328b OR erfüllen. Objektive Leistungs- und Verhaltensdaten werden in der Regel im Rahmen von offenen Mitarbeiterbeurteilungen oder arbeitsrechtlichen Entscheidungen (z. B. Einzelentlassungen oder Massenentlassungen), Daten über Gesundheit und Schwangerschaft normalerweise im Zusammenhang mit der Abwesenheitsverwaltung bearbeitet. Sofern weder die freie und aufgeklärte Einwilligung der betroffenen Personen noch ein anderer Rechtfertigungsgrund vorliegt, dürfen Daten aus der Privatsphäre des Arbeitnehmers im Rahmen des Arbeitsverhältnisses nicht bearbeitet werden.

7. Die Bearbeitung von Daten über die *Schwangerschaft* und über die *Gesundheit* zum Zweck der Entlassung stellt eine unzulässige Zweckentfremdung dar, wenn sie die Rechtsgleichheit (Art. 8 Bundesverfassung, BV, SR 101), den Kündigungsschutz (Art. 336 OR) oder das Gleichstellungsgesetz (GlG, SR 151.1) verletzen. Gesundheitsdaten und Daten im Zusammenhang mit einer Schwangerschaft dürfen auf Entlassungslisten wie TOP OCH nicht bzw. nur dann bearbeitet werden, wenn sie den Kündigungsschutz bezwecken und die Gleichstellung von Frau und Mann fördern, es sei denn, die fraglichen Persönlichkeitseigenschaften beeinträchtigen wesentlich die Zusammenarbeit im Betrieb (Art. 336 Abs. 1 lit. a OR). Im letzteren Fall trägt der Arbeitgeber die Beweislast und muss die Beeinträchtigung der Zusammenarbeit nicht selber verursacht haben. Ausserdem darf der Arbeitgeber die Ausnahme von Art. 336 Abs. 1 lit. a OR nur als ultima ratio geltend machen (Brunner, Bühler, Waeber in «Commentaire du contrat du travail», éditions Réalités sociales 1996, Art. 336 N4). Die Bearbeitung von Daten über die *Zugehörigkeit zu einer Gewerkschaft* oder über die *Ausübung eines Verfassungsrechtes* zum Zwecke der Entlassung kann die Koalitionsfreiheit gemäss Art. 28 BV, die Rechtsgleichheit gemäss Art. 8 BV, den Kündigungsschutz gemäss Art. 336 OR und das Verhältnismässigkeitsprinzip tangieren, es sei denn, die Rechtsausübung verletze eine Pflicht aus dem Arbeitsverhältnis oder beeinträchtige wesentlich die Zusammenarbeit im Betrieb (vgl. Art. 336 Abs. 1 Ziff. b OR). Bemerkungen wie «Delegate of the Union» dürfen somit nicht auf der Entlassungsliste figurieren. Auch die Bemerkung «Leader of the Revolution» gehört nicht auf einer solchen Liste, weil sie subjektiv ist und daraus nicht hervorgeht, worin der Arbeitsvertrag verletzt wurde. Weitere *subjektive Verhaltenswertungen* wie «catastrophic attitude» sind durch objektive Wertungen zu ersetzen (z. B. «attitude problem»). Die Bearbeitung unnötiger *Daten aus der Privatsphäre* (z. B. «personal problem», oder «heiratet demnächst») stellen eine Verletzung von Art. 328b OR und dürfen auf Entlassungslisten nicht figurieren.

8. Das Verhältnismässigkeitsprinzip spielt auch im Zusammenhang mit der *Aufbewahrungsdauer* der Daten eine Rolle. Diese dürfen bis Erreichung des angegebenen Zweckes, gegebenenfalls bis Abschluss hängiger Verfahren und der entsprechenden Rekursfristen aufbewahrt werden.

9. Aufgrund des Gesagten wird festgestellt, dass die Liste TOP OCH ein *Systemfehler* im Sinne von Art. 29 Abs. 1 lit. a. DSG darstellt, da sie geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen.

III. Aufgrund dieser Erwägungen empfiehlt der Eidg. Datenschutzbeauftragte:

1. Soweit die Liste TOP OCH weiterhin besteht oder eine neue bzw. ähnliche Liste hergestellt wird, hat Orange SA die betroffenen Personen über ihr Bestehen zu informieren und den auskunftsersuchenden Personen das Auskunftsrecht gemäss Art. 8 DSG zu gewähren.
2. TOP OCH darf so lange aufbewahrt werden, bis allfällige Gerichtsentscheide in Rechtskraft erwachsen sind.
3. Bei allfälligen weiteren Massenentlassungen hat die entsprechende Entlassungsliste die Schweiz. Gesetzgebung, insbesondere den Kündigungsschutz, die Rechtsgleichheit, die Koalitionsfreiheit und die Gleichstellung von Frau und Mann zu beachten und ist inhaltlich auf jene Datenkategorien zu beschränken, welche für die ordnungsgemässe Durchführung der Massenentlassung nötig und geeignet sind.
4. Orange SA teilt dem Eidg. Datenschutzbeauftragten innerhalb von 30 Tagen nach Erhalt dieser Empfehlung mit, ob sie die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung abgelehnt oder nicht befolgt, so kann der Eidg. Datenschutzbeauftragte die Angelegenheit der Eidg. Datenschutzkommission vorlegen.
5. Die vorliegende Empfehlung wird der Firma Orange SA eingeschrieben zugestellt und gestützt auf Art. 30 Abs. 2 DSG publiziert.
6. Eine Kopie der Empfehlung wird an die Gewerkschaft Kommunikation zugestellt.

DER EIDGENÖSSISCHE

DATENSCHUTZBEAUFTRAGTER

Der Beauftragte:

Hanspeter Thür